Driver's License and Credential Issuance System

CRFP DMV1800000001

ORIGINAL

Gemalto, Inc.
9442 Capitol of Texas Hwy North
Plaza II, Suite 100
Austin, TX 78759 USA

Neville Pattinson
Phone: 512-257-3982
Neville.Pattinson@gemalto.com

Date: July 2nd , 2018

gemalto
security to be free

Table of Contents

Title Page

Table of Contents

(TAB A) Attachment A-Vendor Response Sheet

Appendix 01 Gemalto Facial Recognition Solution Press Release

(TAB B) Attachment B-Mandatory Specification Checklist

(TAB C) Attachment C-Separate Envelope

(TAB D) Attachment D-Regional Offices, Locations, and ICWs

(TAB E) Attachment E-Production Volumes over the last 12 months

(TAB F) Attachment F-WV Division of Motor Vehicles Contract Privacy Policy

(TAB G) Attachment G-Current Card Types

(TAB H) Attachment H-PII acknowledgment

(TAB I) Signed Documents

In a separate envelope

Attachment C-Cost Sheet

State of West Virginia

Division of Motor Vehicles

Driver's License and Credential Issuance System

CRFP DMV1800000001

Attachment A – Vendor Response Sheet

Gemalto, Inc.
9442 Capitol of Texas Hwy North
Plaza II, Suite 100
Austin, TX 78759 USA

gemalto
security to be free

Table of Contents

Confidentiality Disclaimer 5
Statement Concerning Trade Secret Information 5
Qualification and Experience 8
Proposed Staffing Plan 12
Vendor References 17
CENTRAL ISSUANCE 26
Section 4, Subsection 4.1 - REAL ID Compliance Objectives 26
Section 4, Subsection 4.2 - Central Issuance Facility Objective 38
Section 4, Subsection 4.3 - Card Images 40
Section 4, Subsection 4.4 - Card Design 41
Section 4, Subsection 4.5 - Card Carriers 48
Section 4, Subsection 4.6 - Card Durability 50
Section 4, Subsection 4.7 - Quality Assurance (QA) 51
ON-PREMISE 57
Section 4, Subsection 4.8 - Facility Image & Signature Capture Workstation ("ICW") Objectives 57
Section 4, Subsection 4.9 - Secure Temporary DLID 83
Section 4, Subsection 4.10 - Consumables for Secure Temporary DL 84
Section 4, Subsection 4.11 - Signature Capture 85
Section 4, Subsection 4.12 - Credential Issuance System (CIS) Objectives 91
SYSTEM ADMINISTRATION 109
Section 4, Subsection 4.13 - User Account Management 109
Section 4, Subsection 4.14 - System Usage Dashboard 110
Section 4, Subsection 4.15 - Management of Central Issuance Records 112
Section 4, Subsection 4.16 - Reports 113
Section 4, Subsection 4.17 - Controlled Use 115
Section 4, Subsection 4.18 - Protection 115
Section 4, Subsection 4.19 - Data Management 115
Section 4, Subsection 4.20 - Audit functions 117
Section 4, Subsection 4.21 - Equipment installation 118
CARD DESIGN AND SECURITY FEATURES REQUIREMENTS 120

Section 4, Subsection 4.22 - Secure Temporary Driver's License and ID's 120
Section 4, Subsection 4.23 - Card Design Changes 122
PROJECT MANAGEMENT 123
Section 4, Subsection 4.24 123
Section 4, Subsection 4.25 123
Section 4, Subsection 4.26 124
Section 4, Subsection 4.27 - Communication 124
Section 4, Subsection 4.28 - Status Reporting 125
Section 4, Subsection 4.29 - Project Work Plan Objective 128
Section 4, Subsection 4.30 - Test Plan Objective 142
Section 4, Subsection 4.31 - Test Plan 144
Section 4, Subsection 4.32 - Test Scripts 148
Section 4, Subsection 4.33 - Documentation for Testing 149
Section 4, Subsection 4.34 - User Acceptance Testing 151
Section 4, Subsection 4.35 - Test Materials 152
Section 4, Subsection 4.36 - Test Systems 152
Section 4, Subsection 4.37 - Training Plan Objective 154
Section 4, Subsection 4.38 - Training Guide Objective 158
Section 4, Subsection 4.39 - Training Guide 159
Section 4, Subsection 4.40 - User Operations Manuals Objectives 160
Section 4, Subsection 4.41 - Technical Documentation Objective 162
Section 4, Subsection 4.42 - Updates to Documentation Objective 164
Section 4, Subsection 4.43 - Implementation Plan Objective 165
Section 4, Subsection 4.44 - On-site Training 167
Section 4, Subsection 4.45 - Account Manager for Operations 169
SERVICE LEVEL AGREEMENT 169
Section 4, Subsection 4.46 - Replacement of Equipment / Inventory of Spares 169
Section 4, Subsection 4.47 - Service Response Times 170
Section 4, Subsection 4.48 - Help Desk Support 172
Section 4, Subsection 4.49 - Help Desk Reporting System 175
Section 4, Subsection 4.50 - Implementation Plan 177
Section 4, Subsection 4.51 - 14 Day Pre-Post Support Plan 182

Confidentiality Disclaimer

State of West Virginia
Purchasing Division
Request for Proposal (RFP)
To Provide Driver's License and ID Cards
CRFP 0802 DMV1800000001

Statement Concerning Trade Secret Information

Certain information herein qualifies as ***Trade Secret*** and is therefore exempt from disclosure under the West Virginia Freedom of Information Act, West Virginia Code §29B-1-1 *et seq*. (the "WV FOIA"). We respectfully submit this Statement Concerning Trade Secret Information and request that the State of West Virginia, Purchasing Division maintain its confidentiality.

With regard to the as ***Trade Secret*** information, such information includes formulae, plans, patterns, processes, tools, mechanisms, compounds, procedures, production data or compilations of information which are not patented and which are known only to certain individuals within Gemalto, Inc. ("Gemalto") who are using it to fabricate, produce or compound an article or trade a service or to locate minerals or other substances having commercial value, and which gives Gemalto an opportunity to obtain business advantage over competitors. (*W. VA Code §29B-1-4(a)(1))*

Document claiming a statutory exemption to the Freedom of Information Act	**Statutory exception of the Freedom of Information Act that applies**	**Explanation** (*Reason Code*) Manner in which the statutory exception to the Public Records Act applies
Attachment A – Section 4, Subsection 4.2.3	*W. VA Code §29B-1-4(a)(1)*	*8-Facility Layout and Security Systems*
Attachment A – 4.50.1.4	*W. VA Code §29B-1-4(a)(1)*	*6-Project Implementation Method and Process*

The beginning and end of confidential sections, which contain such trade secret information are marked as follows:

-----------------------------------BEGIN Gemalto Trade Secret Information------------------------------

Trade Secret Information

-----------------------------------END Gemalto Trade Secret Information--------------------------------

Table of reason codes and descriptions

Reason code	Textual Description
1-Equipment Operation and Process Description	The information referenced describes the detailed operation of the equipment proposed and the processes that are to be implemented, including configuration and techniques employed to protect the security and integrity of the final solution. Protection of this proprietary, trade secret information is required to preclude the loss of competitive and economic advantage and to protect system and data integrity. This information is generally the subject of efforts to maintain its secrecy from competitors and the general public.
2-System Operation and Process Description	The information referenced describes the detailed operation of the system proposed and the processes that are to be implemented, including programs and methods employed to protect the security and integrity of the final solution. Protection of this proprietary, trade secret information is required to preclude the loss of competitive and economic advantage and to protect system and data integrity. This information is generally the subject of efforts to maintain its secrecy from competitors and the general public.
3-System Security Processes and Techniques	The information referenced describes the detailed techniques of system security of the system proposed and the processes that are to be implemented. This information includes programs, equipment, and methods employed to protect the security and integrity of the final solution. Protection of this proprietary, trade secret information is required to preclude the loss of competitive and economic advantage and to protect system and data integrity. This information is generally the subject of efforts to maintain its secrecy from competitors and the general public.
4-Document Security Patterns and Techniques	The information referenced describes the detailed techniques and patterns of secure document design for the solution proposed. This information includes details of the methods employed to protect the security and integrity of the final secure identity documents. Protection of this proprietary, trade secret information is required to preclude the loss of competitive and economic advantage and to protect document and data integrity. This information is generally the subject of efforts to maintain its secrecy from competitors and the general public.

Reason code	Textual Description
5-Document Production Processes and Techniques	The information referenced describes the detailed processes and techniques of document production of the solution proposed and the configuration of the facilities that are to be implemented. This information includes site designs, equipment, and methods employed to protect the security and integrity of the final solution. Protection of this proprietary, trade secret information is required to preclude the loss of competitive and economic advantage, and to protect system and data integrity. This information is generally the subject of efforts to maintain its secrecy from competitors and the general public.
6-Project Implementation Method and Process	The information referenced describes the detailed methods of project implementation of the system proposed and the project execution and control processes that are to be followed. Protection of this proprietary, trade secret information is required to preclude the loss of competitive and economic advantage. This information is generally the subject of efforts to maintain its secrecy from competitors and the general public.
7-Project Support Method and Process	The information referenced describes the detailed methods of project support of the system proposed and the operational support execution and control processes that are to be followed. Protection of this proprietary, trade secret information is required to preclude the loss of competitive and economic advantage. This information is generally the subject of efforts to maintain its secrecy from competitors and the general public.
8-Facility Layout and Security Systems	The information referenced includes details of facility layouts, contents, and security systems and operations that, if compromised, will represent a real and immediate threat to the Security of the State. This information is generally the subject of efforts to maintain its secrecy from competitors and the general public.
9-Protected Sensitive Corporate Materials	The information referenced includes details of organization, personnel, corporate finance, clients, policies, and Corporate processes associated with corporate management and governance. Protection of this proprietary, trade secret information is required to preclude the loss of competitive and economic advantage. This information is generally the subject of efforts to maintain its secrecy from competitors and the general public.

Qualification and Experience

Staff Qualifications and Experience

Information regarding vendor's firm, such as staff qualifications and experience in completing similar projects; references; copies of any staff certifications or degrees applicable to this project.

VENDOR RESPONSE:

Driver's License Experience
First, it is important to note that **our team is currently supporting West Virginia DMV** in the provision of its driver license and ID cards and all of the required applications including image capture, document authentication, and facial recognition.

Gemalto is the fastest growing provider of Driving License Solutions in North America, and we proudly support 14 DMV jurisdictions in addition to West Virginia: **Alaska, California, Colorado, Hawaii, Idaho, Quebec, Maryland, New Hampshire, Washington DC, Wyoming, and the four Atlantic Provinces (Newfoundland and Labrador, Nova Scotia, New Brunswick, and Prince Edward Island)**. In addition, we awarded the DL contract for the State of Georgia to provide driver licenses, central issuance, image capture, and facial recognition solutions.

In reviewing the work required by this RFP and our deep understanding of your needs, we broke down each of the components solution that West Virginia is seeking and covered our direct experience in providing each of the components to other jurisdictions, in addition to what we have provided to you.

Image Capture
In addition to the state of West Virginia, Gemalto currently provides our image capture solution to eleven (11) other jurisdictions including Alaska, Colorado, Hawaii, Idaho, New Brunswick, New Hampshire, Newfoundland and Labrador, Nova Scotia, Prince Edward Island, Washington DC, and Wyoming.

We assisted West Virginia in becoming one of the first in the country to incorporate the solicitation of applicant information using a signature pad, specifically for address verification and motor voter. We have advanced our capabilities in that we now offer a new signature pad which has a larger display to allow applicants to complete the DL/ID application using the signature pad to avoid having the applicant manually completing it and then having the user scan the documents and then attach the file to the applicant's record. This has proven to be a timesaver in Idaho's business process, in particular.

Document Authentication
In addition to West Virginia, Gemalto currently provides a document authentication solution to five (5) jurisdictions including California, Colorado, Hawaii, Idaho, and New Hampshire.

This past year, Gemalto acquired the identity management business of 3M, which was mainly comprised of 3M Cogent. Part of this acquisition included document authentication scanning equipment. With this acquisition, Gemalto is now the leading provider of this equipment. In fact, many of our competitors use our equipment because of its accuracy and ease of use. While West Virginia has stated in vendors Q&A that a Document Authentication solution is not required, this can be provided to the state as an additional contract option.

Facial Recognition

In addition to West Virginia, Gemalto currently provides our facial recognition solution to nine (9) jurisdictions including Alaska, Colorado, Hawaii, Idaho, Washington DC, West Virginia, New Brunswick, Newfoundland and Labrador, Nova Scotia, and Prince Edward Island. In addition, Gemalto is providing a level one facial recognition review service to New Brunswick and Nova Scotia in an effort to have their investigators only focus on those cases that require thorough investigation.

One of the other key areas of the 3M Cogent acquisition is that they are one of the leading providers of biometric verification solutions that include facial recognition, automatic fingerprint identification systems, and iris verification solutions. In fact, Gemalto participated in a biometric rally for the US Department of Transportation, using our Live Face Identification System (LFIS) as the core technology, and the solution outperformed the average range for most metrics in addition to a 99.44% successful acquisition rate in less than 5 seconds compared to the average of 65%.

You can read the full story In **"Appendix 01 - Gemalto Facial Recognition Solution Press Release"**

Driver License and ID Production and Issuance

Gemalto currently provides driver license and ID cards to thirteen (13) jurisdictions in addition to West Virginia. Of those 14 jurisdictions, Gemalto provides its polycarbonate cards to Quebec, Maryland, Colorado, Washington DC, New Brunswick, Newfoundland and Labrador, Nova Scotia and Prince Edward Island. With eight (8) jurisdictions using polycarbonate, Gemalto provides more jurisdictions with polycarbonate cards than any other provider in the market. We should also note that Georgia has also selected polycarbonate as its substrate of choice.

In addition, all 14 jurisdictions, including West Virginia, are issued centrally either through one of our issuance centers or we have enabled three (3) of the jurisdictions to issue from their facilities using our issuance solution. These three jurisdictions include Maryland, New Hampshire, and Quebec.

We believe that we have the most advanced security features and that our approach to security design is second to none. This can be evidenced by the award we received last year for Maryland's Polycarbonate Driver License – the 2017 International Card Manufacturers Association Design of the Year.

Staff Experience

Gemalto understands that organization and experienced staffing are key to a successful project. Therefore, we will provide the best qualified staff in order to exceed expectations and deliver each deliverable as per the schedule and in accordance to the acceptance criteria. We have a large team based in Austin, TX experienced in the delivery of driver's licenses solutions. For this program, Gemalto will have Tony Wallette, a PMP Certified Project Manager, lead the Gemalto team.

We have included additional information on the proposed key staff and their relevant experience in the below response to the **Proposed Staffing Plan** requirement.

Gemalto Background

Gemalto, Inc. was formed in 2006 by the merger of Gemplus and Axalto. From time-to-time, it has absorbed some of its subsidiary companies through merger (with such subsidiaries merging with and into Gemalto, Inc., which remains the surviving corporation); Gemalto, Inc. has otherwise not changed form, structure or name since then.

In 2014, Gemalto acquired Marquis ID Systems (MIDS), a primary provider of fully integrated solutions and services for Drivers License and Identification. With nearly 14 years servicing and supporting DL/ID programs for AAMVA jurisdictions in the US, including West Virginia, MIDS specialized in secure personalized enrollment and issuance systems to meet the specific requirements of each State. By acquiring MIDS, Gemalto was able to strengthen its experience in the US driver license market. We are currently the fastest growing provider of driver license solutions in the US and Canada. MIDS is currently a wholly owned subsidiary of Gemalto, Inc., but intends to merge with and into Gemalto, Inc. shortly, with Gemalto, Inc. remaining the surviving corporation.

In 2015 Gemalto acquired SafeNet. Headquartered in Belcamp, Maryland, US, and located in 27 countries, SafeNet is one of the largest dedicated digital information security companies in the world, trusted to protect, control the access to, and manage the world's most sensitive data and high value software applications. At the time of the acquisition, SafeNet employed approximately 1,500 employees, who served more than 25,000 customers, both corporations and government agencies, in over 100 countries. SafeNet was an important acquisition for Gemalto because we wanted to improve the level of security of the citizen data we are trusted to protect by adding state-of-the-art encryption and securing the access to that data.

Also in 2015, we acquired a card manufacturing provider, Trüb, which had some of the most advanced security features in the card industry. Gemalto continually introduces new card security features to stay ahead of those that profit from creating fraudulent identity documents. This acquisition has allowed Gemalto to offer to our customers, the largest, most advanced level of security features in the Industry.

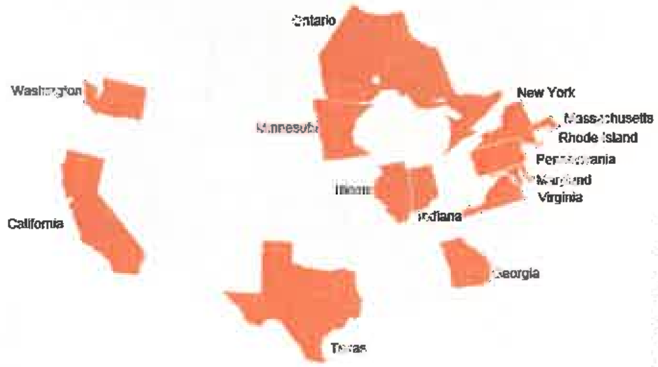
Finally in 2017, Gemalto finalized the acquisition of 3M's Identity Management Business, including 3M Cogent, one of the world leaders in security materials, document readers, fingerprint capture devices, MultiBiometrics and Border solutions. Due to this acquisition, Gemalto is positioned to be the largest provider of document verification devices and has one of the most advanced fingerprint identification and facial recognition solutions with hundreds of references worldwide, including the US Entry program.

The above-mentioned acquisitions were highlighted because these acquisitions have a direct, positive impact to the offer that we can make to you, especially given the acquisition of MIDS. Since the acquisition, we have upgraded one customer previously on the MIDS platform and are in the process of upgrading two others to a robust, state-of-the-art platform and we hope to have the opportunity to do that for you.

Gemalto is now a global company with a strong, local footprint. We have 16,000+ employees that are located in 48 countries, 112 offices, 43 issuance and data centers, 30 R&D centers, and 19 card production facilities. Our global footprint can be seen in the map below:

Our goal is to be close to our customers. With that being said, our strong, local footprint can be seen in the map provided below. Gemalto has approximately 2,200 employees in North America.

Gemalto US & Canada Facilities



- Abingdon, MD
- Atlanta, GA – Issuance Facility
- Austin, TX – Gemalto, Inc Headquarters
- Belcamp, MD
- Bellevue, WA
- Burlington, CAN – Gemalto Canada, Inc.
- Chicago, IL
- Fort Wayne, IN – Issuance Facility
- Fort Worth, TX – Data Center
- Irving, TX
- Latham, NY
- Montgomeryville, PA – Manufacturing
- North Kingstown RI – Issuance Facility
- Ottawa, CAN
- Pasadena, CA
- Redwood City, CA
- Reston, VA
- St Paul, MN
- Tewksbury, MA
- Williamsburg, VA

Proposed Staffing Plan

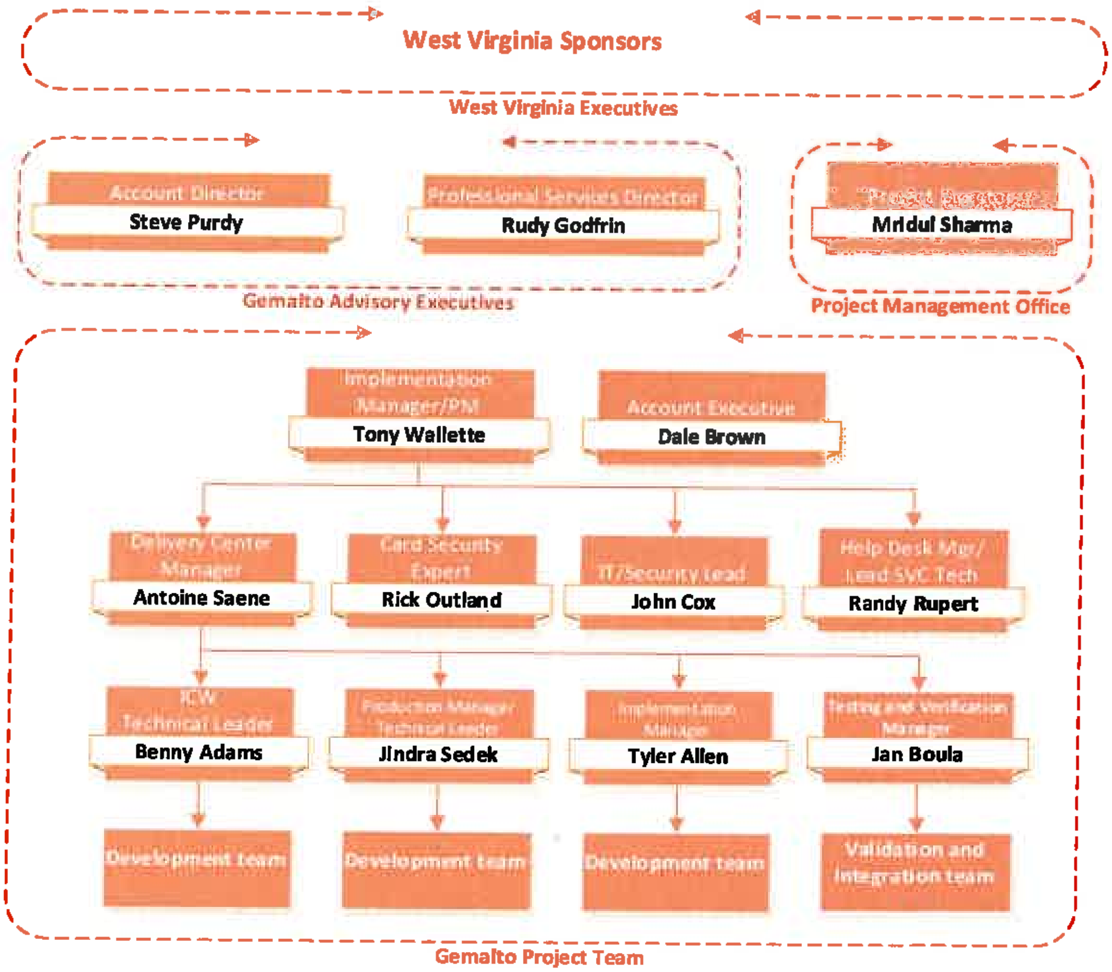
VENDOR RESPONSE:

Gemalto places great value on the impact of strong project planning and organization, and in having experienced staff members supporting throughout the project implementation phases. We believe we illustrated that to you towards the end of 2017. We will leverage the staff that has been supporting you over the past five (5) years and some of the new faces that you have gotten to know in the past couple of years in order to make this transition an overwhelming success. Typically, Gemalto staff will be onsite for the majority of the project planning phase for workshops and onsite for the duration of deployment and training. In addition, the project manager will be on site on a regular basis for meetings throughout the duration of the project.

Key Staff organization:

Driver's License and Credential Issuance System

Gemalto Project Team



From a high level, Gemalto following roles for the project teams who will assist the project manager in the delivery of West Virginia's new Driver's License and Credential Issuance System.

Pre Deployment Staff

- **Account Director** – is the sponsoring executive from Gemalto overseeing and advising on all business items.
- **Account Executive** – serves as the primary point of contact for all business related issues for both pre and post deployment activities.

- **Project Advisor** – senior management from Gemalto with global experience in the delivery of ID and credential issuance solutions provide oversight, experience, and best practices to the Gemalto and DMV project teams.
- **Project Manager** – manages all day to day activities including project planning, communications, and hardware and software delivery.
- **Support Manager** – oversees all support activities for both preventative and remedial maintenance for the entire Gemalto solution.
- **Technical Advisors** – Gemalto leverages subject matter experts (SME) for topics such as IT security, encryption, architecture, and card/document security.
- **Solution Architect** – creates the "blueprint" for Gemalto entire technical solution.
- **Technical Leads** – lead customization efforts for each sub-component of Gemalto solution including the Image Capture Workstation (ICW), Central Server Solution, and Production Management Software.
- **Software Developers** – support technical leads in the development and customization of Gemalto solution for the State of West Virginia
- **Software Validators/QA** – ensures all delivered components meet the DMV's requirements as described in the Requirements Specifications (RQS) and Acceptance Test Plans (ATP).
- **Field Technicians** – are the boots on the ground rapidly deploying Gemalto field office solution.
- **Trainers** - educate DMV staff on their new solution providing training for all components of the solution both in DMV headquarters and Field offices.
- **Technical Writers** – create user guides and training materials for all components of State of West Virginia's new solution.

Post-Deployment Staff

- **Account Director** – is the sponsoring executive from Gemalto overseeing and advising on all business items
- **Account Executive** – serves as the primary point of contact for all business related issues for both pre and post deployment activities.
- **Support Manager** – oversees all support activities for both preventative and remedial maintenance for the entire Gemalto solution.
- **Field Technicians** – embedded staff that perform all preventative and remedial maintenance for the Image Capture Workstations (ICW), Central Server Solution, and Central Issuance Facility.
- **Help Desk/Customer Service Representatives** – answer service request calls for Gemalto' solution and dispatch field technicians if the issue cannot be resolved over the phone.

Key Staff Overview:

Rudy Godfrin – Professional Services Director

Mr. Godfrin is an experienced Director with 10+ years in the Government Program market. His security expertise is on cryptography, data security, and key management systems. Some of Rudy's skills include consulting services, remote and international management, project management, complex solution design, solution implementation, and business process. Rudy has also served as project advisor to Maryland and Idaho as well as Security Technology expert to New Hampshire.

Steve Purdy – Account Director

Mr. Purdy brings over 20 years of experience focusing on business process, project management, customer service, and marketing. His formal education includes a Bachelor's Degree in Marketing and Master's Degrees in Computer Information Systems. Steve managed key government programs in North America covering card management systems, design, personalization, and production.

Steve has served as account advisor and manager to California, New Hampshire, Colorado, Idaho, Maryland, Quebec, and others for similar programs. He has been engaged with the West Virginia program over the past few years. Steve has also led the US e-Passport initiative, the Transportation Workers Identification Credential (TWIC) program for the Transportation Security Administration (TSA), and the General Services Administration's Managed Service Offering for the Homeland Security Presidential Directive – 12 (HSPD-12) for the Personal Identification Verifier (PIV) program for the US Government.

Tony Wallette – Project Manager

Mr. Wallette is a Project Manager with over 10 years of experience managing technical projects, both internal and external. He is PMP certified with a Master's degree in Computer Information System and over 18 years of experience in state government. He has worked as a Project Manager for five different state Driver's License programs with a proven track record of customer service. He has also worked with West Virginia on a proposed DL/ID solution and is familiar with their current system.

Dale Brown – Account Executive

Mr. Brown has recently joined Gemalto and brings 30+ years of experience in the area of product management and sales with 15+years in the government market, i.e., law enforcement and DMVs. His formal education includes a Bachelor's Degree in Business with a concentration in Marketing. Dale's most recent assignment has been working with DMVs in the area of maintaining and building relationships in the DMV community and fulfilling data needs to the insurance market. Dale ensured that his prior organization was in compliance with all DMV regulations and requirements involving the use of DMV data for the insurance market.

Dale is an Associate Member in good standing with the American Association of Motor Vehicle Administrators and currently serves as Vice Chair for the Industry Advisory Board for the DMVs.

John Cox – IT/Security Lead

Mr. Cox is a Senior Systems Engineer professional with 20+ years of experience in the Systems / IT field with the ability to successfully manage a wide range of projects simultaneously, effectively utilizing time, personnel, and resources in both independent and team environments. John has been responsible for the deployment and architecture of the card creation system for multiple jurisdiction centers. John has served as IT Lead to New Hampshire, Maryland, Idaho and Colorado.

Rick Outland – Card Security Expert

Mr. Outland is a highly experienced professional with over 30+ years of comprehensive strategic planning and implementation skills. Mr. Outland is a recognized document security expert and is a Board Member of the Document Security Alliance (DSA), previously serving as President for 6 years. The DSA's goal is to identify methods of improving security documents and related procedures to help combat the growing acts of fraud, terrorism, illegal immigration, identity theft, and other criminal acts. Rick has served as Card Security Expert to Colorado, New Hampshire, Idaho, Quebec, Maryland, and the four Atlantic Provinces. Mr. Outland also recently led a Card Design Forum with West Virginia.

Antoine Saene – Delivery Center Manager

Mr. Saene is a Software engineer/project leader with 14 years of experience in software development. Some of his expertise includes guiding teams through all V-Cycle development phases, customer and end-user satisfaction, complete project organization, quality referent and problem-solving capabilities. Antoine has served as Delivery Center Manager to California, Idaho, Colorado, Maryland, New Hampshire and Quebec. Mr. Saene's team is overseeing and maintaining the State's current driver's license solution.

Randy Rupert – Help Desk Manager/Lead Service Technician

Mr. Rupert brings over 18 years of experience focusing on IT infrastructure management, project management, platforms and services delivery, development, account management and customer service. His formal education includes a Bachelor's degree in Computer Science, a Master's in Business Administration and PMP certification. Mr. Rupert was involved in the State of Maryland's DL implementation and central issuance. Randy was also involved in the Canadian Atlantic Provinces (Newfoundland and Labrador, Nova Scotia, New Brunswick, and Prince Edward Island) implementation, enrollment, facial recognition and central issuance. Mr. Rupert oversees the support technicians for the State of West Virginia's current operations.

Jan Boula – Testing and Verification Manager

Mr. Boula brings over 10 years of experience in system integration and validation and is experienced in Driving Licenses, ID cards, Health cards ,and eGovernment projects. He was lead validation and integration activities in key Government projects across Europe while located in Prague and was selected to lead MIDS' integration and validation team in 2015. Mr. Boula led integration and validation activities for both Idaho and Colorado's new driver's license systems.

Jindrich Sedek – Production Manager Technical Leader

Mr. Sedek brings over 11 years of experience in software development and 7 years in Government Programs. Jindrich has been a technical leader in several public sector projects involving Driver's License, IDs, passports, and Resident Permits. His formal education includes a Master's Degree in informatics from Charles University in Prague.

Mr. Sedek has served as Delivery Team Leader for Gemalto's Platform and Services department and manages a team of engineers delivering national scale projects. He has also supported our production sites with Requirement analysis, specification, solution design, development, and leadership of consolidated Driver License document production for multiple US states. Currently, he is the team leader for the Atlantic Provinces DL, ID and FRS project.

Benny Dean Adams – ICW Technical Leader
Mr. Adams brings over 6 years of experience in development and strong technical skills. Some of his expertise is in database implementation and Web Application development. Mr. Adams formal education includes a Bachelor's of Science in Computer Science. Benny holds certifications in Microsoft Technology Associate (MTA) and Microsoft Certified Professional (MCP). Mr. Adams has supported the Idaho DL project, Digital Driver's License (DDL), and is a direct contributor for the Canadian Provinces DL project. He also developed and supported/maintained the LEOSA (Law Enforcement Officer Safety Act) project for Defense Consulting Services in support of the ARMY and U.S. AIR FORCE.

Shannon McCarty – Training Manager
Ms. Mc Carty has over twenty years of work experience in all areas of learning and development: technical writing, instructor led training, curriculum development, course development for instructor-led and e-learning projects, project management, and sales. Shannon specializes in developing training solutions in most business areas including software, leadership, financial, sales, and marketing. Shannon has worked in a variety of capacities from managing training development for large corporate ERP implementations as well as working as an individual contributor developing eLearning and instructor-led curricula and course content.

Vendor References

Provide a minimum of three (3) references for implementation of other, secure ID production systems, with at least one (1) representing State or Federal government. An implementation in another country, for an equivalent type of government installation, will be acceptable, if no U.S. Federal or State projects have been completed. At least one (1) of these references must be for a jurisdiction or solution with a volume of, at a minimum; 400,000 cards per year. These references must be for implementations of greater than three (3) years duration; and clearly demonstrate both the Vendor's stability and capability of meeting the Agency's card volumes.

VENDOR RESPONSE:

New Hampshire Department of Safety Division of Motor Vehicles

Customer:	New Hampshire Department of Safety Division of Motor Vehicles
Year:	2008
Status:	Active
Description:	Implemented a central issuance driver license program with full document scanning and verification, temporary license production at workstations, real-time upload and retrieval, and statewide web retrieval. The NH driver license includes some of the most advanced security features available today.
Contract Terms:	5 Years plus 2 1-year options (Awarded a new contract for another 5 years)
Annual Card Volumes:	325,000
Solution Components:	We delivered the following: • Photo and Signature Capture • Document Scanning and Verification • Real-time Web Service uploading/downloading • Statewide Web Retrieval to authorized agencies • In-state Central issuance of DL/ID documents • Advanced card security for both permanent and temporary cards.
Software Integration:	Integrated with their Mainframe system (VISION) to: • Upload photo and signature images • Provide production status information regarding DL/ID issuance
Data Conversion:	1.8 million records converted including applicant data and images converted from CICS mainframe files
Number of Users:	200-300 Total Users, 75-150 Concurrent Users
Number of Locations:	14 offices across the State
Number of Workstations:	Installation of approximately 60 workstations
DL/ID Card Offering:	Over 30 PET/PVC different card types that include traditional DL/ID card types plus ID cards for various agencies within the State
Issuance Offering:	Established a central issuance capability within the State's headquarters that is operated by State employees

Legal Name of Company or Governmental Entity	New Hampshire Department of Safety Division of Motor Vehicles
Company Mailing Address	23 Hazen Drive
Company City, State, Zip	Concord, NH 03305
Contact Person	Jeffrey A Oberdank, Supervisor, Bureau of Driver Licensing
Company Telephone Number	603-227-4203
Contact E-mail	Jeffrey.Oberdank@dos.nh.gov
Industry of Company	State Government Agency

Washington D.C. Department of Motor Vehicles

(AAMVA project)
Washington D.C. Department of Motor Vehicles
Gemalto/MIDS was contracted to replace the existing image capture and facial recognition systems and to transition to central issuance out of our Fort Wayne, IN facility.

Customer:	Washington D.C. Department of Motor Vehicles
Year:	2013
Status:	Active
Description:	Gemalto/MIDS was contracted to transition to central issuance and replace the existing image capture and facial recognition systems. By providing some of the most advanced security features within this card, we made it one of the most secure credentials of any AAMVA jurisdiction.
Contract Terms:	1 Year plus 6 1-year options
Annual Card Volumes:	160,000
Solution Components:	We delivered the following: • Photo and Signature Capture • Web-based Card Production System • Web-based Web Reporting System • Real-time Web Service uploading/downloading • 1-to-1 Facial Recognition Matching • 1-to-Many Facial Recognition Matching • Statewide Web Retrieval to authorized agencies • Central issuance of DL/ID documents • Disaster/Recovery in Fort Wayne, IN
Software Integration:	Integrated with the District's mainframe system (DESTINY) to: • Allow our Capture Workstation to pull the Applicant's demographic information and unique identifier information using web services • Allow easy access to photo, signature, and the full image of front and back of the card that is stored in our Central Image Server • Integrated with District's Business Objects server farm to provide to production status report information
Number of Users:	100-150 Total Users, 50-100 Concurrent Users
Number of Locations:	6 offices across the District
Number of Workstations:	Installation of approximately 80 workstations
DL/ID Card Offering:	15 different DL/ID polycarbonate card types
Issuance Offering:	Centrally issue credentials from our Fort Wayne, IN location

Legal Name of Company or Governmental Entity	Washington DC - Department of Motor Vehicles
Company Mailing Address	95 M Street, SW, Suite 304-5
Company City, State, Zip	Washington DC 20024-6322
Contact Person	Amit Vora, CIO, Washington D.C. Department of Motor Vehicles
Company Telephone Number	(202) 729-7110
Company Fax Number	(202) 729-7150
Contact E-mail	amit.vora@dc.gov
Industry of Company	State Government Agency

West Virginia Department of Motor Vehicles

Customer:	West Virginia Department of Motor Vehicles
Year:	2011-renewed January 2016
Status:	Active
Description:	MIDS was contracted to replace the existing image capture and facial recognition systems. Additionally, each Customer Service Representative (CSR) workstation was equipped with a "photo-first" camera and document scanning/authentication equipment. The system is instrumental to West Virginia's REAL ID approval. We centrally issue the credentials from our central issuance facility as well as providing an over-the-counter solution those wishing to not have a Real ID compliant card.
Contract Terms:	3 Years plus 2 1-year options
Annual Card Volumes:	500,000+
Solution Components:	We delivered the following: • Photo and Signature Capture • Document Scanning and Authentication • Web-based Card Production System • Web-based Web Reporting System • Real-time Web Service uploading/downloading • 1-to-Many Facial Recognition Matching • Statewide Web Retrieval to authorized agencies • Central issuance of DL/ID documents • Disaster/Recovery in Fort Wayne, IN
Software Integration:	Integrated with their Mainframe system via 3270 print stream to receive applicant demographic data, and via DB2 to update Mainframe
Data Conversion:	2.4 million records converted including full conversion of facial recognition photos
Number of Users:	350-400 Total Users, 150-200 Concurrent Users
Number of Locations:	23 offices across the State
Number of Workstations:	Installation of approximately 170 workstations
DL/ID Card Offering:	Over 50 different PET/PVC card types that include traditional DL/ID card types plus ID cards for various agencies within the State
Issuance Offering:	Centrally issue credentials from our Fort Wayne, IN location

Legal Name of Company or Governmental Entity	West Virginia Department of Motor Vehicles
Company Mailing Address	*5707 MacCorkle Ave*
Company City, State, Zip	*Charleston, WV 25317*
Contact Person	*Mr. Mark Holmes*
Company Telephone Number	*304-926-3818*
Contact E-mail	*Mark.A.Holmes@wv.gov*
Industry of Company	State Government Agency

Wyoming Department of Transportation

Customer:	Wyoming Department of Transportation
Year:	2010
Status:	Active
Description:	MIDS was contracted to replace the existing Image Capture and Central Issuance Production systems. Additionally, each Customer Service Representative (CSR) workstation was equipped with a "photo-first" camera and document scanning equipment. The system is instrumental to Wyoming's REAL ID approval.
Contract Terms:	5 years contract + 5 year extensions
Annual Card Volumes:	160,000+
Solution Components:	We delivered the following: • Photo and Signature Capture • "Photo First" process • Document Scanning • Web-based Web Reporting System • Real-time Web Service uploading/downloading • 1-to-1 Facial Recognition Matching • Statewide Web Retrieval to authorized agencies • Central issuance of DL/ID documents • Disaster/Recovery in Fort Wayne, IN
Software Integration:	Integrated with their Mainframe system to receive applicant demographic data
Data Conversion:	1.2 million records converted
Number of Users:	200-250 Total Users, 100-150 Concurrent Users
Number of Workstations:	Installation of approximately 75 workstations
DL/ID Card Offering:	12 PET/PVC card types
Issuance Offering:	Centrally issue credentials from our Fort Wayne, IN location

Legal Name of Company or Governmental Entity	Wyoming Department of Transportation
Company Mailing Address	5300 Bishop Blvd.
Company City, State, Zip	Cheyenne, WYO 82009
Contact Person	Debbie Trojovski, Assistant Driver License Administrator
Company Telephone Number	307-777-4866
Company Fax Number	
Contact E-mail	Debbie.trojovski@wyo.gov
Industry of Company	State Government Agency

CENTRAL ISSUANCE

Section 4, Subsection 4.1 - REAL ID Compliance Objectives

Section 4, Subsection 4.1.1 - Vendor should describe what specifications they would propose to address the REAL ID Act of 2005 standards, and how their solution will meet the initial "Photo First" requirements providing compliance with those standards. The Agency is requesting an in-depth description of how this can be handled in "real time", which should consist of a detailed system diagram illustrating server (physical/virtual) locations and on- site equipment at each Agency location.

VENDOR RESPONSE:

Gemalto MIDS has been working in partnership with the State of West Virginia to maintain the existing solution that already provides "Photo First" and Real ID Act 2005 compliance since the state adopted the standards after passing legislation in 2011. Gemalto has an in depth knowledge and experience with the business processes for processing DL/ID applicants throughout the state and is proud to offer its new Capture Suite Solution that will continue to preserve the integrity and security of the applicant DL/ID processing process, as well as improving operational efficiency by offering off-line operation.

Gemalto Capture Suite is a fully integrated workflow and content automation application that can be configured to operate in different modes (e.g. Photo-First, Image Capture Workstation, Scanning Workstation). This allows the state to logically separate the tasks in the workflow process of DL/ID applicant processing into functional steps so that the information and content moves from one operator to another for action according to a set of rules.

The Gemalto Capture Suite (GCS) provides the state with a powerful level of automation to route applicants to the right operator in the best, most intuitive, efficient way to ensure quicker and more efficient applicant processing. Which will undoubtedly improve the customer experience and satisfaction for state citizens when processing their DL/ID applications.

In order to maintain the efficiency and minimize any disruption to the existing business process of DL/ID applicant processing at the state DMV locations we propose to configure GCS in three configurations and propose three business process scenarios (During the workshops the state may choose configurations it deems the most effective).

Scenario 1 – Matching the Current Business Process

At present applicants at DMV locations first approach a Customer Service Representative (CSR) window, at this point they are received and provided a queue ticket to await for the service they require. The existing CSR workstations and peripherals will be reused as the state has not requested for replacement.

GCS Photo-First Configuration

GCS Photo-First will be configured and installed on the existing CSR workstations to reuse the existing web camera, barcode scanner and Panasonic ADF (Automated Document Feeder) Document Scanner.

GCS Photo-First will use the web cam to capture the applicant's photo and store this for reference to ensure that an identity verification process is launched prior to beginning the DL/ID application process.

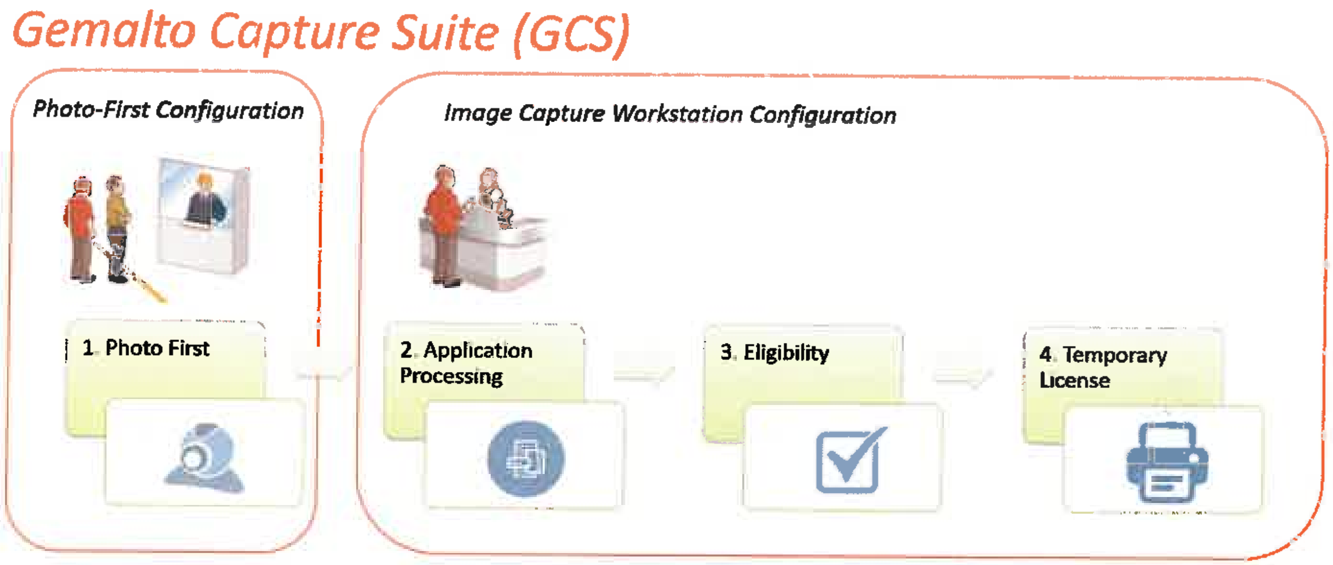

Gemalto Capture Suite (GCS)
Photo-First Configuration
Image Capture Workstation Configuration
1. Photo First
2. Application Processing
3. Eligibility
4. Temporary License

FIGURE 1 -SCENARIO 1 – MATCHING THE CURRENT PROCESS

Photo-First Applicant Data Profile

- Apart from the web cam photo, additional data can be collected as part of the identity vetting process. We are already familiar with interfacing to the State mainframe and can request driver license person demographics to be retrieved to display to the CSR operator and be stored with the profile.
- If required scanning of breeder documents can be performed at the CSR workstations using the existing Panasonic ADF scanner and configured to be stored with the profile.
- The existing barcode scanner can also be utilized to scan driver's licenses that have a valid AAMVA PDF417 barcode, this data can also be configured to be stored with the profile.

Once the Photo-First Applicant Data Profile is completed the profile is pushed to the next process in the workflow this can be another system (At present we also send the Photo-First data to Driver Testing Services - CDL Skills) and/or the GCS Image Capture Workstation (ICW).

In the existing process the applicant is provided a ticket number from the existing queue system and asked to wait to advance to the next part of the process.

GCS Image Capture Workstation (ICW) Configuration

The applicants queue ticket number is called and they approach the ICW, the DMV operator will be able to verify visually the person standing in front of them to be served is the same as the photo in the Photo-First Applicant Data Profile that appears on the list of applicants that have been registered at the CSR Windows within the DMV office.

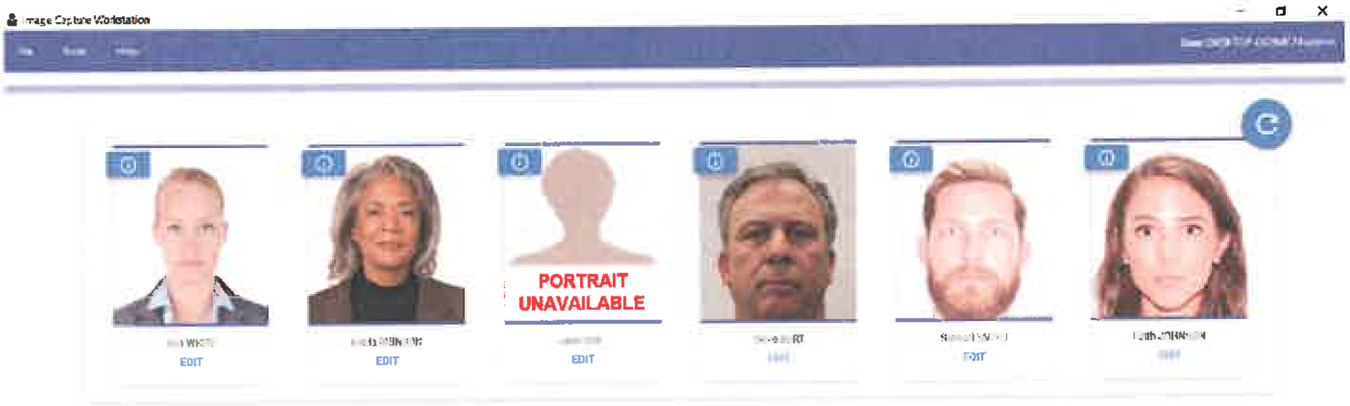


FIGURE 2: IMAGE CAPTURE WORKSTATION PHOTO-FIRST QUEUE

** Please note that the above screenshot is a sample of a previously delivered solution and the final user interface design will be specified during project specification workshops.*

Each of the ICW will be configured with the following hardware peripherals (Full configuration details are elaborated on in our response to RFP Section 4, Subsection 4.8.3):

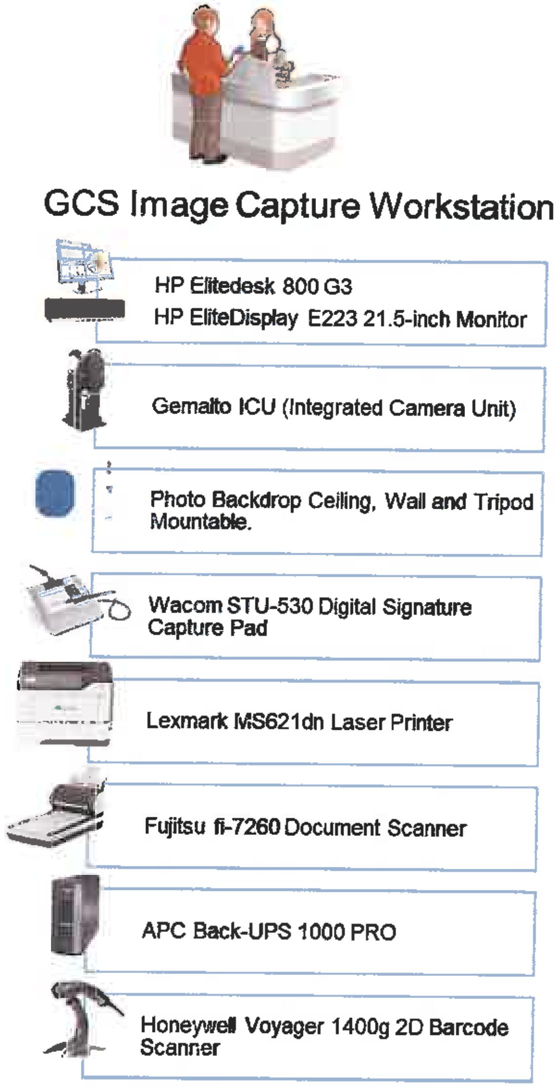

GCS Image Capture Workstation
HP Elitedesk 800 G3
HP EliteDisplay E223 21.5-inch Monitor
Gemalto ICU (Integrated Camera Unit)
Photo Backdrop Ceiling, Wall and Tripod Mountable.
Wacom STU-530 Digital Signature Capture Pad
Lexmark MS621dn Laser Printer
Fujitsu fi-7260 Document Scanner
APC Back-UPS 1000 PRO
Honeywell Voyager 1400g 2D Barcode Scanner

FIGURE 3: ICW WORKSTATION & PERIPHERALS

Notes on functional use of devices:

- Gemalto ICU (Integrated Camera Unit – includes a high definition DSLR camera for ICAO quality portrait photos)
- Signature Pad (Offering both signature and questionnaire user interface)
- Laser Printer (For Temporary Driver's License)
- Scanner with dual functionality (Automated Document Feeder and Flatbed) for passports, DL/ID
- Barcode Scanner for PDF417 AAMVA complaint licenses data capture

The ICW will facilitate the DMV operator with managing the next workflow step for capturing the applicant's portrait photo to be used to personalize their DL/ID card. ICAO and 1:1 Facial Recognition is performed to ensure quality and real-time identity verification with the historical photo for that specific driver record.

The signature pad will display any questionnaire provided by the state (such as Voter Registration) and capture the applicant's signature according to AAMVA standards as it will also be printed on the credential.

A scanner with both Automated Document Feeder (AFD) and Flatbed is provided in the event that the applicant has a document that is delicate (old birth certificates or not suitable for ADF such as thick paged passports, and could not be scanned at the CSR Workstation (ADF Only).

Once the state mainframe (responsible for the primary driver record) acknowledges that the applicant's status and availability to receive a credential is authorized, a temporary DL/ID is then printed from the Laser printer and handed to the applicant.

Scenario 2 – Image Capture Workstation Only

It is possible that the state may wish to redesign the flow of applications in their office to allow DL/ID applicants to go directly to an ICW without visiting a CSR Window. This configuration is also possible and the captured photo will be sent as part of a Photo-First Applicant Data Profile to other systems such as the Driver Testing Services - CDL Skills.

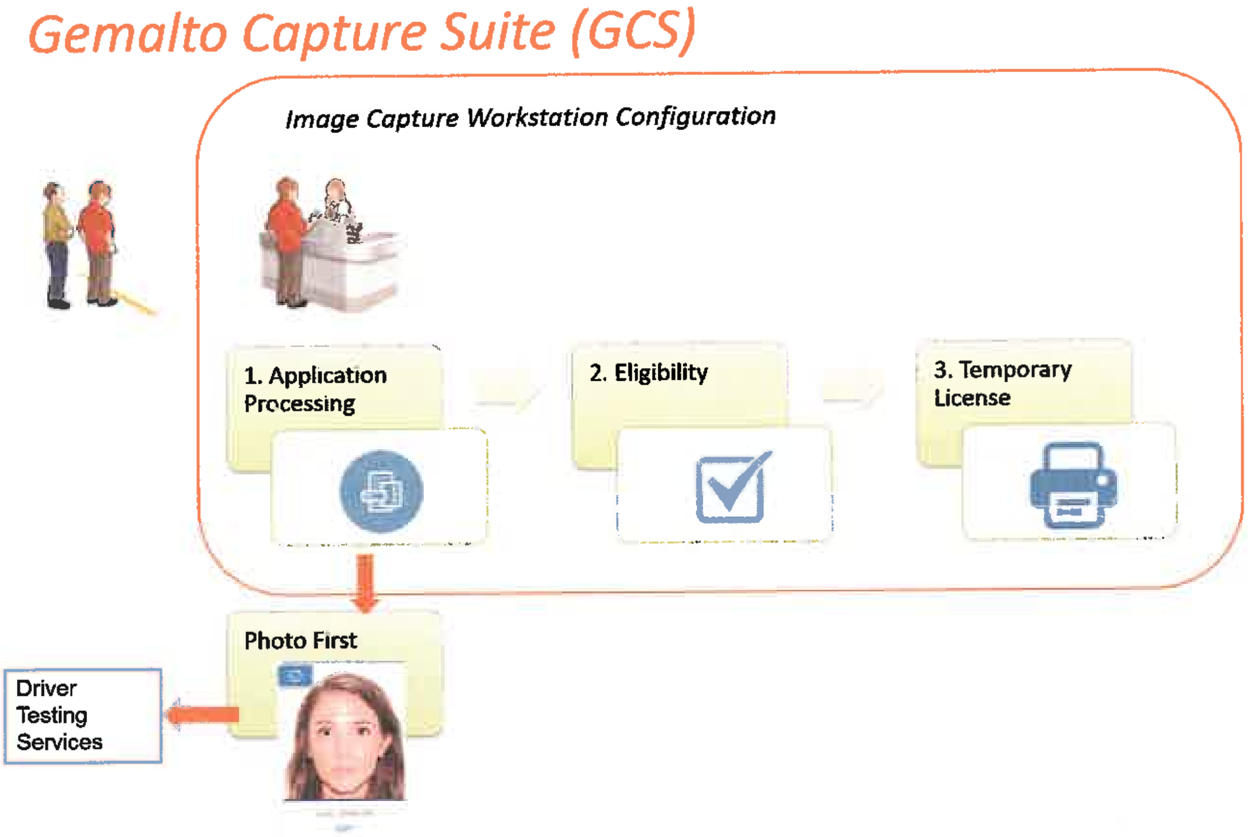

Gemalto Capture Suite (GCS)
Image Capture Workstation Configuration
1. Application Processing
2. Eligibility
3. Temporary License
Photo First
Driver Testing Services

FIGURE 4: SCENARIO 2 – IMAGE CAPTURE WORKSTATION ONLY

Scenario 3 – Over the Counter Issuance for Exceptions

As per the state's request in Addendum No.4 of the RFP, one location in Kanawha DMV Headquarters building will be equipped with one ICW that has the capability to perform instant issuance of DL/ID cards that are of the same standards as those of the cards personalized at the Vendors Facility.

GCS shall be configured at this location as an ICW with the capability to print instant issuance cards, we propose a Datacard CD800 Printer to perform this function.

It is possible to have this configured as an ICW fully standalone or it can be part of a request from a CSR Window at the location to process the applicant at this specific ICW machine.

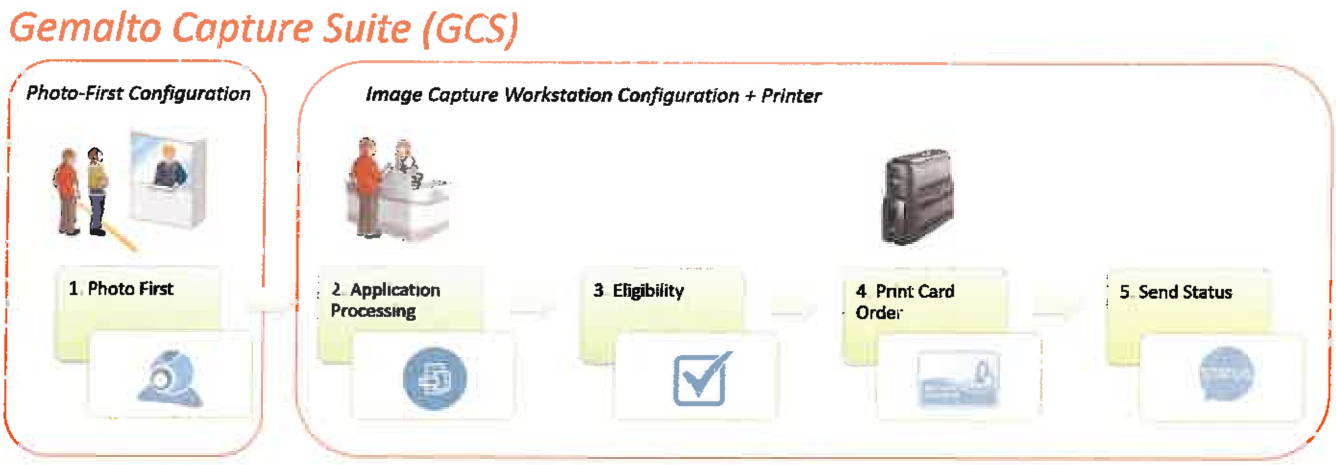

Gemalto Capture Suite (GCS)
Photo-First Configuration
Image Capture Workstation Configuration + Printer
1. Photo First
2. Application Processing
3. Eligibility
4. Print Card Order
5. Send Status

FIGURE 5: SCENARIO 3 – ICW WITH OVER THE COUNTER ISSUANCE PRINTER

Upon successful card personalization the status will be sent to the States mainframe.

In summary the Gemalto Capture Suite (GCS) offers an efficient, flexible and seamless DL/ID application workflow configuration customized to meet the state of WV's DMV business requirements for both Non-Federal and For Federal DL/ID cards. Hence allowing the state to ensure reliable compliance with the requirements and processes (e.g. Breeder Document Capture, Mandatory Facial Image Capture) associated to Real ID that establishes an effective procedure to confirm or verify a renewing applicant's information for an DL/ID.

Solution System Architecture

The diagram below presents the proposed high level logical architecture encompassing all the solution application and services components including integration of existing State systems (Mainframe, Driver Testing Services, Active Directory LDAP [Optional]) and external services gateways (State Board of Elections, Secretary of State, USPS Signed Confirmation and other government agencies). Our application architecture is modular and can integrate easily to other systems across multiple platforms (legacy Mainframe via Middleware, WebSphere, JBoss etc.) and interfaces such as Web Services, MQ Series, FTP/SFTP processes, RPC etc.

Modular, Scalable, Secure

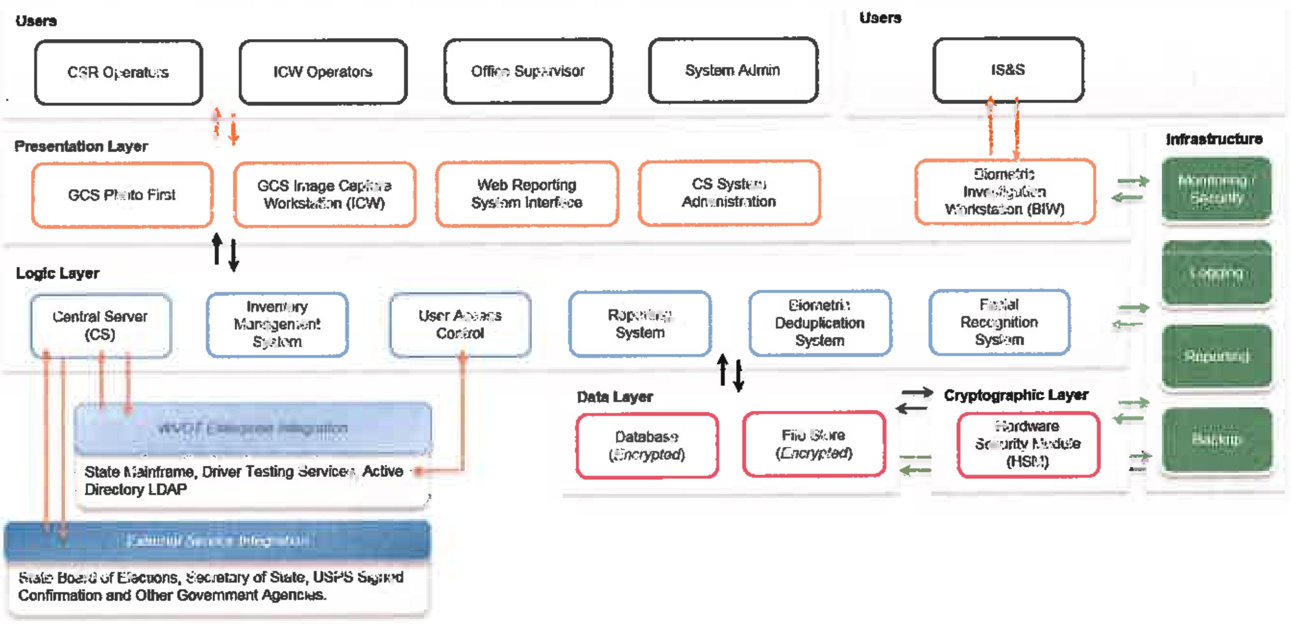

Users
CSR Operators
ICW Operators
Office Supervisor
System Admin
Users
IS&S
Presentation Layer
GCS Photo First
GCS Image Capture Workstation (ICW)
Web Reporting System Interface
CS System Administration
Biometric Investigation Workstation (BIW)
Infrastructure
Monitoring / Security
Logging
Reporting
Backup
Logic Layer
Central Server (CS)
Inventory Management System
User Access Control
Reporting System
Biometric Deduplication System
Facial Recognition System
Data Layer
Database (Encrypted)
File Store (Encrypted)
Cryptographic Layer
Hardware Security Module (HSM)
WVOT Enterprise Integration
State Mainframe, Driver Testing Services, Active Directory LDAP
External Service Integration
State Board of Elections, Secretary of State, USPS Signed Confirmation and Other Government Agencies.

FIGURE 6: HIGH LEVEL SYSTEM ARCHITECTURE

- **Users**
  We envisage that the CSR (Customer Service Representatives), ICW operator and supervisor office users, and IS&S users permitted by WVOT will be part of the WVOT Active Directory. Application permissions are Active Directory role based and configured through Central Server – however if the state wishes we can opt for an internal authentication system.

- **GCS Photo-First**
  Gemalto Capture Suite (GCS) Photo-First configuration will be installed on the existing CSR workstations to reuse the existing web camera, barcode scanner and Panasonic ADF (Automated Document Feeder) Document Scanner. This is if the state wishes to follow this approach.

- **GCS Image Capture Workstation**
  Gemalto Capture Suite (GCS) ICW configuration that will facilitate the DL/ID enrolment workflow to capture photos, ICAO Photo check, 1:1 real-time facial recognition, document scanning, conduct questionnaires, capture signature, issue a temporary license and send a card order completion status to the Central Server. For Kanawha office one ICW will be configured with the ability to print credentials (Instant Issuance).

- **Web Reporting System**
  This web based interface provides users the ability run predefined system reports based on SQL Server Reporting Services.

- **Central Server (CS) System Administration**
  Provides a web based user interface to manage the Central Server.

- **Inventory Management System**
  Enables the DMV to track and electronically order secure paper stock (Temporary Licenses), and printer toner, for each of the Agency's 27 locations

- **Biometric Investigation Workstation (BIW)**
  A suite of tools to perform biometric identity investigation and case adjudication. Ad-hoc facial recognition matching requests are also possible.

- **Central Server (CS)**
  The Gemalto Central Server is the heart of our solution, it orchestrates the workflow and management of data between systems both internal and external, manages user security and configuration amongst other functionalities.

- **User Access Control**
  This module is part of the Central Server and integrates to Active Directory to utilize domain credentials for application authentication and permissions.

- **Reporting System**
  The reporting system is built upon a Microsoft SQL Server Reporting Services data warehouse.

- **Biometric Deduplication System & Facial Recognition System**
  This module is the core component that performs the actual function of integrating to the Facial Recognition System (FRS) engine, it also manages the case management of results returned by the FRS engine and provides the Biometric Investigation Workstation (BIW) with case work.

Our key objective is to work alongside WV DMV as a trusted business partner during the project specifications phase, refining the architecture to ensure our solution exceeds all the business requirements, meeting the state's needs for today and for the future.

Solution Network Architecture

We present below the high level networking architecture between components based on the State hosting the solution at West Virginia Office of Technology (WVOT) and using the Gemalto Capture Suite configured to operate with the current process (Scenario 1 - Photo-First at CSR and ICW).

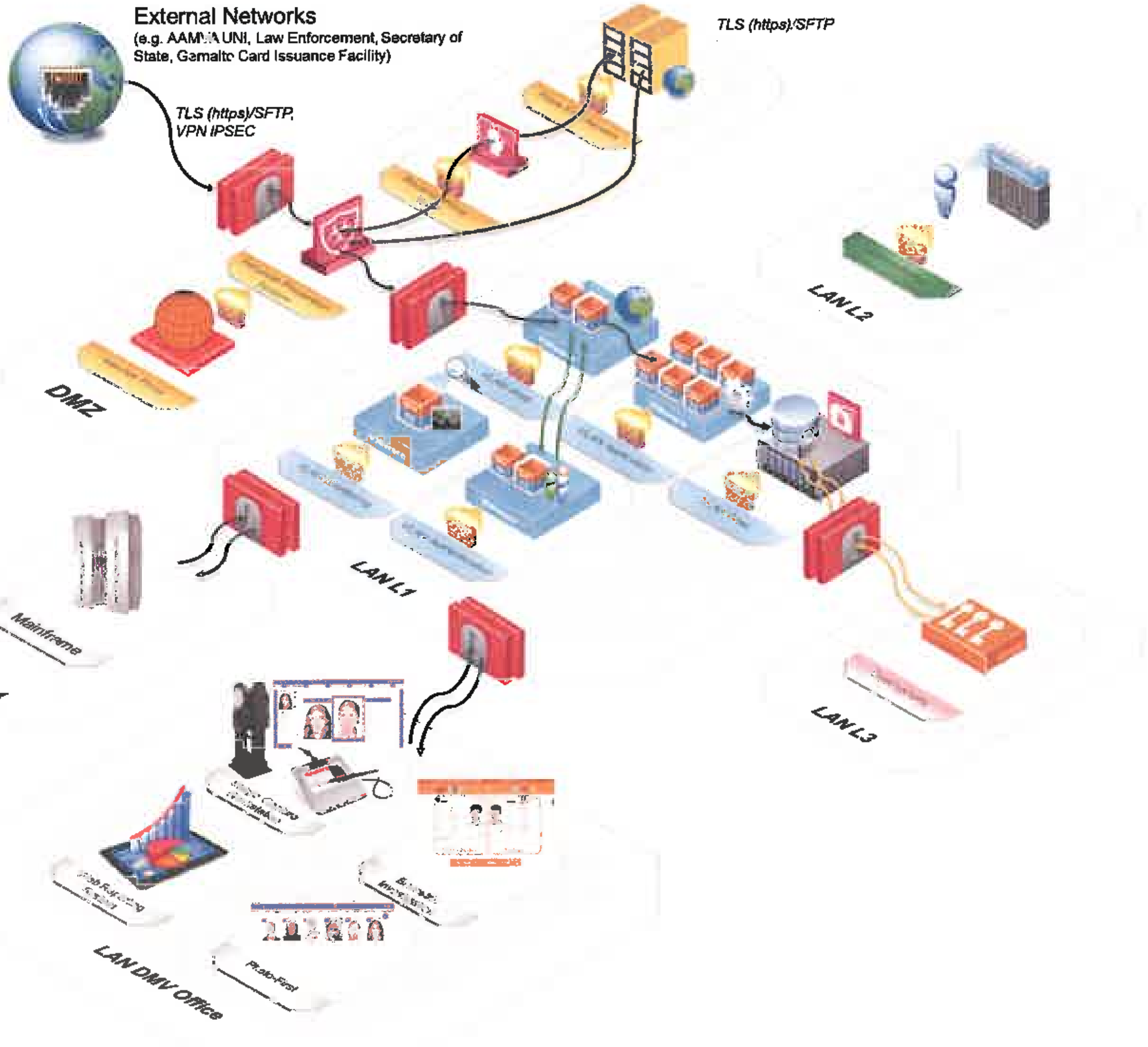

External Networks
(e.g. AAMVA UNI, Law Enforcement, Secretary of State, Gemalto Card Issuance Facility)
TLS (https)/SFTP
TLS (https)/SFTP, VPN IPSEC
DMZ
LAN L2
LAN L1
Mainframe
LAN L4
LAN L3
LAN DMV Office
Photo-First

FIGURE 7: PROPOSED HIGH LEVEL ARCHITECTURE DESIGN AT WVOT EMPLOYING DEFENSE IN DEPTH.

We propose to assist the state with IT Design Consultancy to secure the network infrastructure and Virtual Machines that host our solution in WVOT, this is elaborated on in more depth in our response to Section 4, Subsection 5.9.2.

We follow industry standards in our software design using n-tier architecture and this provides a Defense in Depth approach (A layering tactic, conceived by the National Security Agency (NSA) as a comprehensive approach to information and electronic security), because an infiltrator must pass through and compromise several firewalls to reach the back-end location of cryptographic keys and database.

At each of the DMV office locations we will install GCS Photo-First at all the existing CSR Workstations, and new equipment will be provided for all ICWs.

All our server side components will be hosted at WVOT, the only interface to our Central Issuance Facility will be through the Central Server.

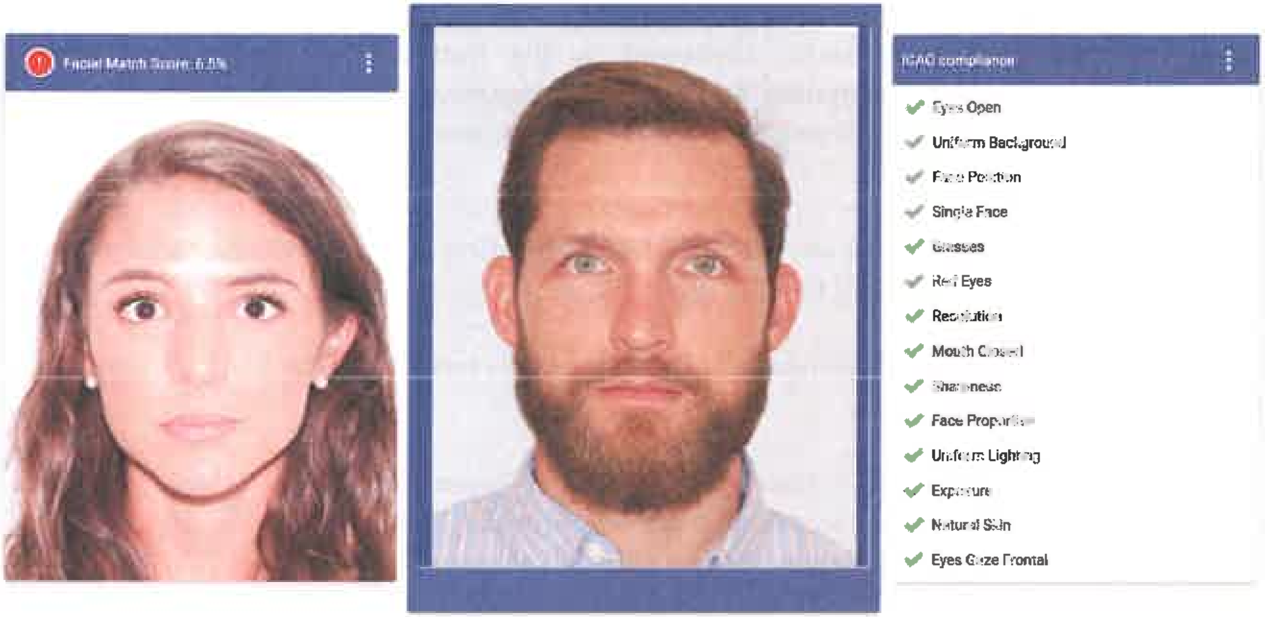
Our web based reporting system is based on SQL Server Reporting Services (SSRS) and Biometric Investigation Workstation (BIW) is accessible over web browser, hence any workstation with firewall access and user privileges and the right security credentials can have access.

Security credentials can be mapped to the existing WVOT Active Directory for user management and security. External integrations are expected through our Central Server which is based on a Service Orientated Architecture (SOA).

Section 4, Subsection 4.1.2 - Vendor should describe any available alert and notification mechanisms within their system, to "flag" image comparison and document authentication issues associated with the image captured during the "Photo First" process, in relation to the image currently on file (One-to-One, or One-to-Many, comparisons). This is intended for the purposes of reducing, or eliminating, the potential for identity fraud. This would generate a notification to the Agency's Investigation, Security and Support Services Unit ("IS&S"), identifying a potential security risk.

VENDOR RESPONSE:

Gemalto confirms that our Image Capture Workstation (ICW) provides 1:1 comparison results in real time to the user during the photo capture process. Our graphical user interface provides a visual alert to the operator if no match is found. The location of the indicator is easy for the operator to see without being overly obvious that there could be a potential issue so as to not alarm the applicant. We have provided an image below:



Facial Match Score: 6.5%

ICAO compliance

- ✓ Eyes Open
- ✓ Uniform Background
- ✓ Face Position
- ✓ Single Face
- ✓ Glasses
- ✓ Red Eyes
- ✓ Resolution
- ✓ Mouth Closed
- ✓ Sharpness
- ✓ Face Proportion
- ✓ Uniform Lighting
- ✓ Exposure
- ✓ Natural Skin
- ✓ Eyes Gaze Frontal

FIGURE 8: FACIAL RECOGNITION MATCH FAILURE

** Please note that the above screenshot is a sample of a previously delivered solution and the final user interface design will be specified during project specification workshops.*

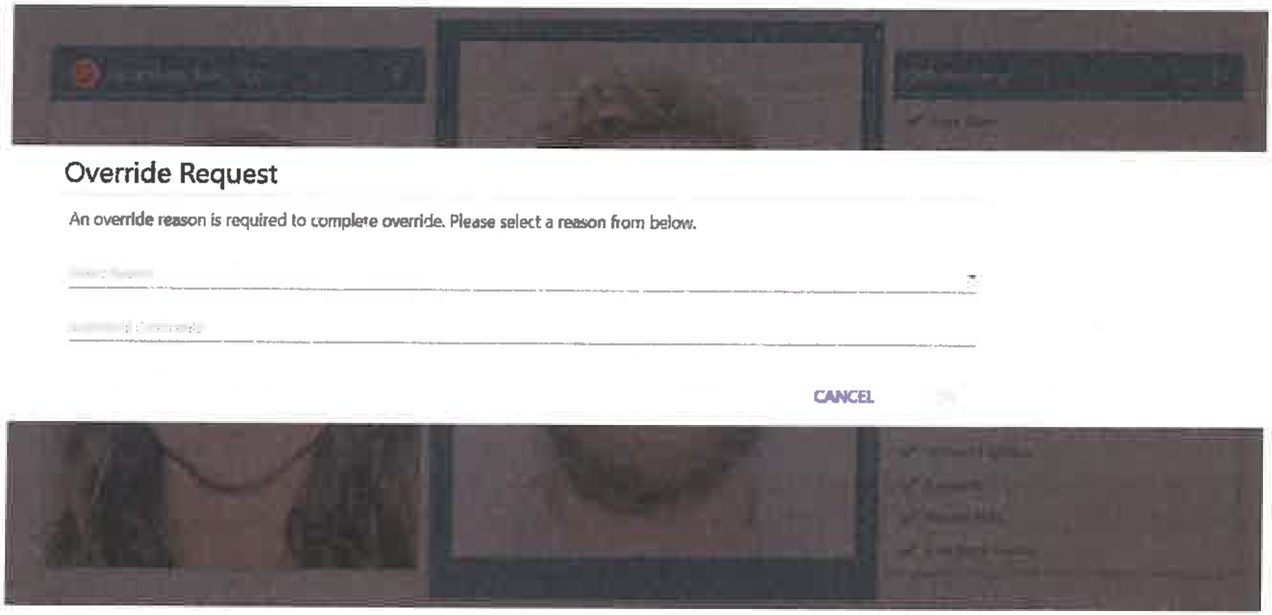
Gemalto's Facial Recognition technology is perfect for a Photo First process because it allows the 1:1 verification process to be performed in a fraction of a second and hence it poses no impact to applicant processing time.

Document Authentication is not proposed because the state has clarified that they do not want such a solution as per the reference to vendor's questions and answers below.

* Reference 1: DMV800000001, Addendum Number: 3, Driver's License and ID Cards Vendor submitted Questions and Agency Answers.

> **Question 83:** Reference: pg. 33 4.1.2 Vendor should describe any available alert and notification mechanisms within their system, to "flag" image comparison and document authentication issues associated with the image ... Is there a "document authentication" solution required as part of this RFP?
> If yes, please specify the RFP paragraph and elaborate on the requirement.
> **WV DMV Answer:** Document authentication is not a requirement of this RFP.

In some cases operators may have the permission to override the One-to-One verification check if it has failed, this event is flagged as a potential act of fraud and logged in the system. In addition a report can be generated of all suspicious overrides for management review and action. This override may then be sent to our Biometric Investigation Workstation (BIW) queue for review.



Override Request

An override reason is required to complete override. Please select a reason from below.

FIGURE 9 – ONE-TO-ONE FACIAL RECOGNITION OVERRIDE

** Please note that the above screenshot is a sample of a previously delivered solution and the final user interface design will be specified during project specification workshops.*

In the event that the DMV does not wish to utilize this verification check it can easily be disabled by configuration settings, using the simple click of a mouse and applying a policy.

When a One-To-Many comparison is run for any applicant, if a fraud is detected, the system will suspend processing of the applicant and send the case to be reviewed by an investigator. The Biometric Investigation Workstation (BIW) software facilitates the ability for users to investigate cases of fraud flagged by the system.

* Reference 2: DMV800000001, Addendum Number: 3, Driver's License and ID Cards Vendor submitted Questions and Agency Answers.

> **Question 55: Reference:** Section 4, Subsection 4.1.2 - Can you describe the interface currently being used to notify the IS&S group?
> **WV DMV Answer:** Currently, no notification is provided.

We are highly experienced in integrating with external systems across various platforms and interfaces and we propose using Web Services or SFTP to notify the Agency's Investigation, Security and Support Services Unit ("IS&S") of any fraudulent activity. In addition they can be granted access to BIW to review and manage cases.

A standard report is also already available in our reporting system that details overrides by operators, in addition all cases managed by operators is fully audited. Thus providing the state full accountability of any actions revolving around fraud.

Discover
Infer
Identify
Report
FRAUD ALERT

Section 4, Subsection 4.2 - Central Issuance Facility Objective

Section 4, Subsection 4.2.1 - Vendor should describe a secure method allowing mobile device notifications for 'FOR FEDERAL' applicants, detailing the status of their credential from application to receipt.

VENDOR RESPONSE:

Gemalto confirms that our solution supports mobile device notifications for "FOR FEDERAL" applicants, and notifications for regular applications may also be supported. For the State of West Virginia's Driver's License and Credential Issuance System, Gemalto has included status updates for each "FOR FEDERAL" card delivery. These will be delivered through SMS (text messages) and notifications can be configured to the DMV's preferences i.e. "Application Processing" or "Credential Mailed". This is a new step in the process for West Virginia that we can easily accommodate in our new platform.

To achieve this, our solution will be integrated with Twilio. Twilio is secure 3rd party SMS and voice messaging provider and is used by major companies like Lyft, Uber, Netflix, Hulu, Twitter, Yelp, Dell, Zendesk, and Intuit for SMS notification and authentications. It should be noted that a secure 3rd party is used in order to separate our secure central issuance system from direct contact with customers. This follows IT security best practices by employing "defense in depth" (A layering tactic, conceived by the National Security Agency (NSA) as a comprehensive approach to information and electronic security), because an infiltrator must pass through and compromise several firewalls to reach the back-end location of secure systems.

Please note that our system is flexible with regards to customer communications and notifications and other methods may be supported i.e. email notifications. Also, in order to provide customer SMS notifications, customer cellphone numbers must be captured. Gemalto can capture and securely store these within our Image Capture Workstation (ICW) enrollment process, or we can push/pull this data directly from DMV systems.

Section 4, Subsection 4.2.2 - Vendor should describe a method for electronic notification to the Agency which proves that the applicant has accepted delivery of the 'FOR FEDERAL' Driver's License or ID. Vendor should describe this process, including all security measures to be implemented.

VENDOR RESPONSE:

Gemalto confirms that we will notify the Agency when applicants have accepted the delivery of "FOR FEDERAL" DL or IDs. Our solution is flexible with regards to communications and notifications and we can pass this information back to the DMV through methods including secure web services, Application Programming Interfaces (API's), or even email notifications. Gemalto will work with the DMV during the planning phase of the project to clearly define delivery notification communication methods.

Please note that we are able to provide this service **free of charge** using USPS's Web Tools API for Signed Confirmation, which enables Gemalto to access and provide valuable shipping information to you at **no additional cost**. However, should USPS decide to charge a fee for this service in the future, we will work with you to investigate the best option moving forward.

Section 4, Subsection 4.2.3 - Vendor should describe the process for Agency designated personnel to inspect the central issuance facilities during the life of the contract.

VENDOR RESPONSE:

Gemalto confirms that Agency inspections are permitted within our central issuance facilities. Due to the high security nature of our central issuance facilities, the following security measures are put in place and visitors must follow the process detailed below.

-----------------------------------BEGIN Gemalto Trade Secret Information-----------------------------

Central Issuance and Manufacturing Facilities - Visitor Access

Reception desks behind security glazing are manned during daytime business hours to manage visitor access. Security officers provide 24/7 coverage, 365 days per year for our manufacturing facilities. Visitor entrance controls (both physical and procedural) are in place to ensure verification prior to granting of access to the building. A person-trap at the entrance provides a safe area enclosed between two interlocking doors, where 3rd parties are held until released by a security officer in a controlled manner.

Visitor access follows the below high level process:

- **Visitors must have been pre-registered by a Gemalto employee at least 24 hours in advance** (due to facility security certifications and audit requirements) of their visit to be allowed access, unless for an emergency or maintenance purposes. Visits to high-security areas require management approval.
- From their secure location behind security glass, the guard opens the outer door of the visitor entrance, remotely releasing the door locks.
- The visitor enters the visitor entrance area. The outer door is closed.
- The security guard checks the identity of the visitor, reviewing acceptable identification such as a Passport or ID Card.
- Non-disclosure agreements are required by default from all visitors who visit the high-security areas or handle classified information.
- The accepted visitor is given a visitor badge. Their access to the area is recorded in the access control system.
- The inner door is opened and visitor proceeds to the shared area. The door is closed. Visitors are always escorted within Gemalto's premises.
- Cellphones are not permitted within our secure production areas.

---------------------------------------END Gemalto Trade Secret Information----------------------------------

Section 4, Subsection 4.3 - Card Images

Section 4, Subsection 4.3.1 - Vendor should describe how cards printed at the secure central issuance facility will be imaged (front and back) after printing and before being attached to the card carrier. Card images should be stored as JPG files as part of the credential issuance system (CIS), and should be retrievable as part of the customer's central issuance record.

VENDOR RESPONSE:

Gemalto confirms that our central issuance solution will take images of the front and back of all personalized cards and that images will be stored and will be retrievable as part of the customers central issuance record enabling the DMV to view cards.

This can be a web services notification or SFTP through secure VPN into the WVOT secure network, we will work with the state during the specifications phase to select the most optimal solution.

We currently provide this feature to the State of Colorado for all of their issued cards. Our solution is flexible with regards to image formats and we can store card images in JPG files or any other format required by the DMV. To achieve this, we used Datacard's Quality Assurance module which not only images the front and back of cards but also reads and verifies cards for print errors. Additional information regarding our 100% automated Visual Verification process is included in **"Section 4, Subsection 4.7 - Quality Assurance (QA)".**

Section 4, Subsection 4.4 - Card Design.

VENDOR RESPONSE:

Over the past 8 years serving as the DL/ID vendor to WV, Gemalto has been able to successfully deliver on our promise to work collaboratively with your state on our unique and thorough process of designing and delivering secure documents to the citizens of West Virginia. Throughout the process, your priorities became our priorities, and our future collaboration will be no different. With your priorities at the forefront of our approach from award through mass issuance for the life of the contract, we will ensure that your citizens will receive equally secure and attractive, state-of-the-art credentials that leave them feeling proud and protected.

Overview of Card Design Forum (CDF) Process

An excellent Security Design forms a perfect balance between the layout (personalization), graphical design and security features. It combines and connects all of the elements into one solid, integrated document which cannot be separated or manipulated without leaving easily identifiable traces. A Security Design also specifies the technical solutions defining the right materials, unique processes, and product construction to be used.

If you recall, in November during the Kick Off Meeting, Mr. Outland presented a sample card design as the starting point for your Collaborative Design process. During this meeting, he presented a suggested image that showcased one of West Virginia's beautiful mountain ranges. He explained that while this was a suggestion, Gemalto wanted to capture in your card design images and icons that distinctly represent what makes West Virginia unique and what your citizens are most proud of.

During this collaboration, we discussed enhancing the DL Card with the New River Gorge Bridge while keeping the suggested mountain range image for the Identification Card so the two cards were distinctly different. In addition, varying color schemes were also discussed, and in Subsection 4.4.1 we present some of the images we would begin with during the next Collaborative Design Forum upon award.

As we stated in November, we would present these suggestions as clearly that of a suggestion and we would begin the Collaborative Design process with these images and revise them to meet the needs of your jurisdiction. These images and field layouts will be enhanced per our discussions and will not be complete until all card types are correctly represented per our discussions. We understand and appreciate your busy schedules and therefore will be prepared to present suggestions for your documents keeping both the AAMVA standards and WV code in mind while presenting the most secure and attractive credential possible.

During the CDF process, we will continue our discussion of content and location of where all AAMVA required and jurisdiction requested demographic data would be displayed on the proposed card. This information will be later presented in a Requirements Specification (RQS) that you will review and approve. As you can see, Gemalto feels it is crucial to the success of any card project that the jurisdiction is heavily involved in the design of their documents. We want you to be proud of what you collaboratively help us design for the citizens of West Virginia.

Designing the cards is just the beginning as you know. We will then go through the actual card color approval process.

Color Approval

Once approved, the final design is submitted by the studio to the selected manufacturing facility to prepare for production. Representative(s) of your jurisdiction will accompany our security experts to our factory for color approval of your documents. This is the point where you will see your cards printed on the proposed PET/PVC substrate for the first time. At least one individual from your team must have signature authority.

During this visit, the manufacturing facility will dedicate one printing line (press, collator, and laminator) to the production of the your cards. Each color on each card side will be reviewed and accepted with signature. Changes to any color(s) require time to clean the press and re-run the proof. During this time, tours of the facility and educational presentations are provided. You should prepare for one day per card per side (front and back).

Pilot Batch

The manufacturing facility will begin production of your jurisdiction's cards following final color approval. Gemalto recommends a pilot batch of 5 to 15k cards, be produced prior to full production. We have found that a pilot batch run lowers the risk of any last minute issues prior to full production. Please note that the pilot batch is included as part of the project cost (**not an additional price per card**).

Providing this pilot batch provides many advantages to your jurisdiction as well. Often the jurisdiction will elect to submit sample cards to AAMVA for compliance testing, these cards can come directly from this pilot batch. Any unexpected problems discovered during this acceptance test can be corrected prior to full production. Also, Factory Acceptance Testing (FAT) by Gemalto requires the use of pilot cards to complete. Pilot cards provide the flexibility to make any unforeseen last minute changes before the jurisdictional documents begin full production.

Final Layout Approval

Before full production of the jurisdictions cards, complete personalization testing of each of the card types should be performed. Utilizing the cards from the pilot batch, the jurisdiction will be on-site at the personalization location. During this testing, all of the jurisdiction documents will be personalized until signature approval is obtained for each. Minor changes – moving fields – can be requested during this approval process.

Full Production

Following Final Layout Approval the factory will be notified and full production will begin. With full production, the CDF concludes its initial purpose. Throughout the life of the project, however, the CDF can be reassembled to address any attacks on the cards deemed critical and apply corrective actions and redesign.

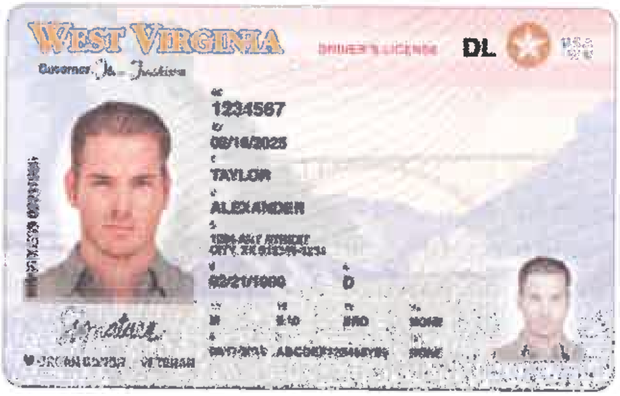
Section 4, Subsection 4.4.1 - While the specific designs for each card type will be determined during the planning phase after contract award. The Vendor should propose a solution for the FOR FEDERAL Driver's License and a FOR FEDERAL Identification Card for evaluation, based on 2016 AAMVA DL/ID Card Design Standard (http://www.aamva.org/2016CardDesignStandard/) and West Virginia Code § Chapter 17B Motor Vehicle Driver's License (http://www.legis.state.wv.us/wvcode/Code.cfm?chap=l7b&art=1)

VENDOR RESPONSE:

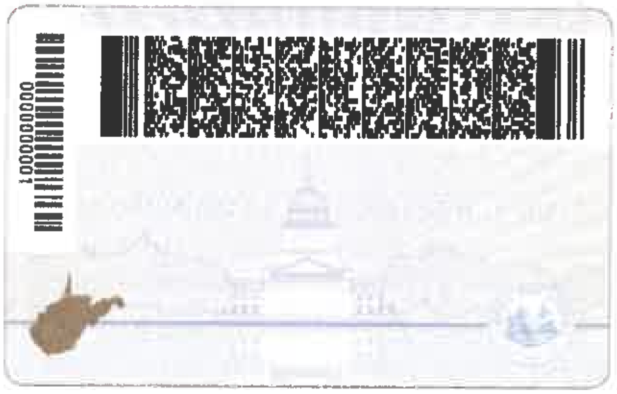
Gemalto's offerings exceed all card format and design requirements in the 2016 release of the "AAMVA DL/ID Card Design Standard; Personal Identification - AAMVA North American Standard", 2014 AAMVA "Design Principles and Guidelines for Secure DL/ID Cards", West Virginia Code § Chapter 17B Motor Vehicle Driver's License, and ISO/IEC standards for image capture, sizing, and placement.

The following samples were developed as an initial proposed design for your FOR FEDERAL Driver License and Identification Card. As stated above, these are just the initial design and they can be revised during the design workshops that will follow contract award. During these workshops, Gemalto will present their complete feature portfolio and will work with you to design placement and content of fields always assuring the card meets AAMVA requirements. Once features and presentation are selected a Requirements Specification (RQS) will be developed to document all selections. This document is a living document that will be maintained throughout the life of the contract to ensure all enhancements are well documented and agreed upon by the jurisdiction.

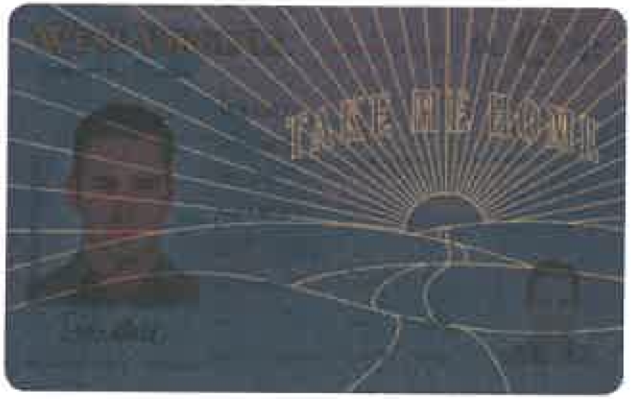
DL Front with personalization



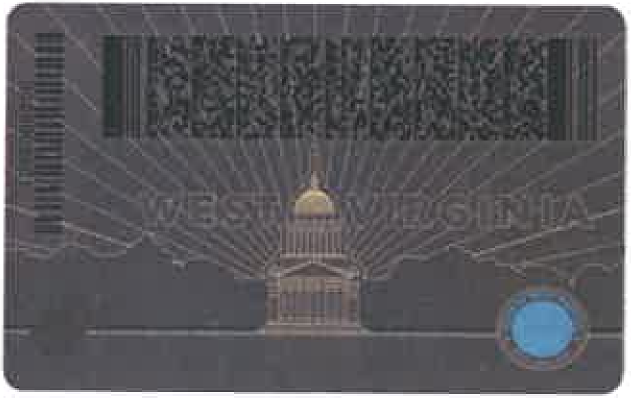
DL Reverse with personalization



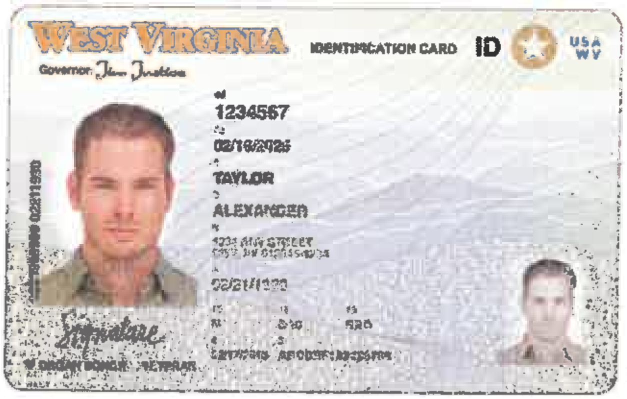
DL Front UV preview



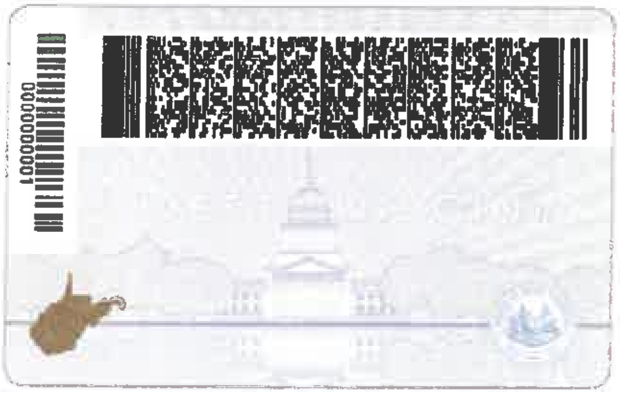
DL Reverse UV preview



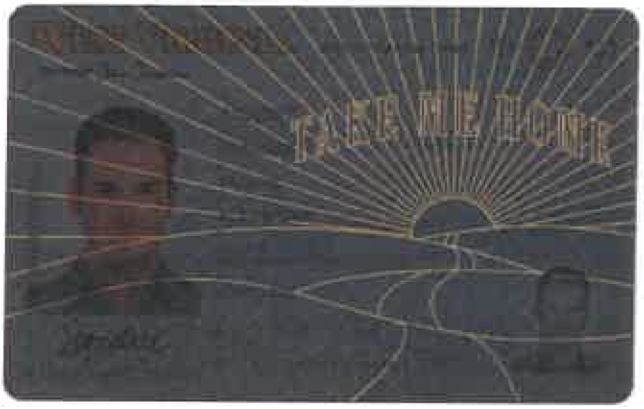
ID Front with personalization



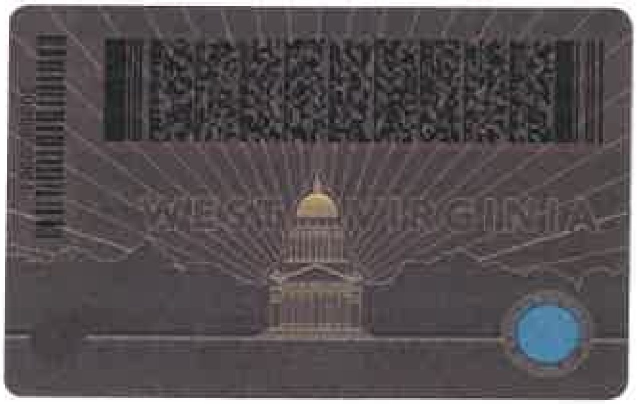
ID Reverse with personalization



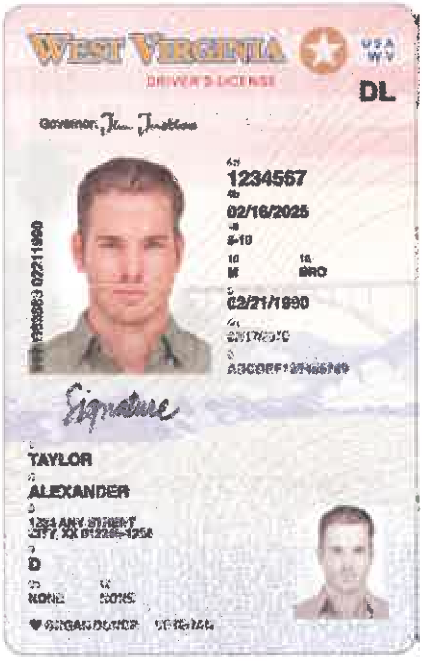
ID Front UV preview



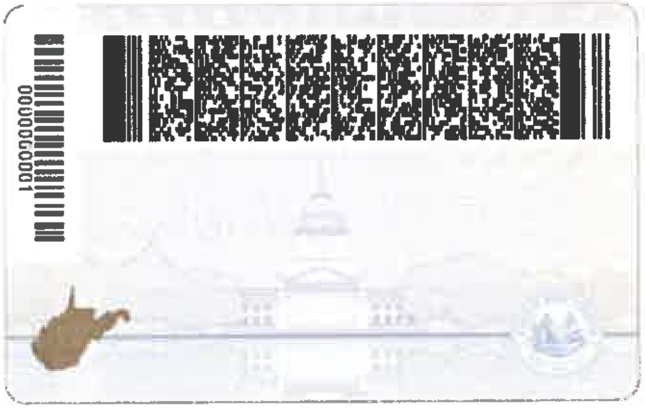
ID Reverse UV preview



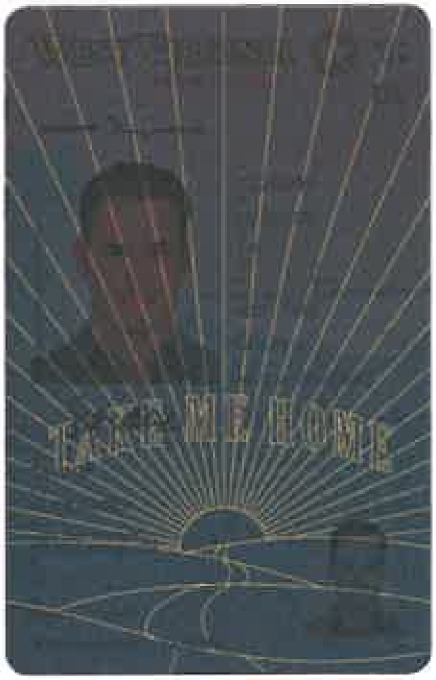
Under 21 DL Front with personalization



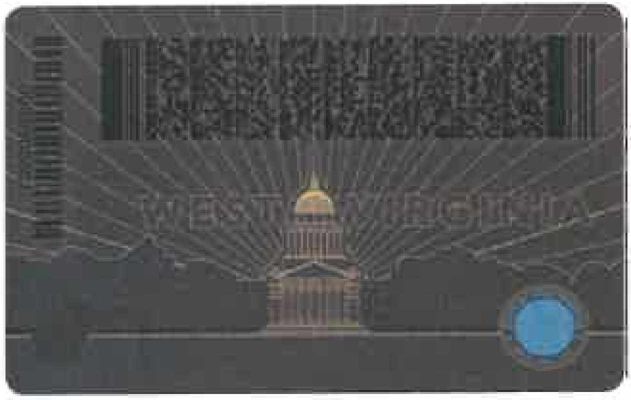
Under 21 DL Reverse with personalization



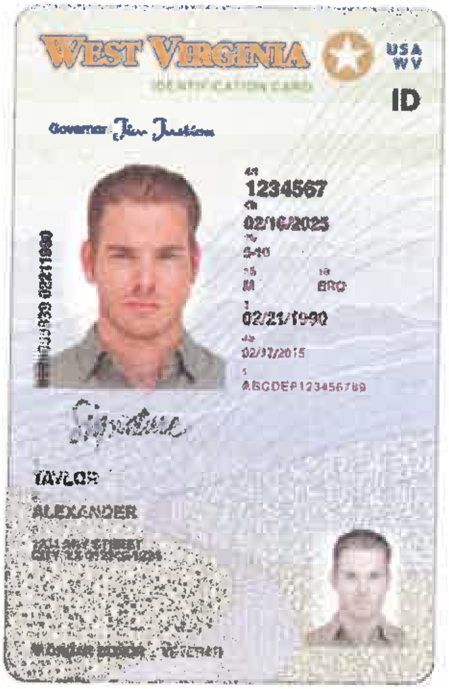
Under 21 DL Front UV preview



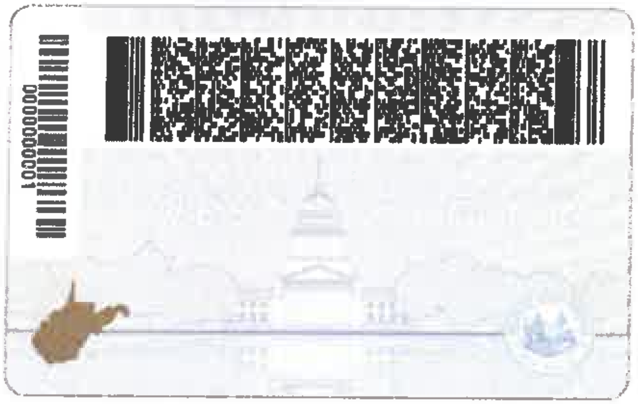
Under 21 DL Reverse UV preview



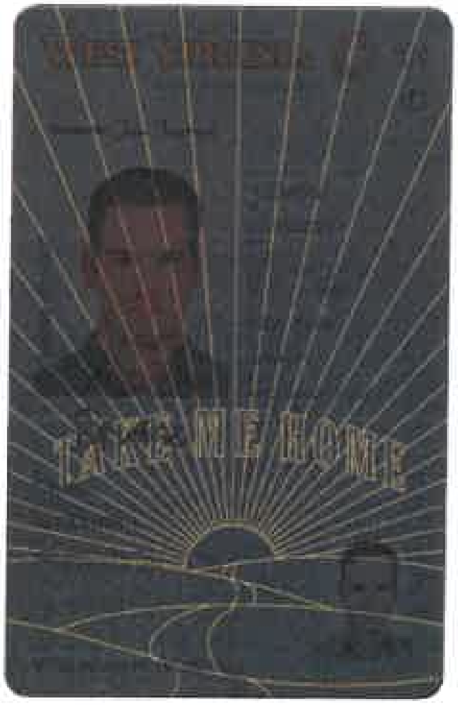
Under 21 ID Front with personalization



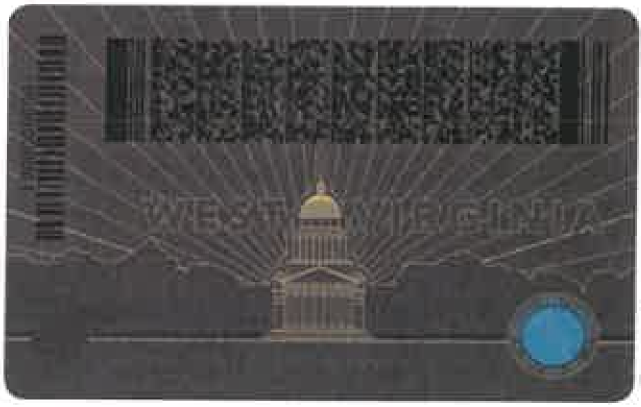
Under 21 ID Reverse with personalization



Under 21 ID Front UV preview



Under 21 ID Reverse UV preview



Section 4, Subsection 4.4.2 - Vendors card design solution should include a version number.

VENDOR RESPONSE:

Per Section D.12.5.2 of the 2016 AAMVA DL/ID Card Design Standards and as we do today, Gemalto will place a Revision Date in the reverse side of the cards in the bottom right corner. In the proposed version of these cards above, you will see the Revision Date under the seal. Each time the card body is revised this field will be updated to include the new Revision Date. Per this standard, this optional data element will be formatted in MMDDCCYY format.

Section 4, Subsection 4.5 - Card Carriers

Section 4, Subsection 4.5.1 - The Vendor should provide at least one (1) card carrier design.

VENDOR RESPONSE:

Gemalto confirms that we will provide at least one card carrier design that the credentials are mailed with as we currently do for the State. Gemalto uses Datacard's MXD (card carrier printing and affixing) and MXI (insertion) card delivery system to print card carriers and affix cards to them. Card carriers with affixed cards are then inserted into envelopes and postage is applied. The entire process is managed by Production Manager and integrated with the Inventory Management System (IMS) allowing Gemalto to easily locate a single card at any point throughout the process. The MXD and MXI units print barcodes on the card carriers to link them to the specific transaction. The barcodes (serial numbers) are then scanned on both the card and card carriers to ensure that they match and that cards are mailed to the appropriate address.

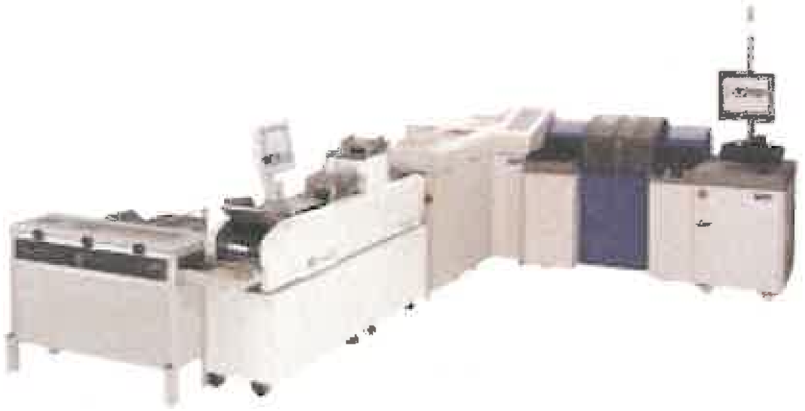


Figure 10: Datacard MXD/MXI Mailing and Insertion Equipment

Section 4, Subsection 4.5.2 - System should affix the credential to the appropriate card carrier.

VENDOR RESPONSE:

Gemalto confirms that our central issuance solution will affix the appropriate credential to the appropriate card carrier. Our solution includes an automated and redundant matching process to ensure that cards are sent to the correct citizen during our fulfillment process as we do today for the State. After cards are personalized, where cards are tracked by barcode (serial number) as the progress through the personalization equipment, they are then sent to one of our fulfillment lines for mailing. Datacard's MXD/MXI mailing and fulfillment equipment then scans the unique serial number on each card and prints the matching card carrier which also has a barcode (serial number) printed on it. Then the equipment scans the card and carrier barcodes to ensure that the correct card is applied to the correct carrier. Please note that we use windowed envelopes so the mailing address is printed on the card carrier is visible on the exterior of the envelope and used for mailing to reduce to potential for errors.

Section 4, Subsection 4.5.3 - Adhesive used to affix the card carrier should be strong enough to hold the card through the mailing process but be easily removed by the applicant.

VENDOR RESPONSE:

Gemalto confirms that the adhesive used to fix cards is strong enough to hold cards through the mailing process but may easily be removed by the applicant. The card affixing module on our Entrust Datacard MX6100 can attach 1-4 cards reliably to the form. Cards are attached using Entrust Datacard formulated double-sided, pressure-sensitive tape. The tape contains an advanced adhesive on one side to prevent tearing of the form when removing the card, and a permanent adhesive on the other side to secure the card tightly to the form. **Please note, this is the adhesive we currently use for centrally issued cards for the State of West Virginia.**

Section 4, Subsection 4.5.4 - Changes to the card earner designs should be allowed two (2) times per year.

VENDOR RESPONSE:

Gemalto confirms that the DMV will be allowed to update the wording and layout of the credential carrier up to two times annually at no additional cost. Card carrier layouts are managed within our card issuance platform, Production Manager (PM), and may be easily updated with minimal impact to the overall system. Gemalto will work the DMV during the planning phase of the project to define all card delivery requirements including card carrier layouts and submit a card carrier design to the DMV for approval. Card carrier layout updates are typically managed through the Change Request process (at no cost for the first two updates per year). The credential carrier is created and edited easily with Microsoft Word so updates can quickly and easily be made with minimal impact to the overall system.

Section 4, Subsection 4.6 - Card Durability

Section 4, Subsection 4.6.1 - Card materials should have a guaranteed life of five (5) years against breakage or significant deterioration or degradation of the data on the front and back of the card.

VENDOR RESPONSE:

West Virginia envisions delivering the most secure and durable credentials to their citizens, and we are more than prepared to deliver that to you. Your goals are our mission as we guarantee the most durable substrate for your citizens.

All Gemalto card products are tested in our internal laboratories to the required limits of standardized testing (AAMVA, ANSI/ISO). Our customers can be assured that no card product leaves our facilities until these internal tests are completed with successful results.

For West Virginia, we will submit all documents to AAMVA for standardized testing. Gemalto will provide these samples to AAMVA following Agency personalization approval utilizing the cards from the pilot batch. A pilot batch customarily consists of a first shipment of 10 thousand cards for the customer to use for personalization testing, marketing materials and external/3rd party testing. The testing results will be sent directly to your designated jurisdictional leader.

Standard acceptable test results of Gemalto PET/PVC cards in compliance with AAMVA standards, ISO/IEC 10373-1 & ISO/IEC 24798-2 & ANSI 322 would resemble the following:

Adhesion Cross-Hatch Tape	ANSI INCITS 322, Section 5.3	Pass
Card Flexure	ANSI INCITS 322, Section 5.4	Pass
Static Stress	ANSI INCITS 322, Section 5.5	Pass
Static Stress and Plasticizer Exposure	ANSI INCITS 322, Section 5.6	Pass
Impact Resistance	ANSI INCITS 322, Section 5.7	Pass
Elevated Temperature and Humidity Exposure	ANSI INCITS 322, Section 5.8	Pass
Surface Abrasion	ANSI INCITS 322, Section 5.9	Pass
Bar Code Abrasion	ANSI INCITS 322, Section 5.10	Pass
Temperature- and Humidity- Induced Dye Migration	ANSI INCITS 322, Section 5.13	Pass
Plasticizer Induced Dye Migration	ANSI INCITS 322, Section 5.14	Pass
Ultraviolet (UV) Light Exposure	ANSI INCITS 322, Section 5.15	Pass
Daylight Exposure Image Stability (7 days)	ANSI INCITS 322, Section 5.16	Pass
Laundering Test	ANSI INCITS 322, Section 5.17	Pass
Card Structural Integrity/Test Sequence	ANSI INCITS 322, Section 6.1	Pass
Card warpage	ISO/IEC 10373-1 & ISO/IEC 24798-2	Pass
Dimensions of cards 1/2 (thickness)	ISO/IEC 10373-1 & ISO/IEC 24798-2	Pass
Dimensions of cards 2/2 (height & width)	ISO/IEC 10373-1 & ISO/IEC 24798-2	Pass
Peel strength	ISO/IEC 10373-1 & ISO/IEC 24798-2	Pass

Resistance to chemicals 1/2	ISO/IEC 10373-1 & ISO/IEC 24798-2	Pass
Resistance to chemicals 2/2 (salt mist)	ISO/IEC 10373-1 & ISO/IEC 24798-2	Pass
Card stability and warpage with temperature and humidity	ISO/IEC 10373-1 & ISO/IEC 24798-2	Pass
Adhesion or blocking	ISO/IEC 10373-1 & ISO/IEC 24798-2	Pass
Bending stiffness	ISO/IEC 10373-1 & ISO/IEC 24798-2	Pass
Dynamic bending stress	ISO/IEC 10373-1 & ISO/IEC 24798-2	Pass
Dynamic torsional stress	ISO/IEC 10373-1 & ISO/IEC 24798-2	Pass
Opacity	ISO/IEC 10373-1 & ISO/IEC 24798-2	Pass
Ultraviolet light	ISO/IEC 10373-1 & ISO/IEC 24798-2	Pass
X-rays	ISO/IEC 10373-1 & ISO/IEC 24798-2	Pass
Resistance to Heat	ISO/IEC 10373-1 & ISO/IEC 24798-2	Pass
Xenon Arc Light Exposure	ISO/IEC 10373-1 & ISO/IEC 24798-2	Pass

Section 4, Subsection 4.6.2 - For any individual card not lasting the five (5) years, the Vendor's sole liability should be to provide a credit to a subsequent invoice.

VENDOR RESPONSE:

Gemalto warrants that all their PET/PVC documents will endure a minimum of five years under normal use conditions. If any document fails under normal use before the five years, Gemalto will research the cause of the failure to mitigate similar future issues. Gemalto will then accept the responsibility of providing a credit to the jurisdiction on the next invoice. A new document will be provided to replace the one that failed.

Section 4, Subsection 4.7 - Quality Assurance (QA)

Section 4, Subsection 4.7.1 - The Vendor QA process should guarantee that 100% of all cards mailed will be free from any defect in printed data or card design features, incorrect data, incorrect card type, and card materials must be free from any material defect.

VENDOR RESPONSE:

For the fulfilment and mailing of cards, we will host a turnkey Issuance Solution utilizing the Datacard MX6100 platform. The Datacard MX6100 is a modular card personalization system consisting of a Base System with optional Modules added in order to meet card personalization requirements for both desired personalization feature application as well as throughput requirements. The MX6100 can provide color printing for PET/PVC card bodies and full laser engraving for polycarbonate card bodies.

Our MX6100 printers are equipped with an automated Quality Assurance module that reads and verifies printed cards for print errors. If errors are detected by this module, they are immediately reported to our production platform which in turn immediately alerts the operator that an error has occurred. Our MX6100s have integrated cameras that will take and store pictures of every personalized card throughout the life of the contract enabling the State to physically view cards even after they have already been mailed.

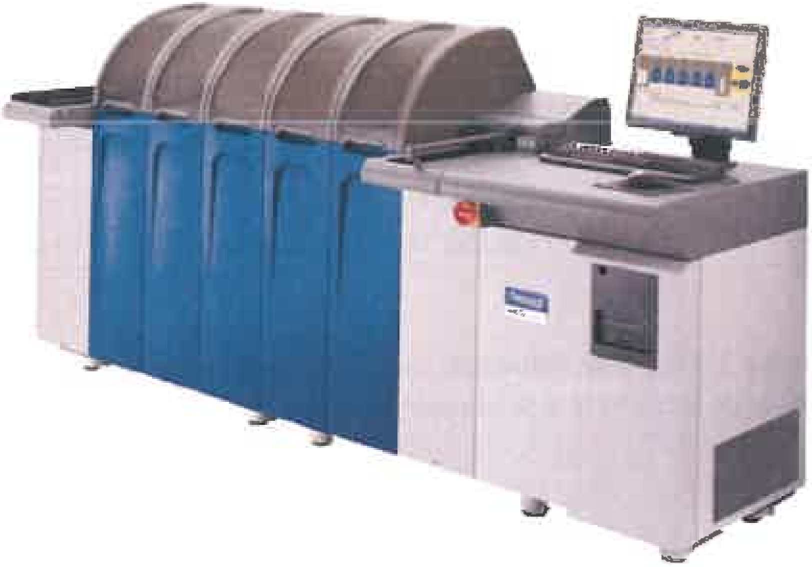


FIGURE 11 - DATACARD MX6100 CARD ISSUANCE SYSTEM

100% Visual Verification

For central issuance, the quality control process offered by Gemalto ensures **100% verification** utilizing Datacard's Vision Verification Module which performs the following types of quality checks. We can even capture and store photos of every card produced.

- ***Pattern Matching:*** The Vision Verification Module uses pattern matching to ensure that not only the photo but also the signature that was printed matches the photo and signature that were sent to the machine in the production request.
- ***Optical Character Recognition (OCR):*** The Vision Verification Module is able to extract ALL text printed on the front and back of the card and verify that it matches the data sent to the machine. In addition, the module is able to verify that the print quality is acceptable and will reject any cards with text with smudges or drips.
- ***Machine Readable Zones (MRZ):*** The Vision Verification Module is also able to read and decode all machine readable zones (i.e., PDF417 barcodes) and verify that the data matches the data sent to the machine.

It should be noted that all checks and verifications above are performed within the machine and data printed is verified against the data sent to the machine. To ensure that the data is sent to the machine is not accidentally separated or associated with the wrong card (i.e., the printed photo does not match the demographic data), Gemalto bundles all personalization data into a single .xml file when sending data to the MX6100 to ensure the data cannot be separated. In addition, the MXD/MXI inline mailing unit verifies that the correct mailer is affixed to the correct card to ensure applicants are not mailed someone else's ID.

Data Quality

Gemalto ensures data integrity by using a unique barcode per card that is assigned to a unique record ID. The record ID will be the single source of data for card personalization. When Gemalto is required to make changes to the card personalization process, we will create a 100 card test production batch containing all card types and examine 100% of the data following the changes. We currently do this for the State of West Virginia for centrally issued documents.

Section 4, Subsection 4.7.2 - The Vendor QA process should ensure that the correct image is printed on the card and that the image quality meets or exceeds ICAO standards.

VENDOR RESPONSE:

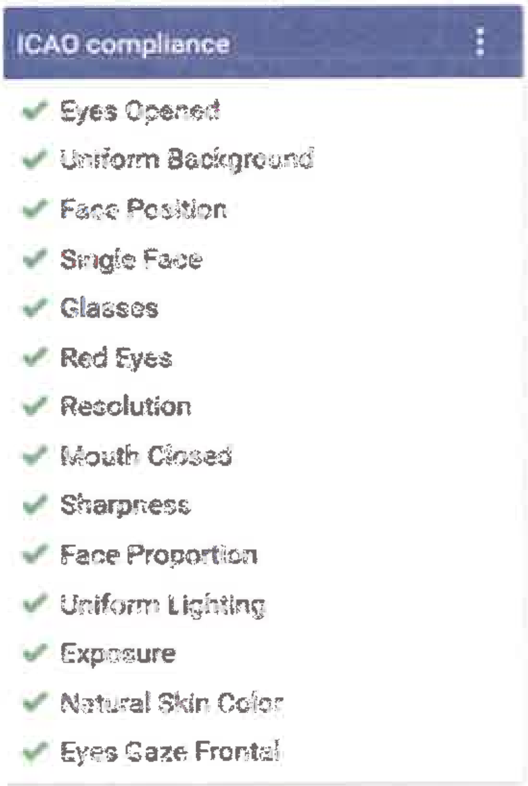
Gemalto confirms that our card personalization process ensures that the correct image is printed on the correct card and that image quality meets or exceeds ICAO standards. **As described above, the Datacard MX6100 in our central issuance facility has a Vision Verification Module that uses pattern matching to ensure that not only the photo but also the signature that was printed matches the photo and signature that were sent to the machine in the production request.** In addition, our solution wraps all card personalization data for each card production request into a single file in order to prevent the possibility of printing the wrong image on a credential.

ICAO Feedback

Gemalto's solution performs advanced evaluation algorithms on the photo image during capture **to ensure the image is acceptable for use with facial recognition systems** and meets the State's requirements. These checks are automatically performed including the ICAO checks as shown below. Visual feedback is provided to the DMV user based upon the results found. Both icons and text are displayed so the user can instantly identify any issuance and address it. Checks are performed against all ICAO standards (which are based on ISO/IEC 19794-5) and can be configured to any additional photo requirements of the DMV. ICAO checks can also be configured (turned on or off) by the DMV in our administration module. While we currently perform ICAO checks and conform to ISO requirements, we have made enhancements in the interface and usability of our solution making it easier for users to clearly see feedback.

The ICAO checks performed include (what is listed next to each check is the message that will be displayed to assist the user in correcting the photo):

- **Eyes Opened** – Ensure the applicant's eyes are opened, if possible
- **Uniform Background** – Ensure the white canvas covers the entire background area of the photo
- **Face Position** – Ensure the applicant's face is positioned correctly in the photo
- **Single Face** – Ensure no other persons are present in the photo
- **Glasses** – Ensure the applicant removes eyewear
- **Red Eyes** – Ensure camera settings are correct
- **Resolution** – Ensure the applicant is not standing too far from the camera
- **Mouth Closed** – Ensure the applicant's mouth is closed
- **Sharpness** – Ensure camera settings are correct
- **Face Proportion**
- **Uniform Lighting** – Ensure the applicant and camera are positioned correctly to allow uniform lighting
- **Exposure** – Ensure the flash settings are correct
- **Natural Skin Color** – Ensure the flash settings are correct
- **Eyes Gaze Frontal** – Ensure the applicant is looking directly at the camera



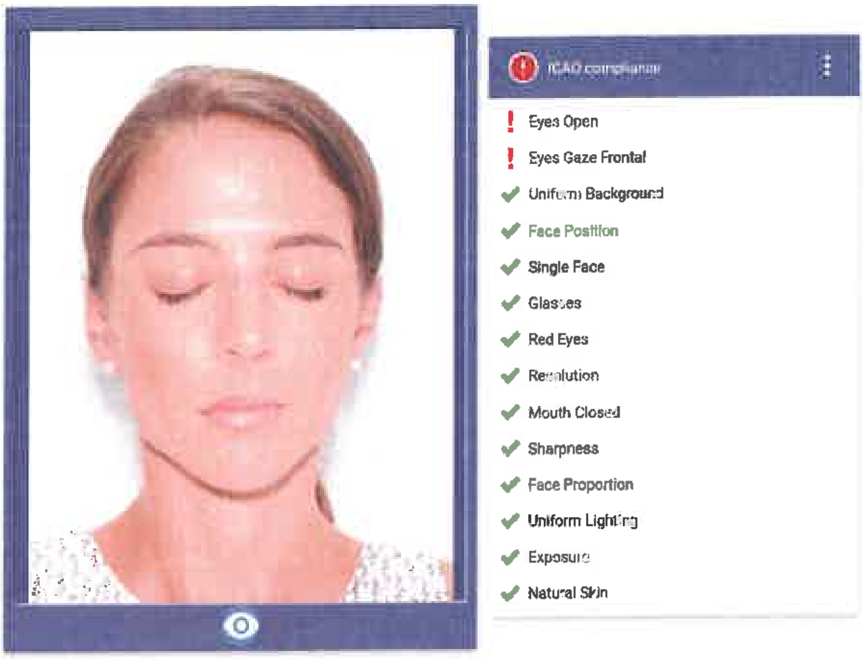
ICAO compliance

✓ Eyes Opened
✓ Uniform Background
✓ Face Position
✓ Single Face
✓ Glasses
✓ Red Eyes
✓ Resolution
✓ Mouth Closed
✓ Sharpness
✓ Face Proportion
✓ Uniform Lighting
✓ Exposure
✓ Natural Skin Color
✓ Eyes Gaze Frontal

Figure 12: ICAO Compliance Results – Sample Pass

** Please note that the above screenshot is a sample of a previously delivered solution and the final user interface design will be specified during project specification workshops.*

In the below example, the capture preview in the center fails two of the ICAO checks for eyes not being open to simulate a case of blinking (An extreme case as the Gemalto Integrated Camera Unit is calibrated to minimize flash tolerances to not stun the subject). The second check also fails as the system cannot detect the person's eyes to check that they are looking directly frontal to the camera.



ICAO compliance

- ! Eyes Open
- ! Eyes Gaze Frontal
- ✓ Uniform Background
- ✓ Face Position
- ✓ Single Face
- ✓ Glasses
- ✓ Red Eyes
- ✓ Resolution
- ✓ Mouth Closed
- ✓ Sharpness
- ✓ Face Proportion
- ✓ Uniform Lighting
- ✓ Exposure
- ✓ Natural Skin

Figure 13: ICAO Compliance Results – Sample Fail

** Please note that the above screenshot is a sample of a previously delivered solution and the final user interface design will be specified during project specification workshops.*

The Facial Match Score is used to determine if the image captured is the same as the person's photo on record using One-To-One facial recognition. The example above shows that the system gave a score of 99.1% matching of facial features which is an acceptable threshold to ascertain the identity of a person. In comparison to a human being presented with determining whether two images showed the same face that will get the answer correct only 97.53% of the time.

Section 4, Subsection 4.7.3 - The Vendor QA process should guarantee that 100% of card carrier forms produced will be of high quality with professional printing, as determined by the Agency.

VENDOR RESPONSE:

Gemalto confirms that our QA process and the Entrust Datacard MX6100 equipment will ensure that 100% of card carrier forms produced will be of high quality with professional printing. This solution also provides for 100% of the cards to be matched to the correct card carrier. The Datacard mailing system will read either magstripe, smartcard, or barcode from the card itself and also read a barcode that is printed on the card carried to ensure the proper card is attached to the proper carrier. If the data read from the card and carrier match, the system continues production without interruption. If the data read from the card and the carrier provide unexpected values from either component, the system will alert the operator to the error condition and pause production. The operator at this point will resolve the error using the processes in place for the exact issue that has occurred.

The Datacard 610 Mailer solution also provides the ability to customize the card carrier design for any given program including the ability to use variable data that is personalized on the individual card carrier forms. The Datacard 610 mailer system is very flexible and allows for the carriers to be easily modified as needed throughout the life of the program including to the text, colors and the overall design of the carrier. The system also uses an HP M806 inline printer that provides up to 55 pages per minute at 600 dpi (resolution dependent on quality of original input image). This solution is ideal for issuers running black and white one-to-one carrier forms.

Section 4, Subsection 4.7.4 - Card Carrier form should not be smudged, wrinkled, tom, or otherwise damaged during the production process.

VENDOR RESPONSE:

Gemalto confirms that 100% of card carrier forms will not be smudged, wrinkled, torn, or otherwise damaged during the production process. We will be using the same Entrust Datacard MX6100 series personalization and mailing/fulfillment equipment that is currently used to produce centrally issued cards and print card carriers for West Virginia. Entrust Datacard has been in the card production and mailing business for over 20 years. They have used that industry knowledge to create our latest mailing solution that provides unprecedented reliability in the successful production of a finished product that includes, printed cards, customized carries, specialized inserts that are not torn, smudged, or wrinkled, all inserted into envelopes that are properly sealed and ready to be delivered to the postal service.

Section 4, Subsection 4.7.5 - Envelopes for card mailing should be secure, properly sealed, and not smudged, wrinkled, tom, or otherwise damaged in the production process.

VENDOR RESPONSE:

Gemalto confirms that envelopes will be securely and properly sealed and not be smudged, wrinkled, torn, or otherwise damaged during the production process. We will be using the same Entrust Datacard MX6100 series personalization and mailing/fulfillment equipment that is currently used to produce centrally issued cards insert them into envelopes for West Virginia. Entrust Datacard has been in the card production and mailing business for 20 years. They have used that industry knowledge to create our latest mailing solution that provides unprecedented reliability in the successful production of a finished product that includes, printed cards, customized carries, specialized inserts that are not torn, smudged, or wrinkled, all inserted into envelopes that are properly sealed and ready to be delivered to the postal service.

ON-PREMISE

Section 4, Subsection 4.8 - Facility Image & Signature Capture Workstation ("ICW") Objectives

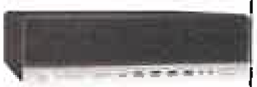
Section 4, Subsection 4.8.1 - Vendor should explain the entire process their proposed solution will use to handle new applicants. This should include how the information will be collected, both digital and physical documents, and the equipment required to produce the secure temporary DL/ID and the material used.

VENDOR RESPONSE:

Gemalto's Capture Suite (GCS) Image Capture Workstation (ICW) has been designed to easily integrate with existing government platforms and solutions based on common requirements from various jurisdictions in addition to our experience and lessons learned delivering capture solutions to our customers.

Image Capture Workstation Hardware

Gemalto confirms that we will provide all required Image Capture Workstations (ICW) and peripherals as required. All of the proposed hardware is supported by both Windows 7 and Windows 10. We have also made improvements to the proposed hardware. For example, we have upgraded the flash unit in our camera tower so that it will have a longer usable life and bulb failures will be reduced. For the State of West Virginia, we have included the following hardware:

Item #	Item Name	Description	Qty.
ICW	Image Capture Workstations	The items and quantities proposed by Gemalto to satisfy the RFP requirements.	
ICW 01	 **Workstation**	Gemalto proposes the HP Elitedesk 800 G3 with the following features: • Mouse • Keyboard • 500GB **SDD** • Intel Core i5, 8GB RAM • DVD+/-RW, Windows 7 Professional 64-bit, Integrated Intel HD Graphics	32 + spares
ICW 02	 **Monitor**	Gemalto proposes the HP EliteDisplay E223 21.5-inch Monitor the following features: • 1920 x 1080 resolution • 1000:1 static; 50000000:1 dynamic contrast ratio • 5 ms on/off • 1 HDMI (with HDCP support); 1 VGA; and 1 DisplayPort • Anti-glare • Anti - static	32 + spares

ICW 03	 **Document Scanner**	Gemalto proposes the Fujitsu fi-7260 Document Scanner the following features: • Fast, 60ppm / 120ipm scanning in color, grayscale and monochrome • 80-sheets Automatic Document Feeder (ADF) • Advanced paper handling technology for the ultimate in feeding reliability • LED light-source • Built-in flatbed (216 mm x 297 mm or 8.5 in x 11.69 in.) • Embossed card scanning • Ultrasonic multi-feed Detection sensor for security against lost images	32 + spares
ICW 04	 **Image Capture Tower**	Gemalto proposes an integrated camera tower and stand that, in addition to the required features, above, includes: • Secure camera mount and enclosure • 18 megapixel DSLR camera • Professional-grade flash • User-adjustable camera height and angle • Secure base plate	32 + spares
ICW 05	 **Photo Backdrop**	Gemalto proposes a professional photo backdrop system consisting of: • Color material – blue on one side, white on the opposite side • 35" wide x 42" tall when expanded • Internal self-expanding frame • Free-standing backdrop tripod stand, or • Mounting clips and additional mounting hardware for wall or ceiling attachment	32 + spares
ICW 06	 **Signature Pad**	Gemalto proposes the Wacom STU-530 digital signature capture pad with the following main features: • 5" diagonal screen (4.3" x 2.6") • Tethered stylus (battery-free, cordless) • USB powered (no external power required) • 5 Color LCD screen for enhanced user experience/interaction. • Sensor resolution	32 + spares

ICW 07	 **Uninterruptable Power Supply**	Gemalto proposes the APC Back-UPS 1000 pro Uninterruptible Power Supply: • 1000VA / 600W Battery Backup Uninterruptible Power Supply (UPS) • 8 Total Outlets: 4 Outlets provide UPS Battery Power Backup and Surge Protection; 4 Outlets offer Surge Protection Only • Automatic Voltage Regulation (AVR) maintains safe voltage conditions without using backup battery power	32 + spares
ICW 08	 Laser Printer	Gemalto proposes the Lexmark MS621dn with the following features: • Laser • Duplex (2-sided) Printing: Integrated Duplex • Print Speed: 50 ppm • Recommended Monthly Page Volume: 2000 - 20000 pages	32 + spares
ICW 09	 2-D Barcode Scanner	Gemalto proposes the Honeywell 1400G2D 1D/2D barcode scanner with the following main features: • 1D and 2D barcode scanner • May be operated handheld, or resting in the 'gooseneck' stand • Omni-directional scan pattern • USB cable • Gooseneck stand	32 + spares

Enterprise level software is typically robust with features and functionality but the User Experience (UX) is often overlooked making it clunky or hard to use. We try to make things fast, simple, and efficient by reducing steps and keystrokes whenever possible to help keep customer processing times to a minimum. We also try to integrate and interface as much as possible. For example, we can scan a PDF-417 barcode on the back of a document and autofill forms or fields.

Gemalto's design displays relevant applicant data on screen, enabling the users to quickly and securely process the applicant. All unnecessary keystrokes and screens are eliminated to increase user efficiency. Additionally, without user intervention, the software performs real-time ICAO compliance feedback, photo quality assessment and other important processes that aid the user in performing their duties.

Our ICW solution has been designed to be flexible in nature as it is comprised of various modules allowing us to provide a solution that perfectly matches our customers' business processes and workflows. Our ICW solution contains the following functionality however we are able to add additional features and integration during project implementation upon customer request:

- Portrait Capture
- Automated cropping, exposure adjustment, and image optimization
- ICAO compliance feedback
- Signature Capture
- Document Scanning
- Electronic customer forms, questionnaires and surveys
- 1:1 Facial Recognition Feedback
- PDF417 Barcode Reading
- Temporary License Issuance
- Over The Counter Card Issuance (For Kanawha City exceptions)

Scenario 1 – Matching the Current Business Process

At present applicants at DMV locations first approach a Customer Service Representative (CSR) window, at this point they are received and provided a queue ticket to await for the service they require. The existing CSR workstations and peripherals will be reused as the state has not requested for replacement.

CSR Windows

GCS Photo-First Configuration

GCS Photo-First will be configured and installed on the existing CSR workstations to reuse the existing web camera, barcode scanner and Panasonic ADF (Automated Document Feeder) Document Scanner.

GCS Photo-First will use the web cam to capture the applicant's photo and store this for reference to ensure that an identity verification process is launched prior to beginning the DL/ID application process.

Gemalto Capture Suite (GCS)

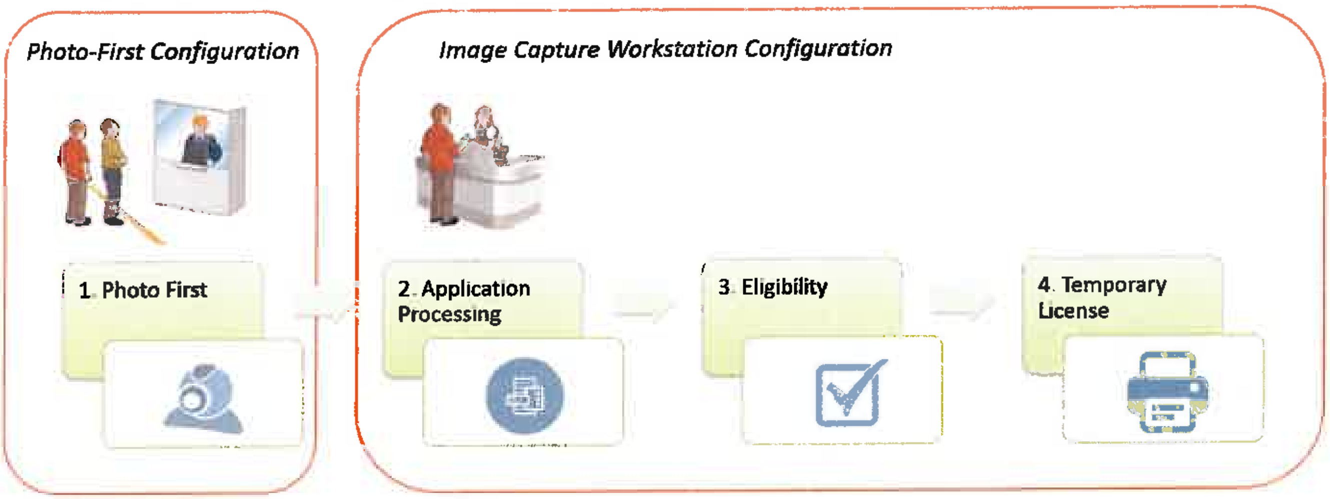


Photo-First Configuration
Image Capture Workstation Configuration
1. Photo First
2. Application Processing
3. Eligibility
4. Temporary License

FIGURE 14 -SCENARIO 1 – MATCHING THE CURRENT PROCESS

Step 1. Photo-First

The applicant arrives at the CSR window, a photo of them is taken using the existing web cam, breeder documents are scanned (As per the states answer to Vendor questions, a Document Authentication solution is not required), any driver's license with AAMVA PDF417 is scanned and the details registered.

The applicant is requested to take a ticket using the existing queue system, and wait for an ICW operator to be available.

Once the Photo-First Applicant Data Profile is completed the profile is pushed to the next process in the workflow this can be another system (at present we also send the Photo-First data to Driver Testing Services - CDL Skills) and/or the GCS Image Capture Workstation (ICW).

Watch List

One of the unique features included in our Photo First process is the "Watch List". If an applicant enters a DMV location and the operator believes the applicant to be suspect, the operator can immediately and quickly place the applicant on the Watch List. Placing an applicant on the Watch List will automatically push the photo and relevant information to all Photo First stations across the State to provide protection in the event that the applicant tries to visit other offices.

Step 2. Application Processing

The applicants queue ticket number is called and they approach the ICW, the DMV operator will be able to verify visually the person standing in front of them to be served is the same as the photo in the Photo-First Applicant Data Profile that appears on the list of applicants that have been registered at the CSR Windows within the DMV office.

The signature pad will display any questionnaire provided by the state (such as Voter Registration) and capture the applicant's signature according to AAMVA standards as it will also be printed on the credential.

A scanner with both Automated Document Feeder (AFD) and Flatbed is provided in the event that the applicant has a document that is delicate (old birth certificates or not suitable for ADF such as thick paged passports, and could not be scanned at the CSR Workstation (ADF Only).

Capturing the applicant's portrait photo to be used to personalize their DL/ID card. ICAO and 1:1 Facial Recognition is performed to ensure quality and real-time identity verification with the historical photo for that specific driver record.

A summary is presented to the DMV operator to ensure review all supporting application evidence. The operator may choose to go back or review.

Step 3. Eligibility

The state mainframe (responsible for the primary driver record) acknowledges that the applicant's status and availability to receive a credential is authorized

Step 4. Temporary License

A temporary DL/ID is then printed from the Laser printer and handed to the applicant. The Temporary License is a secure document with security features described further in.

Scenario 2 – Image Capture Workstation Only

It is possible that the state may wish to redesign the flow of applications in their office to allow DL/ID applicants to go directly to an ICW without visiting a CSR Window. This configuration is also possible and the captured photo will be sent as part of a Photo-First Applicant Data Profile to other systems such as the Driver Testing Services - CDL Skills.

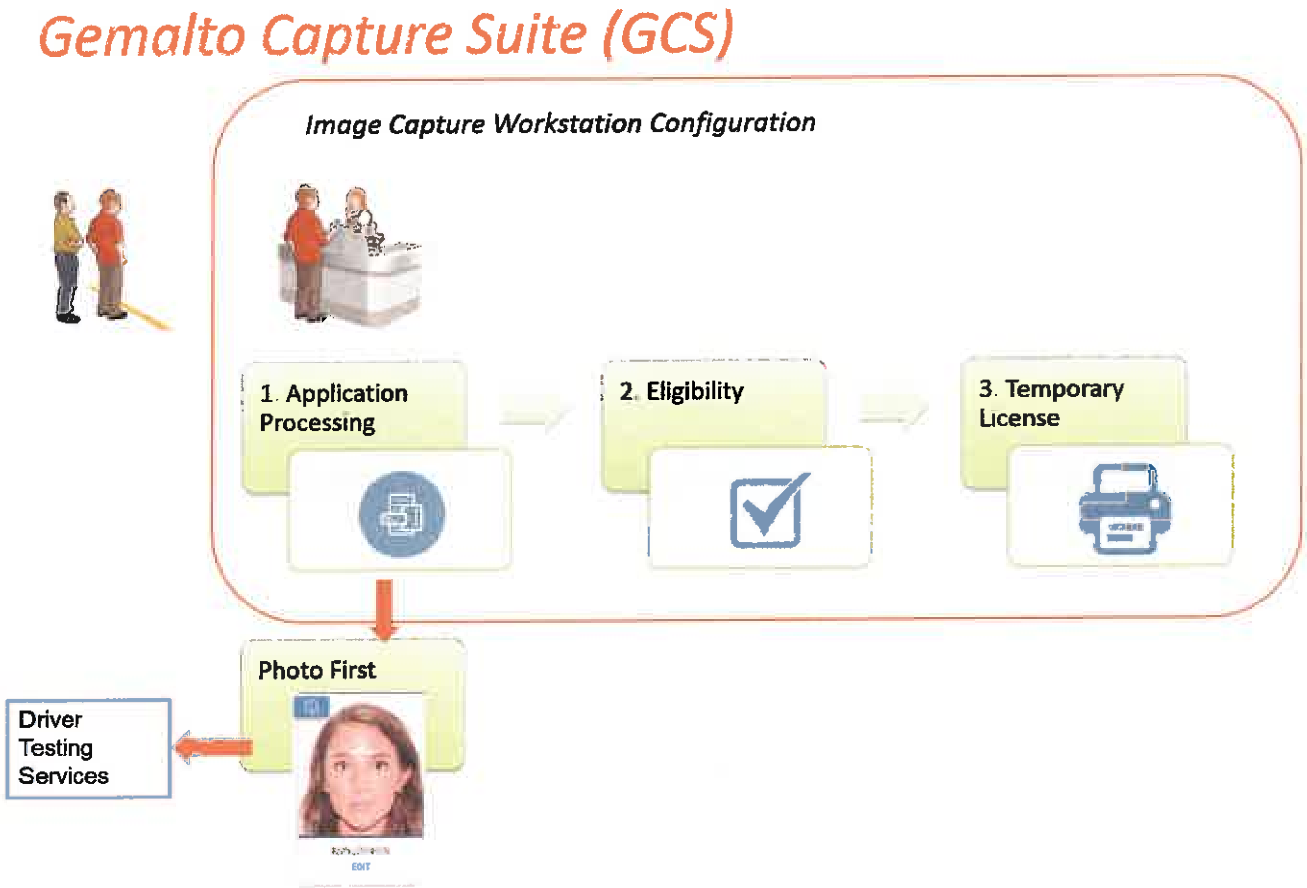

Gemalto Capture Suite (GCS)
Image Capture Workstation Configuration
1. Application Processing
2. Eligibility
3. Temporary License
Photo First
Driver Testing Services

FIGURE 15: SCENARIO 2 – IMAGE CAPTURE WORKSTATION ONLY

Scenario 3 – Over the Counter Issuance for Exceptions

As per the state's request in Addendum No.4 of the RFP, one location in Kanawha DMV Headquarters building will be equipped with one ICW that has the capability to perform instant issuance of DL/ID cards that are of the same standards as those of the cards personalized at the Vendors Facility.

It is possible to have this configured as an ICW fully standalone or it can be part of a request from a CSR Window at the location to process the applicant at this specific ICW machine.

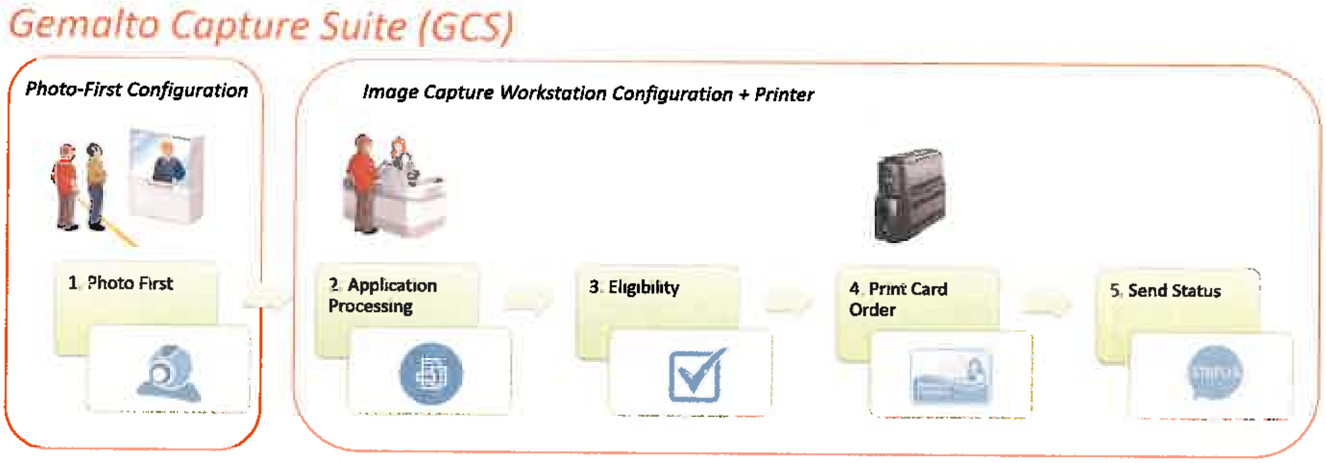

Gemalto Capture Suite (GCS)
Photo-First Configuration
Image Capture Workstation Configuration + Printer
1. Photo First
2. Application Processing
3. Eligibility
4. Print Card Order
5. Send Status

FIGURE 16: SCENARIO 3 – ICW WITH OVER THE COUNTER ISSUANCE PRINTER

Upon successful card personalization the status will be sent to the States mainframe.

GCS shall be configured at this location as an ICW with the capability to print instant issuance cards, we propose a Datacard CD800 Printer to perform this function. The CD800 is a powerful desktop solution for secure card programs.

FIGURE 17: DATACARD CD800 PRINTER

The Datacard® CD8000™ card issuance system integrates the sophisticated technologies governments, integrators, financial institutions, retailers, service bureaus and other card issuers require to produce a wide range of cards and secure IDs.

Optimized for performance. The CD8000 system outstanding efficiency. The innovative platform enables issuers to meet challenging production schedules for complex cards and jobs, while maintaining exceptional card integrity. A Microsoft® Windows® operating system interface promotes ease of use, and the system enhances productivity with secure, diagnostics and troubleshooting.

CD800 Specifications

- Print technology
  - Direct-to-card dye-sublimation/resin thermal transfer
- Print capabilities
  - One-sided (simplex) or optional two-sided (duplex) edge-to-edge printing
  - Full-color and monochrome printing capability in the same printer
  - Alphanumeric text, logos and digitized signatures; 1D/2D bar code images
  - Printer pooling/sharing (available soon)
- Print resolution
  - Standard mode: 300 x 300 dots per inch; standard text, bar code and graphics printing
  - High-quality mode: 300 x 600 dots per inch for enhanced text, bar code and graphics printing; 300 x 1200 dots per inch for enhanced text and bar code printing
  - 256 shades per color panel
- Print speed
  - Full-color: Up to 220 cards per hour, one-sided (YMCKT); up to 165 cards per hour, two-sided (YMCKT-K)
  - Monochrome: Up to 1,000 cards per hour, one-sided (Black HQ)
- Card capacity
  - Automatic feed: 100-card input for 0.030 in. (0.76 mm) cards; 25-card output standard
  - Front exception card slot
  - Separate reject location and holding tray (two-sided printer model only)
  - Input hopper empty detection

- Physical dimensions
  - One-sided printing: L 17.4 in. x W 8.8 in. x H 8.8 in. (44.2 cm x 22.4 cm x 22.4 cm)
  - Two-sided printing: L 21.2 in. x W 8.8 in. x H 8.8 in. (53.8 cm x 22.4 cm x 22.4 cm)
  - Six-compartment multi-hopper: L 27.5 in x W 16.5 in. x H 14.5 in. (69.9 cm x 41.9 cm x 36.8 cm)
- Weight
  - One-sided printing: 9.0 lbs. (4.1 kg) (depending on options)
  - Two-sided printing: 12.0 lbs. (5.4 kg) (depending on options)
  - Six-compartment multi-hopper: 33.0 lbs. (15.0 kg)
- Operating system support for printer driver
  - Windows® 7 / Windows 8 (32 and 64 bit)
  - Windows XP SP3 / Windows Server® 2003 R2 (32 bit)
  - Windows Server 2012/2008 (64 bit)
  - Microsoft Windows® Hardware Quality Labs (WHQL) certified
- Environment/energy-saving features
  - Biodegradable supply cores made with EcoPure® additive
  - Recyclable enclosure plastics (marked with recycle symbol per Resin Identification Code)
  - Recyclable packaging

Printer Business Continuity

With this factor in mind we propose to the state one CD800 for the Kanawha city office as well as one hot standby spare unit at the same office, in the event that the primary CD800 machine is not operable a seamless switchover to the standby spare can be made to ensure exception cases for instant issuance can continue to be fulfilled.

The following sections describe the features of our Gemalto Capture Suite Image Capture Workstation in more detail:

Photo First

Our Image Capture Workstation (ICW) will provide a photo first process like we currently provide to WV DMV. This is a common requirement, therefore we are providing photo first functionality to many of our current customers. This Photo First process can quickly take a photo and make it available to all other applications if needed such as knowledge testing stations so that it can be displayed on the screen at all times when the applicant is taking the test helping to prevent test substitutions.

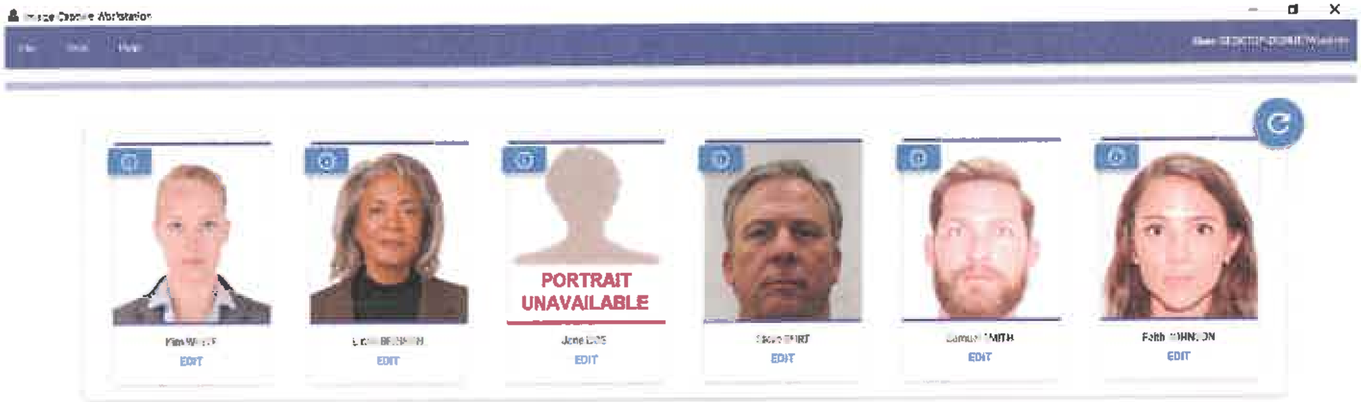
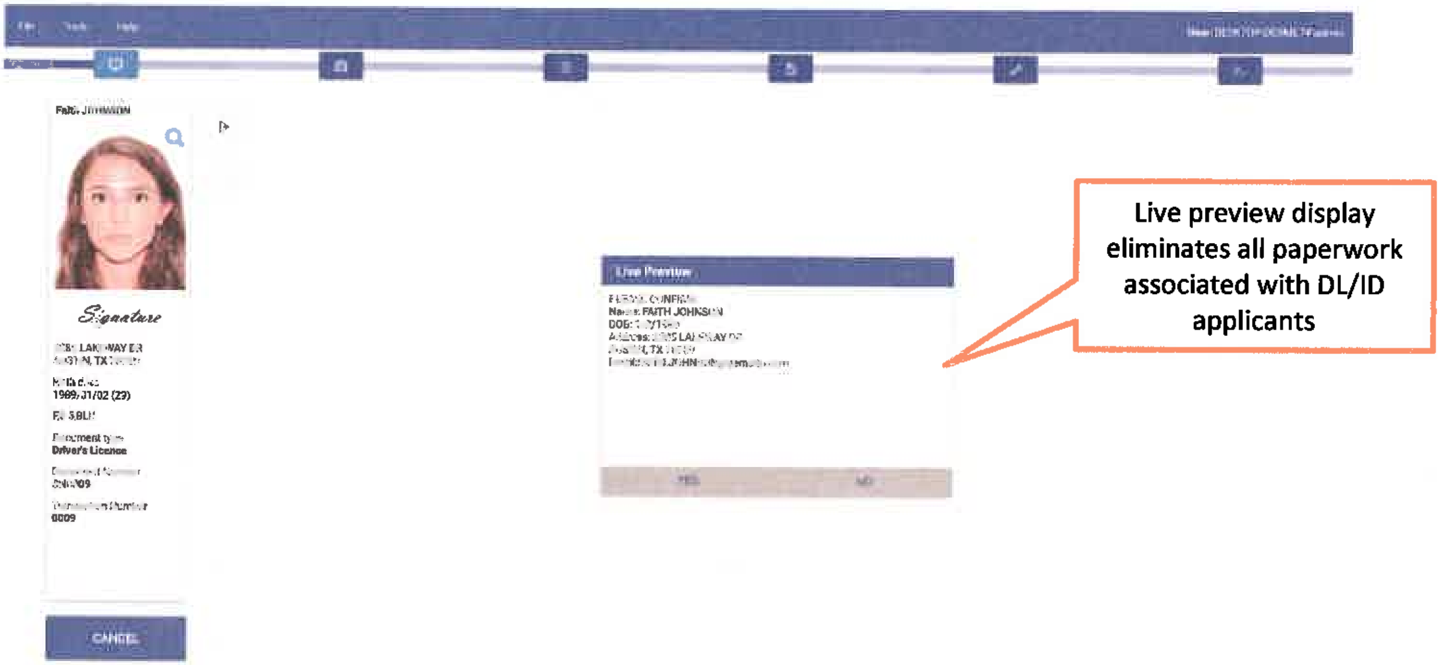


FIGURE 18: IMAGE CAPTURE WORKSTATION - PHOTO FIRST QUEUE

** Please note that the above screenshot is a sample of a previously delivered solution and the final user interface design will be specified during project specification workshops.*

Questionnaire

Our Image Capture Workstation and signature pad can display customer specific information with business specific application questions and capture customer responses and input with free form and (yes/no) responses required. Gemalto will work with the DMV during the planning phase of the project to define all business specific application questions and implement them with minimal free form. **For example, we currently provide the State of West Virginia with an integrated voter registration process into the signature pad allowing applications to answer a series of questions though check boxes on the signature pad to complete the registration process.** The application is then transmitted to the Secretary of State to complete the voter application process.



Live preview display eliminates all paperwork associated with DL/ID applicants

FIGURE 19: IMAGE CAPTURE WORKSTATION - QUESTIONNAIRE (ADDRESS VERIFICATION)

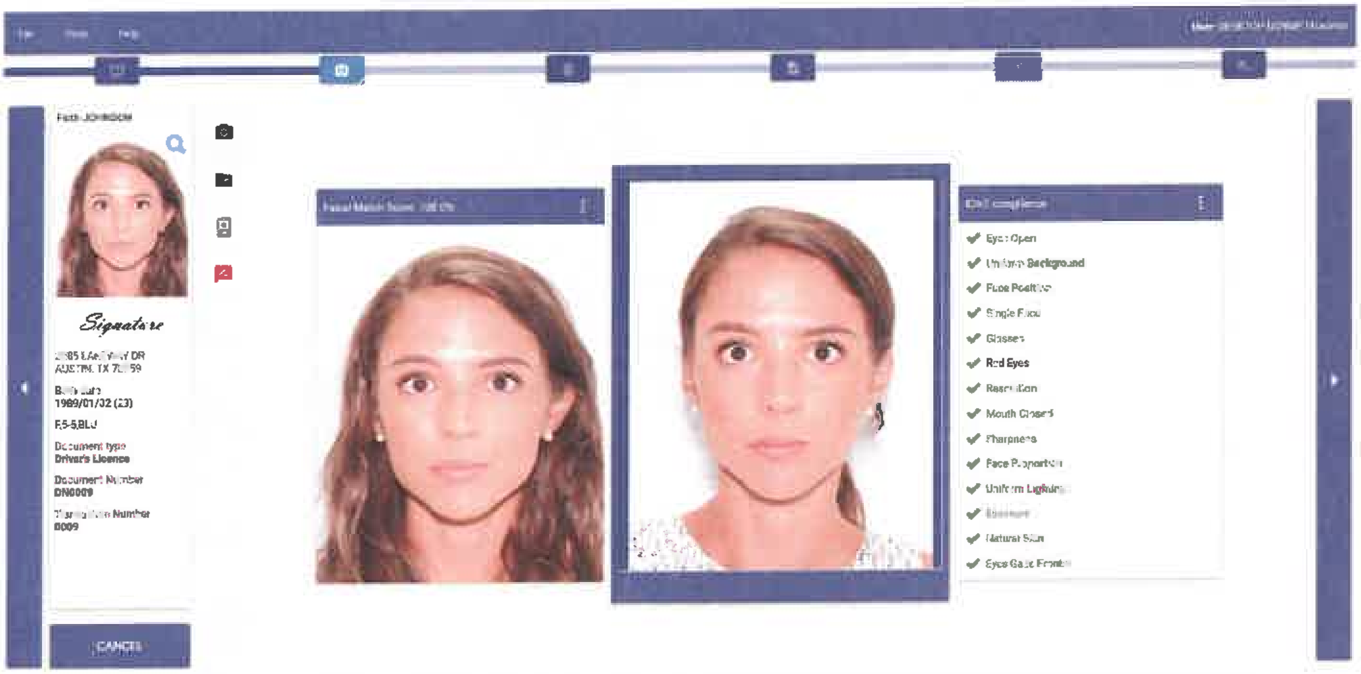
** Please note that the above screenshot is a sample of a previously delivered solution and the final user interface design will be specified during project specification workshops.*

We have also used the signature pad to enable applicants in the State of Idaho to preview and confirm their demographic data and addresses in addition to adding a questionnaire which removed all paperwork associated with DL/ID applications. We also used the signature pad in Idaho to replace all paper application forms with our questionnaire.

Photo Capture

When a photo is captured, Gemalto's solution automatically locates the eyes and therefore properly crops and rotates the photo. It also automatically adjusts for lighting and applicant heights (including applicants seated in wheelchairs). Our Image Capture process includes the following features:

- **1:1 Facial Recognition Feedback**
- **ICAO checks**
- **Automatic Exposure and Contrast Adjustment**
- **Live Preview**
- **Auto-cropping**
- **Auto-rotation**



Faith JOHNSON

2085 LAKEVIEW DR
AUSTIN, TX 78759

Birth date
1989/01/02 (23)

F,5-5,BLU

Document type
Driver's Licence

Document Number
DN0009

Transaction Number
0009

- ✓ Eyes Open
- ✓ Uniform Background
- ✓ Face Position
- ✓ Single Face
- ✓ Glasses
- ✓ Red Eyes
- ✓ Resolution
- ✓ Mouth Closed
- ✓ Sharpness
- ✓ Face Proportion
- ✓ Uniform Lighting
- ✓ Exposure
- ✓ Natural Skin
- ✓ Eyes Gaze Frontal

FIGURE 20: IMAGE CAPTURE WORKSTATION - IMAGE CAPTURE WITH 1:1 FEEDBACK AND ICAO CHECKS

** Please note that the above screenshot is a sample of a previously delivered solution and the final user interface design will be specified during project specification workshops.*

Gemalto's solution performs advanced evaluation algorithms on the photo image during capture to ensure the image is acceptable for use with facial recognition systems. These checks are performed using ICAO checks as shown below. There are 18 checks performed automatically. Visual feedback is provided to the DMV user based upon the results found. Checks are performed against all ICAO standards (which are based on ISO/IEC 19794-5) and can be configured to any additional photo requirements of the DMV.

ICAO checks can also be configured (turned on or off) by the DMV in our administration module. It is here that 1:1 comparison failures are also displayed to the user. Our solution supports overrides for scenarios where ICAO or 1:1 feedback checks are not passed due to medical or other reasons. Overrides may be logged and supervisor approval may be required for certain overrides i.e. 1:1 comparison failures.

Fingerprint Capture

Gemalto is experienced in providing biometric solutions and we most recently deployed a Driver's License System to the State of Colorado that enrolls, manages, and verifies the fingerprints of all customers who apply for driver's licenses. While this feature was not requested by the State of West Virginia, we can provide this as an option.

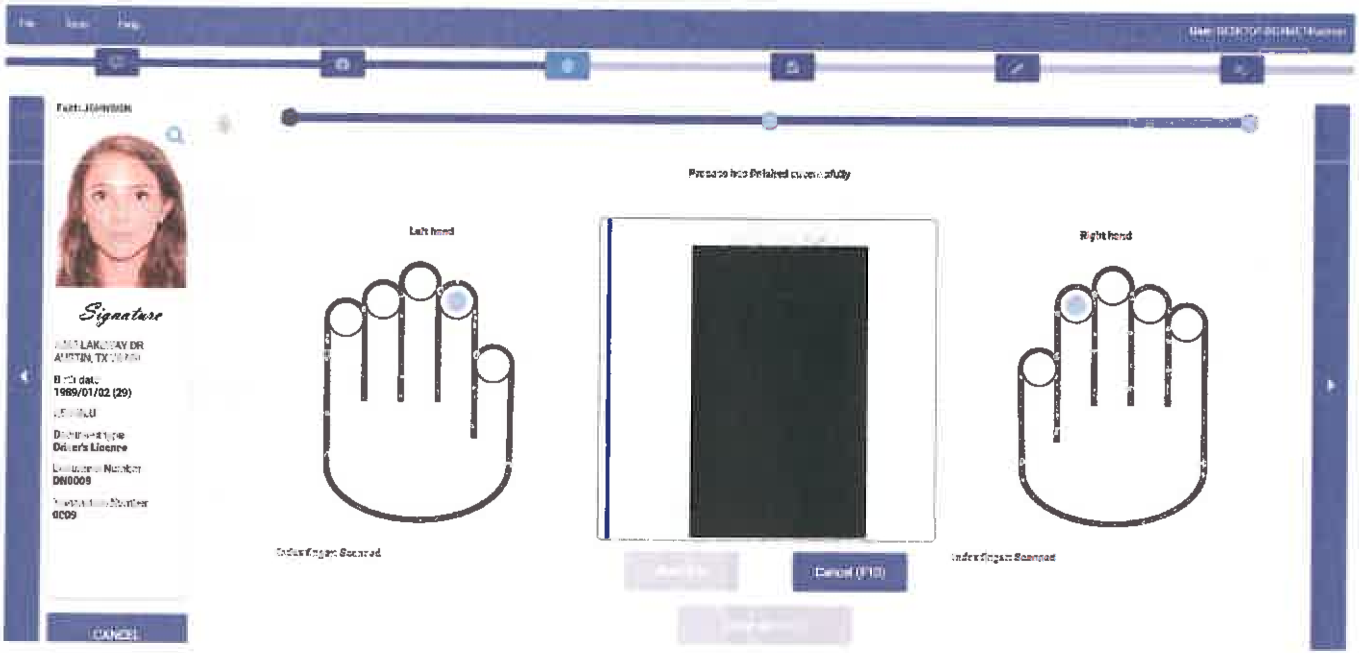


FIGURE 21: IMAGE CAPTURE WORKSTATION - FINGERPRINT SCANNING

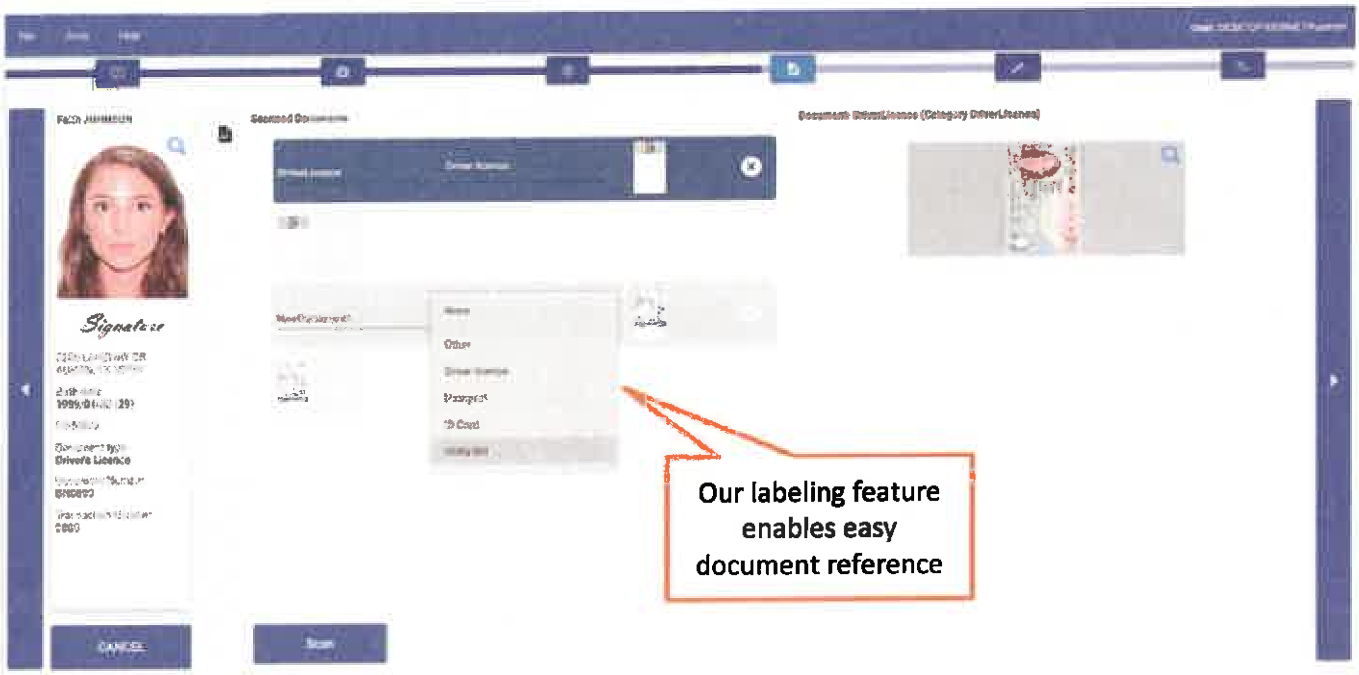
** Please note that the above screenshot is a sample of a previously delivered solution and the final user interface design will be specified during project specification workshops.*

Document Scanning

When designing the Gemalto's document scanning functionality within our Image Capture Workstation, we gathered extensive user input on the functionality required to be an efficient and useful system. This input gave us the clear insight that the ability to process applicants quickly and efficiently greatly hinges on a properly designed document scanning process. We took this insight, and designed a truly revolutionary document scanning system, a markplace leader in every way. This second to none system offers you the fastest applicant processing time.

Our Image Capture Workstation supports high-speed desktop auto feed scanners, flatbed scanners, and optional document authentications scanners. Our ICW includes a labeling feature that allows the operator to quickly select a label to identify a document so it is easier to look up the document at a later date and to assist in providing statistical analysis on the types of documents provided. Various views and tools are available to zoom in on elements on the document(s) to verify their authenticity or rotate a document for better viewing.

Within our Image Capture Workstation, documents can be easily scanned, labeled, rotated, edited, and deleted as illustrated below. Our solution also supports multipage scanning where documents can be easily separated from the multi-page scan using a simple drag and drop interface. Documents may be scanned individually or as a batch and then easily separated.



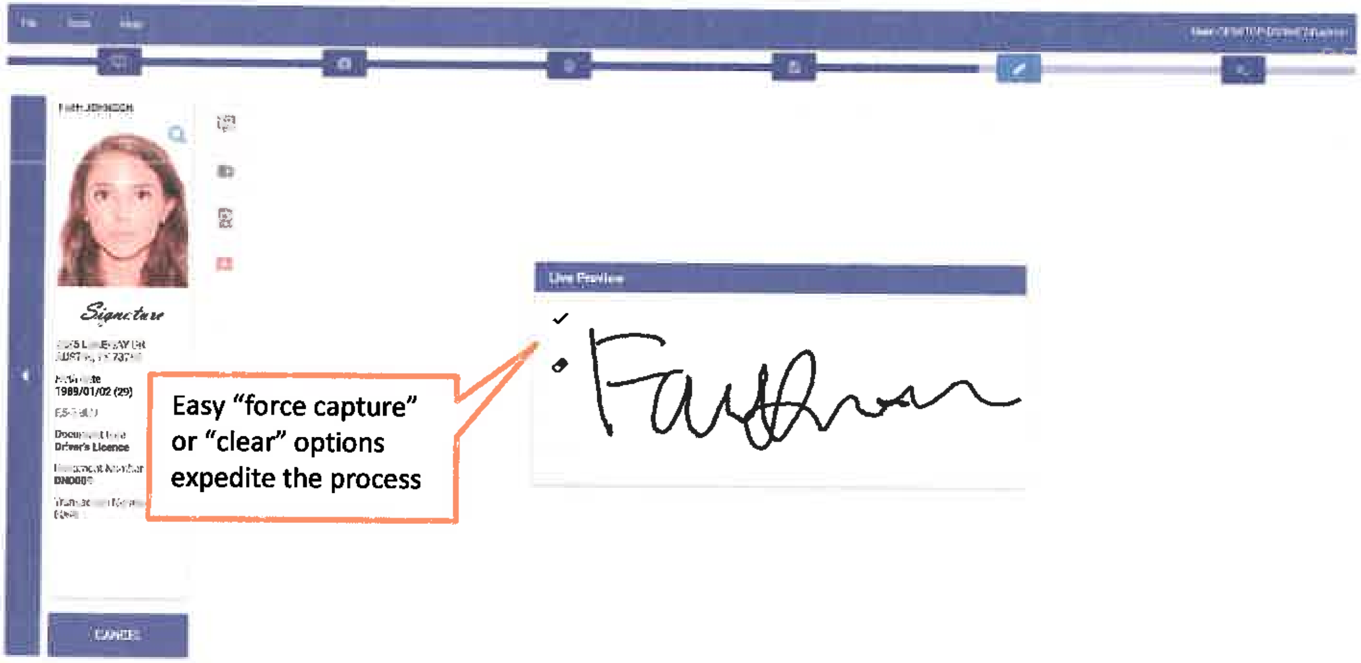
Our labeling feature enables easy document reference

FIGURE 22: IMAGE CAPTURE WORKSTATION - DOCUMENT SCANNING

** Please note that the above screenshot is a sample of a previously delivered solution and the final user interface design will be specified during project specification workshops.*

Signature Capture

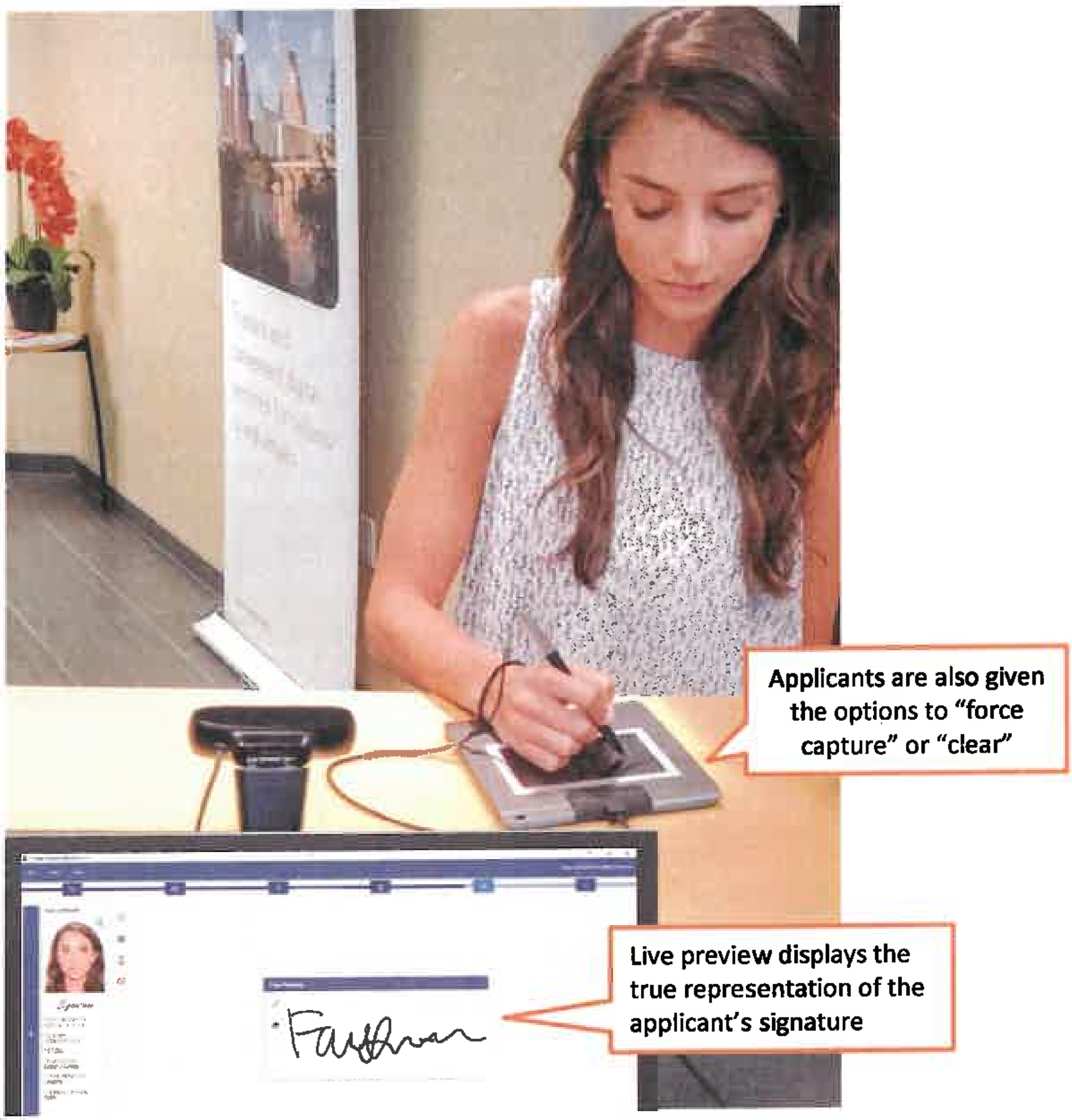
Gemalto's Image Capture Workstation (ICW) and proposed signature pad provides a true representation of the applicant's written signature. Our ICW allows for a live preview of signatures and enables the operator to expedite the process by force capturing or clearing an applicant's signature. Applicants are also given these options on the signature pad.



Easy "force capture" or "clear" options expedite the process

FIGURE 23: IMAGE CAPTURE WORKSTATION - SIGNATURE CAPTURE WITH LIVE PREVIEW

** Please note that the above screenshot is a sample of a previously delivered solution and the final user interface design will be specified during project specification workshops.*



Applicants are also given the options to "force capture" or "clear"

Live preview displays the true representation of the applicant's signature

FIGURE 24: IMAGE CPATURE WORKSTATION - SIGNATURE CAPTURE

Additional Functionality

While not specified by the DMV, we have provided some of the following functionality to other customers which can be added during the initial delivery of the project or throughout the life of the contract:

- Document/ID authentication
- Integration with queuing systems
- Kiosk integration

As requested, we have addressed each of the individual requirements listed in the RFP below.

Section 4, Subsection 4.8.2 - Vendor should describe the capabilities of the proposed image capture device. Description should include:

Gemalto's Image Capture Workstation and Camera Tower have been designed to be robust, efficient, and consistent with regards to the capture of image. Our solution includes automated functions to optimize and standardize portraits and ensures that they meet quality check standards as described below.

Image Cropping

When a photo is captured, the Gemalto's solution automatically locates the eyes and therefore properly crops and rotates the photo, as can be seen in the figure below. If, for any reason, such as an applicant's medical condition, the solution has difficulty locating the eyes, the user can manually place the yellow locators (as seen in the following image) over the eyes and it will automatically adjust. This feature ensures 100% consistency in cropping across all DMV offices and reduces the user processing time compared to the current solution we have provided to the State. .

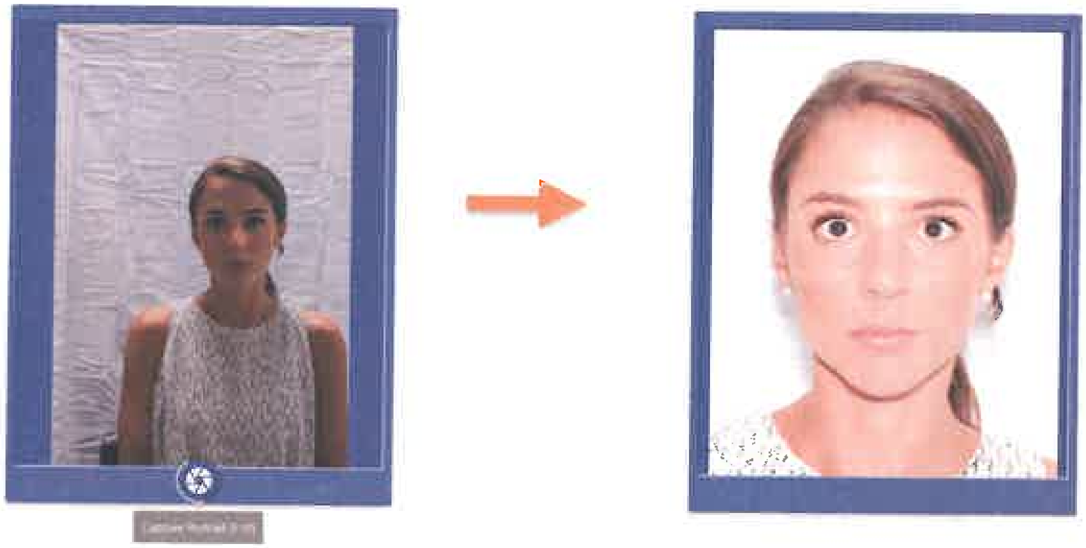
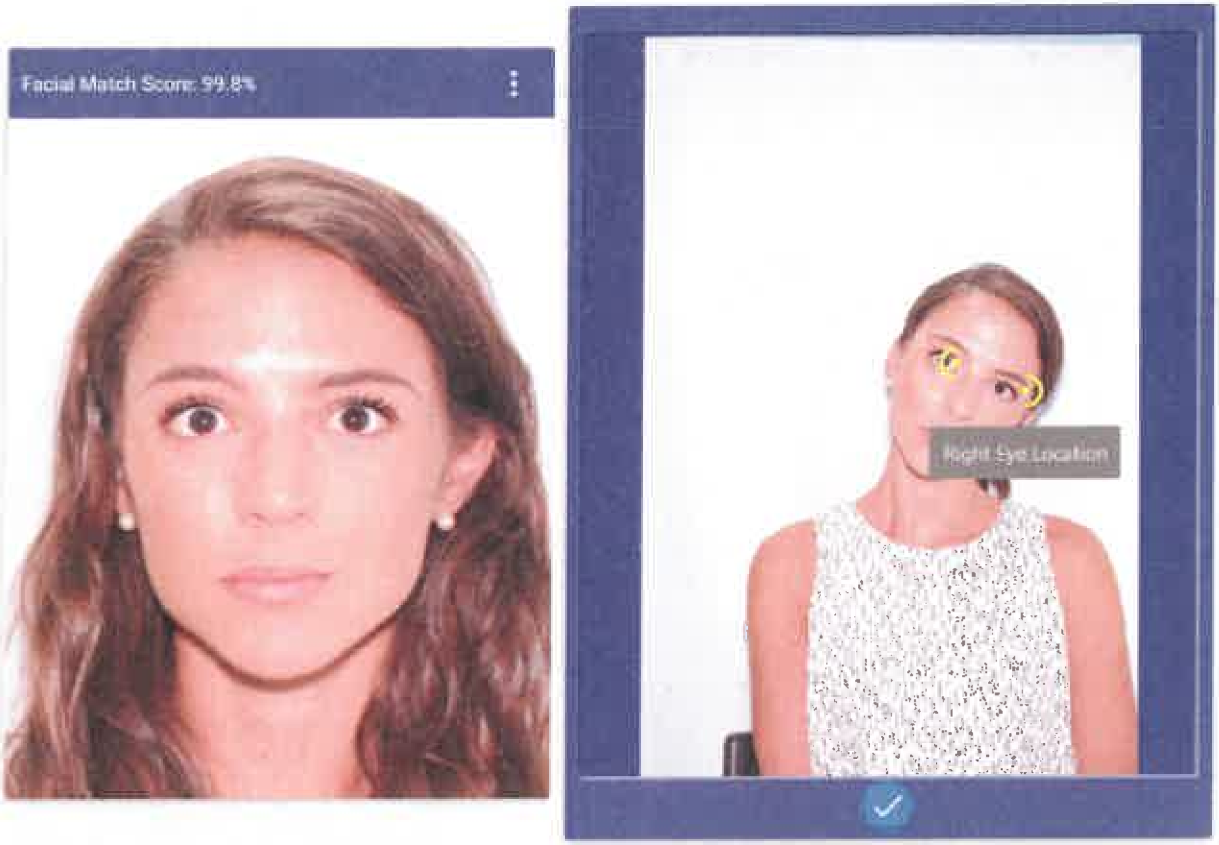


FIGURE 25: IMAGE CAPTURE WORKSTATION - AUTOMATIC CROPPING

** Please note that the above screenshot is a sample of a previously delivered solution and the final user interface design will be specified during project specification workshops.*



Facial Match Score: 99.8%

FIGURE 26: IMAGE CAPTURE WORKSTATION - EYE POSITION ADJUSTMETN

**** Please note that the above screenshot is a sample of a previously delivered solution and the final user interface design will be specified during project specification workshops.***

It should also be noted that the automatic eye location feature is also beneficial for adjusting for heads that may be tilted, such as someone who cannot sit straight in a wheel chair. The eyes will be automatically detected and the solution will properly adjust the image so that the head is no longer tilted, as illustrated below. **You can also clearly see how our Image Capture solution can return high quality portraits even in poor lighting conditions.**

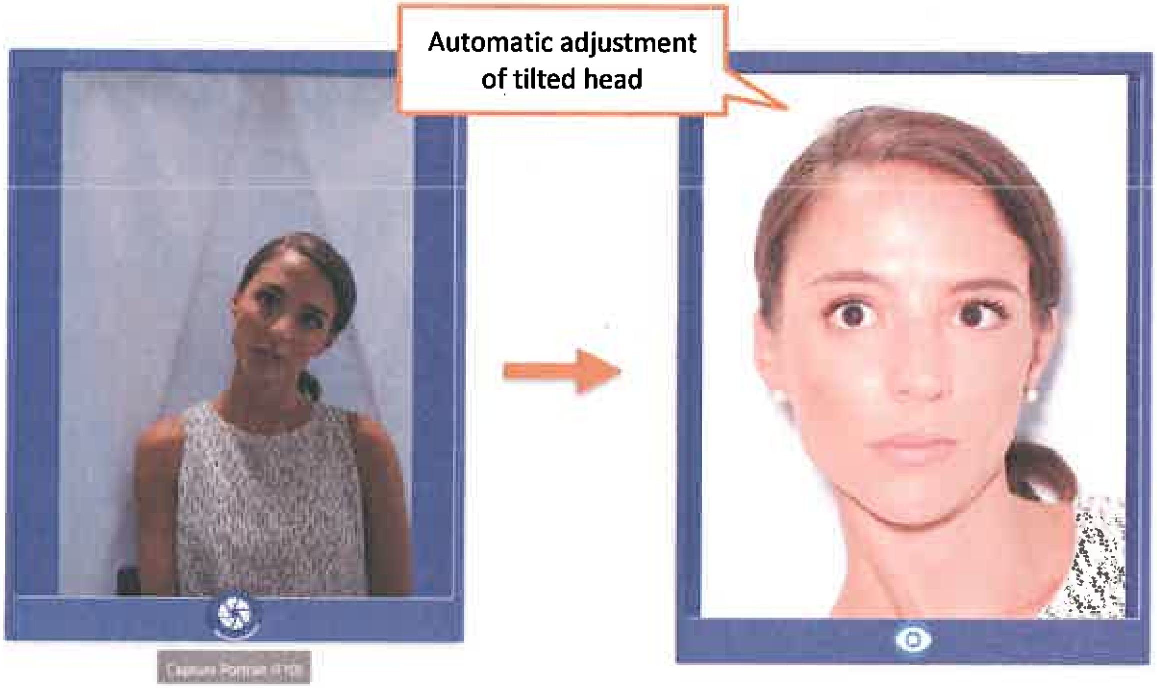


FIGURE 27: AUTO IMAGE ADJUSTMENT FOR HEAD TILT

***** *Please note that the above screenshot is a sample of a previously delivered solution and the final user interface design will be specified during project specification workshops.*

Image Placement

Once the image is captured, our software automatically locates the eyes of the applicant and automatically crops, rotates, and optimizes the captured image to provide consistent portraits between different applicants, offices, and varying lighting conditions at differing times of the day. One of the ICAO checks automatically performed in our solution is the "Face Position Check", as seen in Figure 20 below, which checks for the proper face size and position within the image.

Light Sensitivity Adjustment

Our Image Capture Tower automatically focuses and adjusts for varying lighting conditions. One of the automatic checks that are performed is the "Uniform Lighting Check", as seen in Figure 30 below, which ensures that we are checking the consistency of the lighting when we are capturing an image. For extreme changes in lighting conditions, which occur rarely, we provide manual adjustments of the flash to compensate for any changes to strengthen or soften the flash.

In addition, after the image has been captured, our Image Capture Workstation allows users to adjust brightness (gamma) settings manually. While we can allow users a greater level of control in image adjustments after the image is taken, we recommend providing simple adjustments as, in our experience, too much control results in users taking longer to process applications.

Color Correction of Images

Gemalto's solution provides consistent images through a few different mechanisms. First, the proposed DLSR housed in our camera tower and the commercial grade flash provide consistent lighting. In addition, exposure is automatically managed at the camera level, providing consistency across images with varying lighting condition and skin tones. Our Image Capture Workstation (ICW) software is configured during setup for each camera tower to account for any variances in-between field offices or camera tower locations providing default settings for each camera tower we deploy. Users may also manually adjust gamma settings to quickly and easily adjust both contrast and exposure in one easy step. Please note that our ICAO checks include exposure/contrast checks alerting the user when a captured portrait is not within the acceptable threshold.

Red Eye Station

In our experience, red eye in captured photos is rare occurrence when a solution is properly deployed. Understanding red eye is key to preventing them. Red eye typically occurs when too much flash is used in a poorly lit scenario. By including a commercial grade flash with a soft diffuser within our image capture tower, we are able to greatly reduce the frequency of red eye in the field. Our flash is fully integrated and controlled by our Image Capture Workstation software.

Automatic Focus and Centering

The focus of our Image Capture Tower is handled by a DSLR camera housed internally. Modern DSLRs, like the ones that we are providing, include face detection and depth sensors to automatically provide consistent "in focus" portrait image. This is a mature technology and has proven to be reliable in the field.

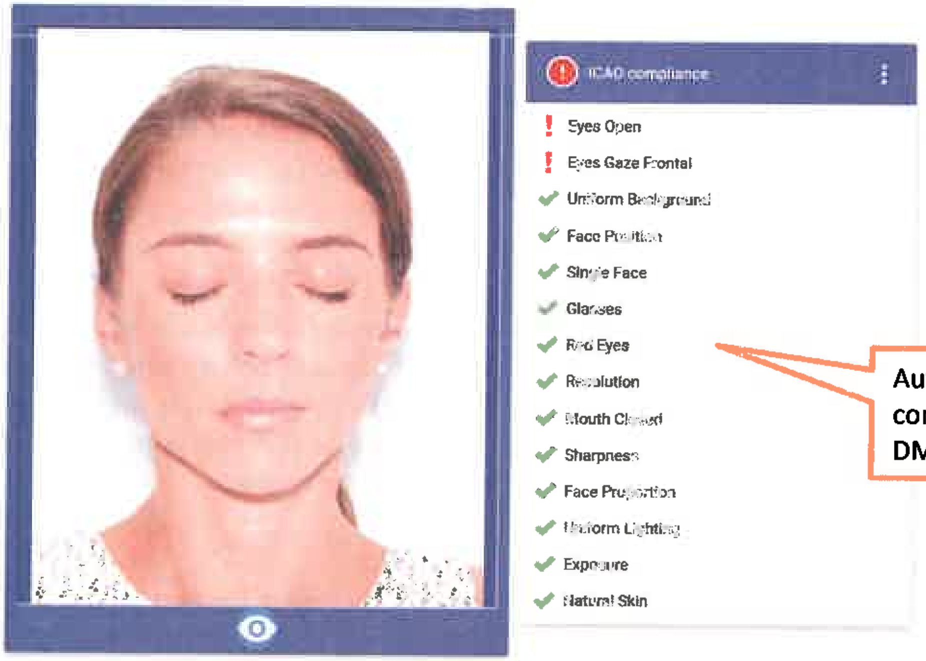
While our cameras do not physically move to follow and center on the applicant, our solution provides consistently centered portraits due to face detection and cropping as described above. This allows us to provide a more consistent look and feel from card to card for our customers.

Strobe or Other Lighting Device

Gemalto's Image Capture Tower has an integrated professional flash which adapts to the most problematic lighting environments. A soft diffusor is included to prevent applicants from blinking during photo capture and to reduce red eye. The commercial grade flash unit is fully integrated with our Image Capture Tower and controlled by our Image Capture Workstation (ICW) software. We have included a more robust flash unit that the current model used by the State with a bulb life of 250,000 flashes reducing the required maintenance and bulb burnouts.

Meeting Minimum Resolution for Facial Recognition Software

Gemalto's solution performs advanced evaluation algorithms on the photo image during capture to ensure the image is acceptable for use with facial recognition systems. These checks are performed using ICAO as described above. ICAO's photo quality standards were designed taking usability in facial recognition systems into account. When a photo is checked against ICAO standards, we are confirming its usability in our FRS. Photo resolution is also checked by our system however this is typically not an issue due to the high resolution in today's DLSR cameras and specifically the camera included in our capture tower.



ICAO compliance

- ! Eyes Open
- ! Eyes Gaze Frontal
- ✓ Uniform Background
- ✓ Face Position
- ✓ Single Face
- ✓ Glasses
- ✓ Red Eyes
- ✓ Resolution
- ✓ Mouth Closed
- ✓ Sharpness
- ✓ Face Proportion
- ✓ Uniform Lighting
- ✓ Exposure
- ✓ Natural Skin

Automatic checks are configured to your DMV requirements

FIGURE 28: ICAO PHOTO QUALITY CHECKS

** Please note that the above screenshot is a sample of a previously delivered solution and the final user interface design will be specified during project specification workshops.*

Our Image Capture Workstation provides feedback if the captured image does not meet quality check standards. Users are provided clear feedback with both a color change (typically from green to red) and text identifying which quality control checks did not pass. These automatic checks can be configured to DMV requirements and individually disabled if required by DMV business rules i.e., if smiling is allowed by the State (however we recommend against this as varying facial expressions lead to greater variation in the portrait database and can decrease the accuracy of the Facial Recognition System).

Image Capture Tower – Setup and Calibration

Our Image Capture Tower is easy to setup and calibrate enabling the DMV to take high quality and consistent photos across all offices in varying lighting conditions and environments. Our Image Capture Workstation (ICW) includes an automatic calibration tool to setup both exposure (illustrated below) and white balance. This configuration tool takes a series of photos and automatically indicates the recommended setting, illustrated by an orange box below, however operators or technicians can select different settings based on environmental conditions. Our calibration tool is easy to use and automatically selects the optimized settings for the user and allows us to quickly and effectively set up the workstations at each location, with two simple mouse clicks.

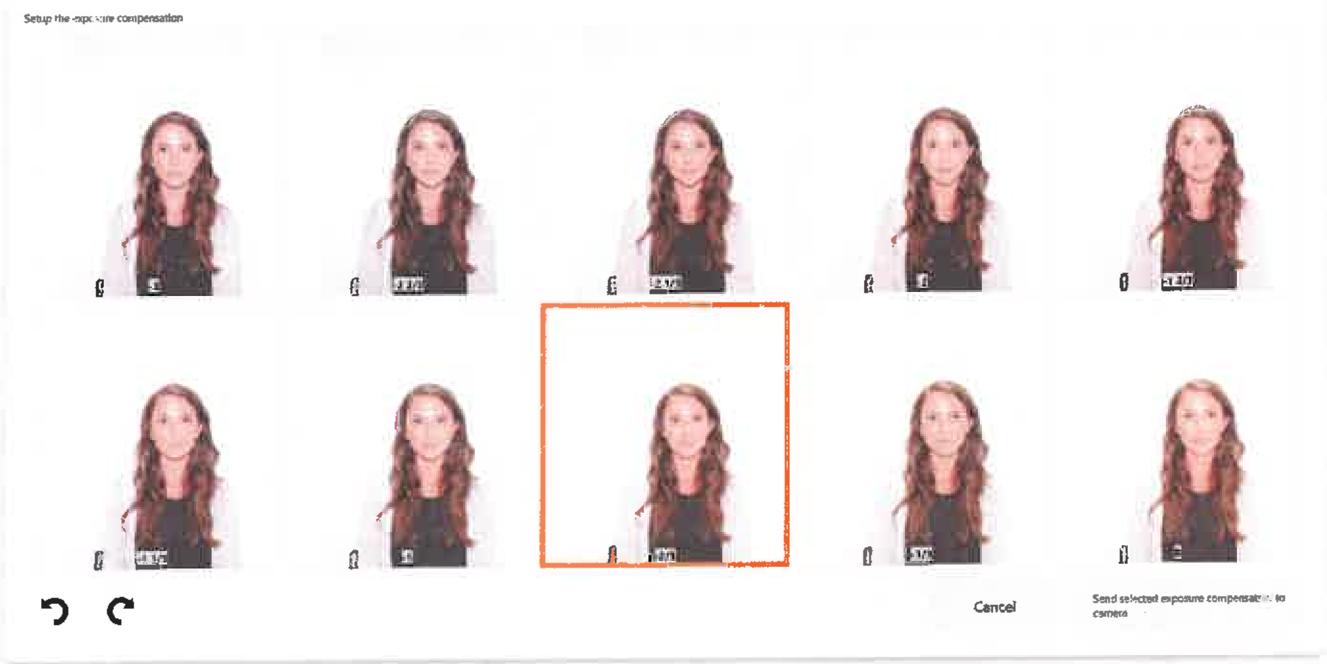

Setup the exposure compensation
Cancel
Send selected exposure compensation to camera

FIGURE 29: AUTOMATED CAMERA SETUP - EXPOSURE

** Please note that the above screenshot is a sample of a previously delivered solution and the final user interface design will be specified during project specification workshops.*

4.8.2.1 How live video of the applicant will be displayed.

VENDOR RESPONSE:

Gemalto confirms that a live video (live preview) is included within our Image Capture Workstation (ICW). This is a standard feature delivered to many of our customers, including Colorado, Idaho, New Hampshire, and the Atlantic Provinces most recently. In the below screenshot, you can see the live preview window on the left and the final captured image on the right. **You can also clearly see how our Image Capture solution is able to produce high quality portraits, even in poor lighting conditions.**

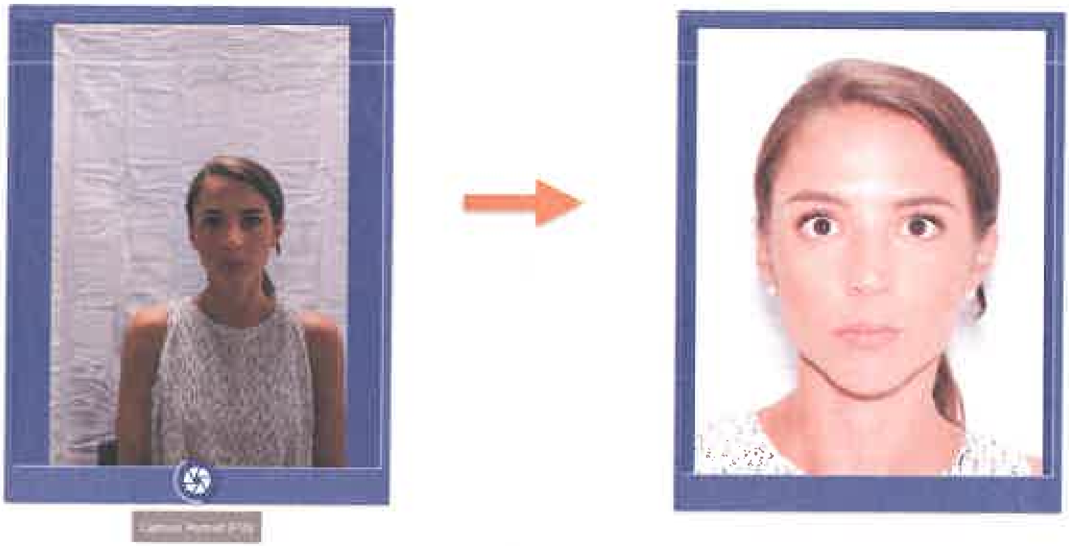


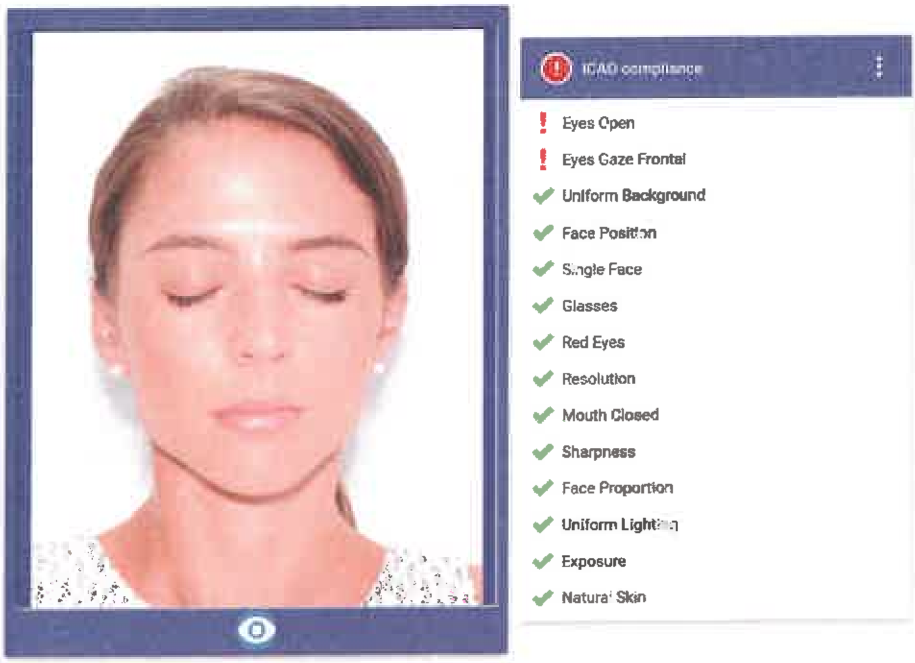
FIGURE 30: IMAGE CAPTURE WORKSTATION – LIVE PREVIEW AND CAPTURED IMAGE

** Please note that the above screenshot is a sample of a previously delivered solution and the final user interface design will be specified during project specification workshops.*

4.8.2.2 How the employee can perform configuration ICAO checks and how these results will be returned to the employee

VENDOR RESPONSE:

Gemalto's solution performs advanced evaluation algorithms on the photo image during capture to ensure the image is acceptable for use with facial recognition systems. These checks are performed against ICAO standards as shown below and we have provided newer, more robust comparison algorithms in our solution. There are 18 checks performed automatically. Visual feedback is provided to the DMV user based upon the results found. A green check provides clear feedback to the user. A red response denotes a problem along with the red background is a description of the issue that caused the problem so the user can instantly address it. Checks are performed against all ICAO standards (which are based on ISO/IEC 19794-5) and can be configured to any additional photo requirements of the DMV. ICAO checks can also be configured (turned on or off) by the DMV in our administration module. It is here that 1:1 comparison failures are also displayed to the user.



ICAO compliance

- ! Eyes Open
- ! Eyes Gaze Frontal
- ✓ Uniform Background
- ✓ Face Position
- ✓ Single Face
- ✓ Glasses
- ✓ Red Eyes
- ✓ Resolution
- ✓ Mouth Closed
- ✓ Sharpness
- ✓ Face Proportion
- ✓ Uniform Lighting
- ✓ Exposure
- ✓ Natural Skin

FIGURE 31: ICAO PHOTO QUALITY CHECKS

** Please note that the above screenshot is a sample of a previously delivered solution and the final user interface design will be specified during project specification workshops.*

4.8.2.3 How an employee can recheck for ICAO compliance after manual adjustments

VENDOR RESPONSE:

Gemalto confirms that our solution automatically rechecks for ICAO compliance after manual adjustments. This could be after cropping is adjusted or after brightness or contrast is adjusted (however we recommend against allowing too much adjustment on photo settings as we have found it drastically slows down citizen processing times). Photos are automatically rechecked to ensure that they are still of sufficient quality to be used in our Facial Recognition System (FRS) and Biometric Investigative Workstation (BIW).

4.8.2.4 How checks will be configurable to allow the Agency's system administrator to select the specific ICAO checks to be enabled.

VENDOR RESPONSE:

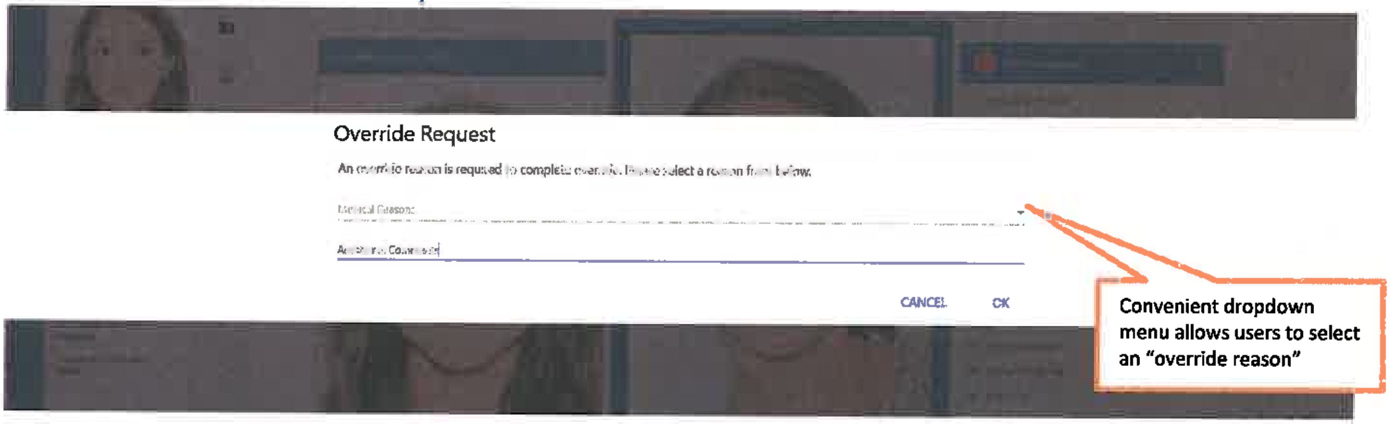
Gemalto confirms that our solution allows individual or all ICAO checks to be disabled through our central server administration module. This is a standard feature within our solution and allows the State to quickly adapt to any operational issues or changes to legislation. For example, one of our customers is currently discussing a new law in their State Senate which will allow smiling in driver's license and ID photos. If this law is passed, we are able to quickly adapt without any changes to our solution.

4.8.2.5 How checks will be configurable to allow the Agency's system administrator to select the specific ICAO checks where overrides are allowed.

VENDOR RESPONSE:

Gemalto confirms that our Image Capture Workstation allows overrides. Overrides may be allowed for only certain check failures and this may be configured by the DMV in the Central Server (CS) administration module. Our solution can also be configured to require supervisor approval for certain types or failures i.e. 1:1 checks that fail due to medical or other reasons. In the below example, users can select the reason for an override from a dropdown menu and are allowed to enter additional comments. Please note that all overrides may be logged within our system.

Note that any override pertaining to a potential fraud is audited, provided in reports and can be flagged to be sent to the states IS&S department.



Override Request

An override reason is required to complete override. Please select a reason from below.

Medical Reasons

Additional Comments

Convenient dropdown menu allows users to select an "override reason"

FIGURE 32: IMAGE CAPTURE WORKSTATION - OVERRIDES

** Please note that the above screenshot is a sample of a previously delivered solution and the final user interface design will be specified during project specification workshops.*

Section 4, Subsection 4.8.3 - Vendor should explain the process and provide a detailed list of hardware the proposed solution will use to capture images and signatures when communication with the central image/demographic system is off-line. The system should be able to link new data and images to existing records when communication with the server is restored.

VENDOR RESPONSE:

As described in the below response to "Requirement 4.12.2.3", Gemalto has also designed its Image Capture Workstation (ICW) to manage power failure scenarios. Software settings for our ICW are maintained in a separate configuration file so they will not be affected by a loss of power and will return to the previous status when restarted. When the ICW is restarted, users may be given the option to continue the current transaction or to start a new transaction and save the previous transaction as incomplete.

Transactional data is also maintained in the event of a power loss or loss of communication with the Central Server. In "Off-line" mode newly captured transactional data and images are locally stored, in an encrypted format, until connectivity to the Central Server is restored and successful transmission is confirmed (i.e. new data and images are linked to existing records).

Section 4, Subsection 4.9 - Secure Temporary DLJID

Section 4, Subsection 4.9.1 - Vendor solution should produce a secure temporary driver's license with the applicant's image and signature.

VENDOR RESPONSE:

Gemalto confirms that a secure temporary driver's license will be produced by our Image Capture Workstation (ICW) including the applicant's image and signature. Temporary DL/ID can include all of the data elements produced in the final credential including portraits, signatures, demographic data, and the PDF417 barcode. Overall, the look and feel is designed to match the final credential however it is constructed from paper and not plastic.

Section 4, Subsection 4.9.2 - Vendor solution should print a temporary DL/ID from the Vendor's image and signature capture workstation or from a Vendor web application accessed from the Agency's workstations.

VENDOR RESPONSE:

Gemalto confirms that our solution prints a temporary DL/ID from the Image Capture Workstation (ICW) following successful completion of the enrollment process. **We currently provide this functionality to many of our customers including West Virginia (currently for centrally issued credential), Colorado, Idaho, and New Hampshire).**

Section 4, Subsection 4.9.3 - If the print request is triggered from the ICW, the printing of the temporary DL/ID should be automatic and should not require employee action.

VENDOR RESPONSE:

Gemalto confirms that print requests for the temporary DL/ID may be automatically triggered from the ICW and will not require employee action. Workflows within our Image Capture Workstation (ICW) are configurable and will be updated to match the business processes and flows of the DMV. Our solution can automatically print the temporary DL/ID at the completion of a transaction or we can add dedicated buttons to trigger the printing or re-printing of a temporary DL/ID in the event of a paper jam or any other issues.

Section 4, Subsection 4.9.4 - In event of printing error, the Vendor solution should include a function for reprinting the temporary DL.

VENDOR RESPONSE:

Gemalto confirms that our Image Capture Workstation is capable of reprinting a temporary DL/ID in the event of a printing error (i.e. paper jam, out of toner, communications error, etc....). Our solution even allows for employees to reopen completed transactions and to reprint the original temporary DL/ID (with the original expiration dates) in the event that an applicant loses their temporary document.

Section 4, Subsection 4.10 - Consumables for Secure Temporary DL

Section 4, Subsection 4.10.1 - Vendor should provide a system for electronically ordering and tracking the secure paper stock for use in each of the Agency's 27 locations.

VENDOR RESPONSE:

Gemalto confirms that our solution enables the DMV to track and electronically order secure paper stock, and printer toner, for each of the Agency's 27 locations. Gemalto has a robust Inventory Management System (IMS) that is capable of tracking card bodies and consumables from manufacturing through personalization and can be used in both central issuance or over the counter issuance models. We have designed a new and easier IMS reducing the manual input required and improving automation.

For over the secure paper stock (Temporary License), toner and card stock (For exceptional cases in Kanawha City location), our solution can count when consumables are used and subtract them from the current inventory for each of the Agency's 27 locations. When inventories drop below configurable levels, we can create automated alerts within our system to allow the weekly system reporting to flag these events.

All consumables will be controlled and documented though the IMS. Consumables will be traceable though barcode scanning, at a minimum, through the following steps:

- Receipt of all consumables at Gemalto's distribution facility will be verified based on records received from the original manufacturer.
- Consumables will be received in large volumes initially and will be broken down into smaller lots for field offices. All consumables will be scanned and assigned a specific location for distribution.
    - The Consumables will be marked as shipped during distribution to field offices and may be sent using a courier like FedEx or hand delivered by field technicians.
- Upon receipt of the consumables at the field offices, the consumables will need to be scanned in order for the materials to complete the assignment process within the IMS. Without completing this step, the IMS can provide an alert to the operator that the consumables were not properly received.
- The system can identify if a shipment is not received by the expected arrival date, automatically create a report.

Section 4, Subsection 4.11 - Signature Capture

Section 4, Subsection 4.11.1 - Vendor solution should allow for the capture of true representation of the applicant's written signature.

VENDOR RESPONSE:

Gemalto confirms that our proposed signature pad and Image Capture Workstation (ICW), which also captures signatures, meets the DMV's requirements set forth in this request for proposal.

Proposed Signature Pad

The proposed Wacom STU-530 signature pad included a battery-free pen with 1024 levels of pressure sensitivity to accurately capture the unique pen pressure profile of a signature to be included in the biometric data. . It offers a very comfortable signing experience with a thin design and low profile. The large high quality, high resolution color LCD screen provides ample space to view and sign documents. The hardened glass signing surface protects the LCD and is highly resistant to scratches. A single USB cable supplies power and data, minimizing clutter at the counter or point-of-sale. This model has a larger screen and higher resolution compared to the current Topaz model used by the Agency.

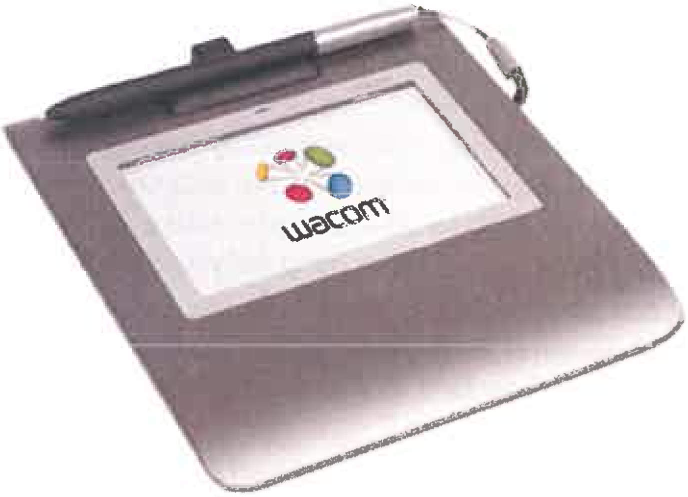


FIGURE 33 - WACOM STU-530

Gemalto confirms that the proposed signature pad provides a true representation of the applicant's written signature. The proposed signature pad delivers 2540 dpi (non-interpolated) high resolution digital images of the applicants hand written signature with ± 0.02 inch coordinate accuracy, and report rate of 200 points per second/800 4D coordinates.

In addition, our Image Capture Workstation (ICW) software and the proposed Wacom signature pad facilitates the capabilities to capture the signature to ensure that at personalization it will meet all AAMVA DL/ID Card Design Standards for the captured signature (e.g. Orientation, Size, Scaling, Color, Borders, and Printing Resolution). The issue of "Cropping" is avoided in the signature pad because the user is presented with a rectangular signature box (dimensions are proportional to standards to maintain the aspect ratio at personalization time) to sign within. If the user signs outside of the boundaries of the signature box, the signature will be automatically rejected and the user asked to sign again. This is a standard offering and all solutions that have been delivered to all of our customers have been compliant.

Section 4, Subsection 4.11.2 - Vendor solution should allow applicant to clear and sign again.

VENDOR RESPONSE:

Gemalto confirms that our Image Capture Workstation (ICW) allows users to recapture applicant signatures. Applicants can select "clear" and resign if they are not satisfied with their signature. Please note that all of this functionality is configurable and can be included or disabled based on your preferences. In addition, all of the buttons, verbiage, and interfaces may be configured based on your preferences.

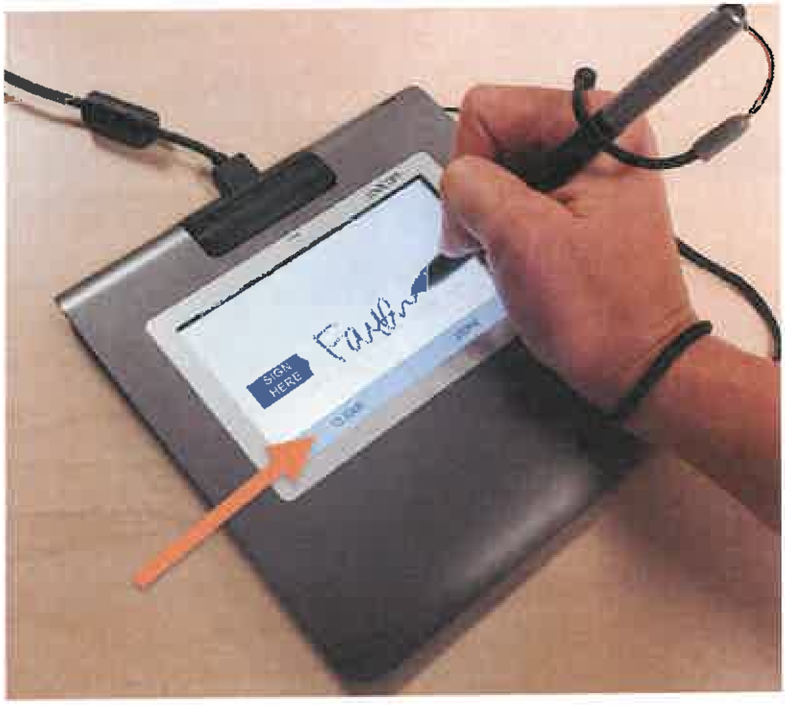


FIGURE 34: SIGNATURE CAPTURE - RECAPTURE

Section 4, Subsection 4.11.3 - Vendor solution should display a live signature on the workstation for the employee to view.

VENDOR RESPONSE:

Gemalto confirms that our Image Capture Workstation allows for a live preview of signatures. This is a standard feature of our software and is illustrated below:

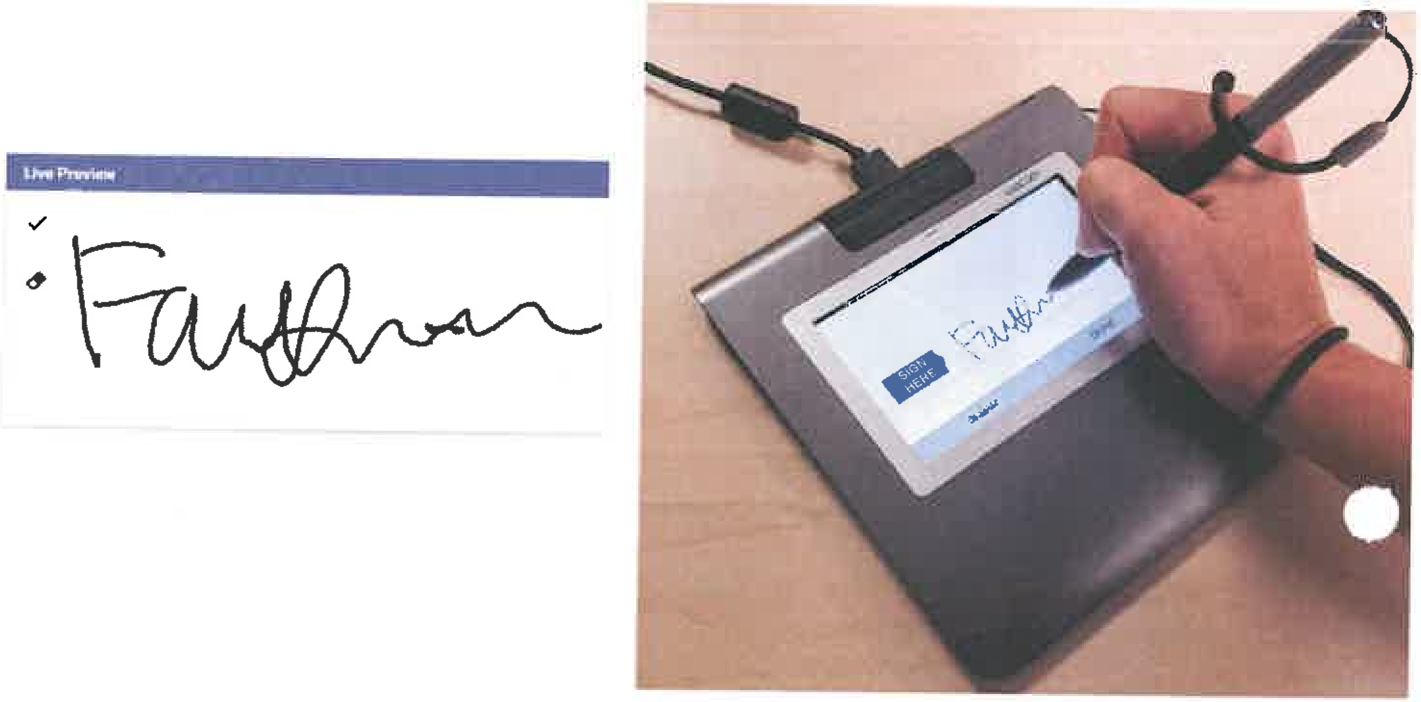


FIGURE 35: LIVE SIGNATURE PREVIEW

** Please note that the above screenshot is a sample of a previously delivered solution and the final user interface design will be specified during project specification workshops.*

Section 4, Subsection 4.11.4 - Vendor solution should allow employee to freeze and accept signature on the workstation, over-riding the clear selection on the signature pad.

VENDOR RESPONSE:

Gemalto confirms that our Image Capture Workstation (ICW) allows employees to freeze and force accept signatures. This is done by clicking on the check icon as illustrated in the below example. Please note that all of this functionality is configurable and can be included or disabled based on your preferences. In addition, all of the buttons, verbiage, and interfaces may be configured based on your preferences. The system can also audit whether the DMV operator confirmed the signature or if it was the applicant.

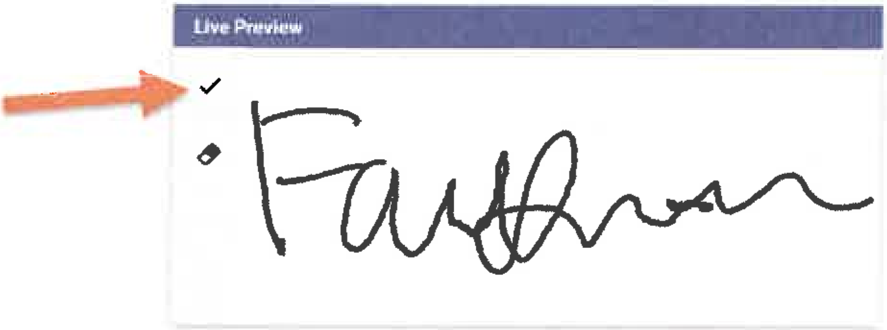


FIGURE 36: SIGNATURE CAPTURE - FORCE ACCEPT

** Please note that the above screenshot is a sample of a previously delivered solution and the final user interface design will be specified during project specification workshops.*

Section 4, Subsection 4.11.5 - Vendor solution should allow employee to clear signature to allow the applicant to sign again.

VENDOR RESPONSE:

Gemalto confirms that our Image Capture Workstation (ICW) allows employees to clear signatures to allow applicants to sign again just like we do today. This is done by clicking on the eraser icon as illustrated in the below example. Please note that all of this functionality is configurable and can be included or disabled based on DMV preferences. In addition, all of the buttons, verbiage, and interfaces may be configured based on DMV preferences.

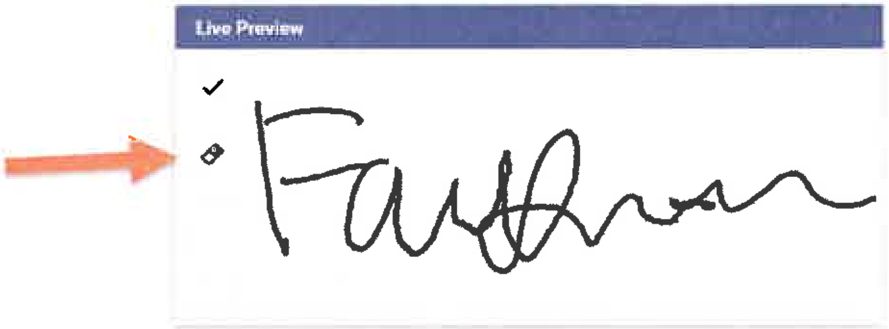


FIGURE 37: FORCE CLEAR

** Please note that the above screenshot is a sample of a previously delivered solution and the final user interface design will be specified during project specification workshops.*

Section 4, Subsection 4.11.6 -Vendor solution should allow employee to select "Unable to Sign" for those applicants who are unable to provide a signature.

VENDOR RESPONSE:

Gemalto confirms that our Image Capture Workstation (ICW) allows employees to select "Unable to Sign" for applicants that are unable to provide a signature. We are also able to re-use existing signatures or manually upload images of signatures if required by the DMV.

Section 4, Subsection 4.11.7 - Vendor solution should allow for the display and recording of responses to questions prompted on the signature capture device.

VENDOR RESPONSE:

Gemalto confirms that our Image Capture Workstation and signature pad can display and record responses and input with free form and (yes/no) responses required. Gemalto will work with the DMV during the planning phase of the project to define all business specific application questions and implement them with minimal free form.

Currently, in West Virginia, we have successfully integrated the voter registration process into the signature pad allowing applications to answer a series of questions though check boxes on the signature pad to complete the registration process. Their application is then transmitted to the Secretary of State to complete the voter application process.

We have also used the signature pad to enable applicants in the State of Idaho to preview and confirm their demographic data and addresses in addition to adding a questionnaire which removed all paperwork associated with DL/ID applications. We also used the signature pad in Idaho to replace all paper application forms with our questionnaire.

Section 4, Subsection 4.12 - Credential Issuance System (CIS) Objectives

Section 4, Subsection 4.12.1 - Vendor should describe how their proposed solution will handle image and data retrieval for business related inquiries. This description should include:

VENDOR RESPONSE:

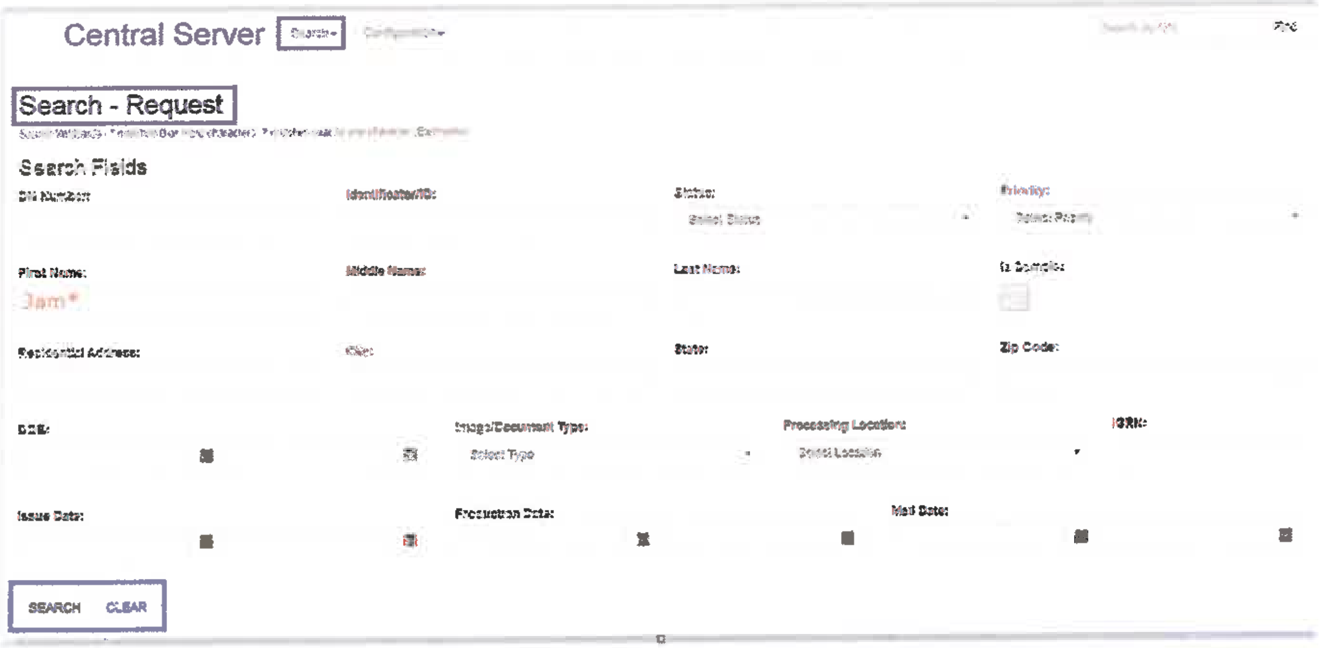
Gemalto confirms that our solution allows image and data retrieval for business related inquires. These are typically performed within two different modules of our solution:

- **Web Reporting System Interface (WRS)** – Our WRS is based on SQL Server Reporting Services and allows the DMV to look up and investigate trends and statuses within our solution.
- **Central Server (CS) administration module** – Our administration module manages more advanced lookups for photos, individual statuses of cards, and other audit data.

4.12.1.1 How wildcard searches can allow for all data elements, including first character searches. Search results should be returned in a format that allows for easy sorting and selection of individual records to view.

VENDOR RESPONSE:

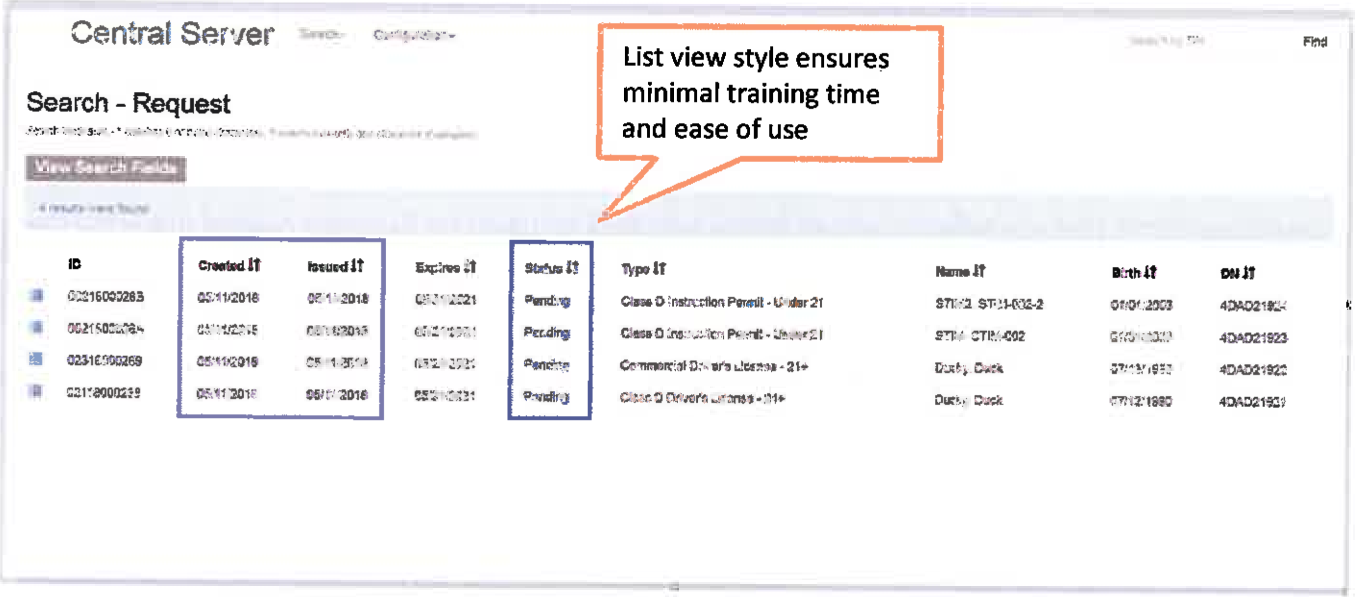
Gemalto confirms that wildcard searches are allowed within our solution for all data elements. Sorting of results and the selection of individual results is also allowed in our WRS and CS administration module in addition to our Biometric Investigative Workstation (BIW).



First Name: Jam*

FIGURE 38: CENTRAL SERVER SEARCH AND WILDCARDS

** Please note that the above screenshot is a sample of a previously delivered solution and the final user interface design will be specified during project specification workshops.*



Central Server

Search - Request

View Search Fields

Find

List view style ensures minimal training time and ease of use

	ID	Created	Issued	Expires	Status	Type	Name	Birth	DN
■	00216000263	05/11/2016	05/11/2016	05/11/2021	Pending	Class D Instruction Permit - Under 21	STI#2 STI-1-002-2	01/01/2003	4DAD21924
■	00215000264	05/11/2016	05/16/2016	05/21/2021	Pending	Class D Instruction Permit - Under 21	STIM CTIM-002	[illegible]	4DAD21923
■	02316000269	05/11/2016	05/11/2016	05/21/2021	Pending	Commercial Driver's License - 21+	Ducky, Duck	07/13/1953	4DAD21922
■	02116000239	05/11/2016	05/07/2016	05/21/2021	Pending	Class D Driver's License - 21+	Ducky, Duck	07/12/1990	4DAD21921

FIGURE 39: SEARCH RESULTS LISTING AND ORDERING CONTROLS

** Please note that the above screenshot is a sample of a previously delivered solution and the final user interface design will be specified during project specification workshops.*

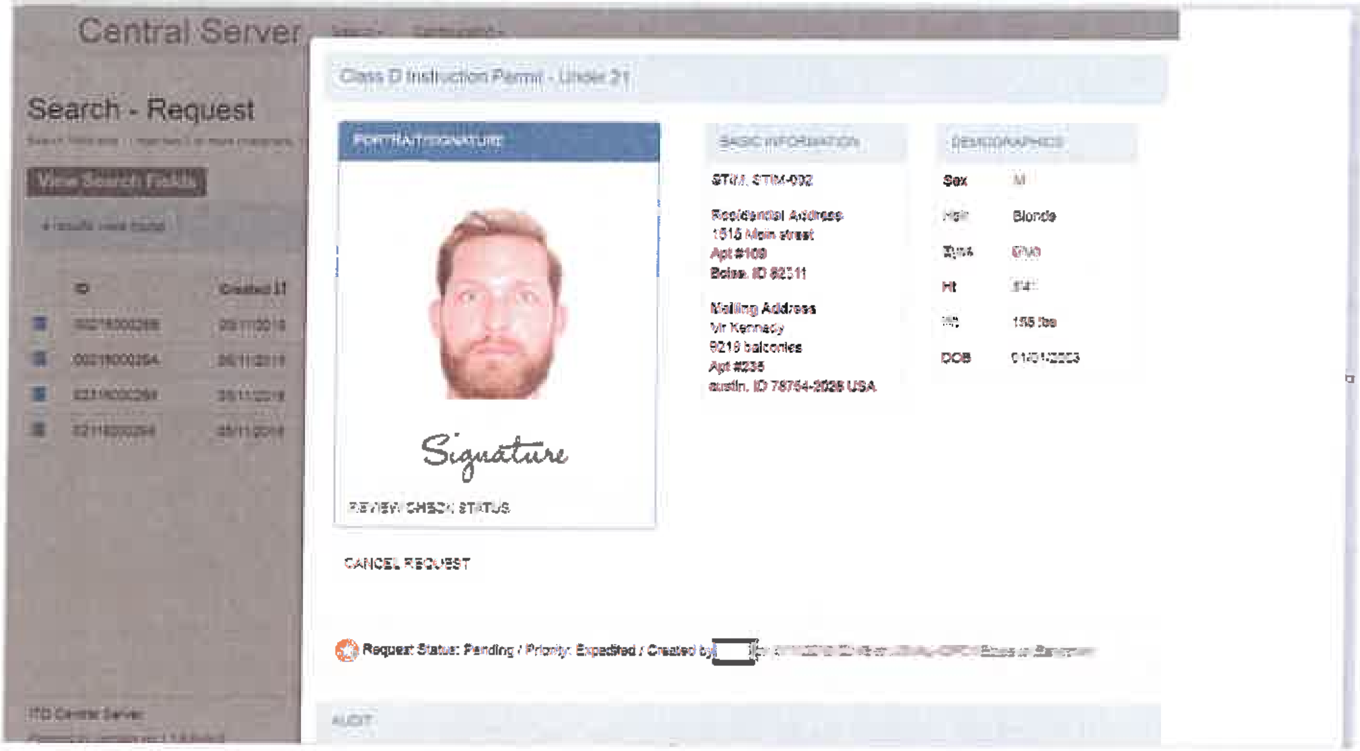
Results are returned in a list view style that is common with existing Windows user interfaces for familiarity and use. Sort buttons are represented by easily recognizable icons above each column.

4.12.1.2 How the application can allow for easy navigation between the search results list, individual detail records, and back to the search results list without searching again.

VENDOR RESPONSE:

Gemalto confirms that easy navigation between search result lists and individual result lists is allowed in all web based modules of our solution including the following modules:

- Web Reporting System (WRS)
- Central Server (CS) administration module
- Biometric Investigative Workstation (BIW)



Class D Instruction Permit - Under 21

STIM, STIM-002

Residential Address
1515 Main street
Apt #109
Boise, ID 83311

Mailing Address
Mr Kennedy
9219 balconies
Apt #235
austin, ID 78754-2035 USA

Sex	M
Hair	Blonde
Eyes	[illegible]
Ht	[illegible]
Wt	155 lbs
DOB	[illegible]

Request Status: Pending / Priority: Expedited / Created by [redacted]

FIGURE 40: INDIVIDUAL CARD ISSUANCE RECORD DETAILS

** Please note that the above screenshot is a sample of a previously delivered solution and the final user interface design will be specified during project specification workshops.*

4.12.1.3 How the record detail screen can default to display data for the most recent issuance but allow selection of detail for historical issuances.

VENDOR RESPONSE:

Gemalto confirms that record search results display data from the most recent issuance but additional details for historical issuances are available when the individual record is selected. This is a standard feature of our solution.

Section 4, Subsection 4.12.2 - Vendor should describe how their proposed solution will recover after power outages or communication failures. This description should include:

VENDOR RESPONSE:

Gemalto's solution has been designed with robustness and reliability in mind. Our Image Capture Workstations (ICW) has been designed to manage power and communication failures and to recover without a loss of data. We also have included APC Uninterruptable Power Supplies (UPS) so that power surges or loss of power will not prevent our ICW from saving data to be synchronized after power returns.

4.12.2.1 How in-process transactions in system queues will be able to restart.

VENDOR RESPONSE:

Gemalto confirms that in the event of power failure, in process transactions will be started without loss of transaction data, software settings will return to previous conditions, and the application software will restart at the point displayed prior to the power failure. In addition, all required audit and statistical data will be maintained and continue to function as if no interruption occurred.

To mitigate against power loss, uninterrupted power supplies (UPS) should be provided by the State datacenter. Gemalto's Central Server (CS) solution is capable of performing structured shutdowns in the event of power loss. Our system is designed so that UPSs may communicate with our server and notify the server when five minutes of power remain which triggers the servers to safely shut down instead of crashing which ensures all required audit and statistical data will be maintained and continue to function as if no interruption occurred. This also ensures that all settings and statuses will be maintained in the event of power failure.

4.12.2.2 How the system will roll back, if a transaction cannot be restarted.

VENDOR RESPONSE:

Gemalto's Image Capture Workstation (ICW) has been designed to seamlessly handle rollbacks if transactions cannot be restarted. Our solution has been designed to write over partial incomplete transactions in the event that the transaction cannot be restarted. In this scenario, users are presented with a prompt to confirm that the user would like to overwrite a failed transaction.

4.12.2.3 How pending data will be stored locally and uploaded to the image server, once power or communication is restored.

VENDOR RESPONSE:

Gemalto has also designed its Image Capture Workstation (ICW) to manage power failure scenarios. Software settings for our ICW are maintained in a separate configuration file so they will not be affected by a loss of power and will return to the previous status when restarted. Transactional data is also maintained in the event of a power loss or loss of communication with the Central Server. Captured transactional data is locally stored, in an encrypted format, until connectivity to the Central Server is restored and successful transmission is confirmed. When the ICW is restarted, users may be given the option to continue the current transaction or to start a new transaction and save the previous transaction as incomplete.

Section 4, Subsection 4.12.3 - Vendor should describe how their proposed solution will handle Review and Fraud Case Management. This description should include:

VENDOR RESPONSE:

Gemalto has created an advanced Facial Recognition System (FRS) that provides our customers with fraud identification at all critical points during applicant processing. The system is being used in multiple jurisdictions with great success. Law enforcement personnel find it very intuitive and easy to use, while providing an extremely powerful set of tools for fraud detection. We will be replacing the current biometric engine used by West Virginia to a more advanced engine that takes advantage of a new advanced in-house owned algorithm from Gemalto Cogent (Also used by other US Agencies such as the Department of Homeland Security).

Gemalto Cogent continues to expand its position as a leading innovator in the biometrics industry as part of its avid commitment to R&D. Throughout regular participation in NIST testing, Gemalto Cogent algorithms consistently rank within the top-tier results for finger, face, and iris, due in large part to advances drawn from our focused research and development.

The National Institute of Standards and Technology (NIST) identified Gemalto Cogent as a "Leading Commercial Supplier of Facial Recognition technology" following the conduct of their 2013 Facial Recognition Vendor Test (FRVT) evaluation.

The test evaluated face recognition algorithms from 17 participants around the world through three submission phases. The face identification test exercises 1:N searching on different data sets, including mugshots, visa photos, webcam photos. The NISTIR 8009 final report, published in May 2014, established Gemalto Cogent as a "Leading Commercial Supplier" along with four other vendors.

All applicants processed throughout the day are sent to a One-To-Many process where each photo is compared against all other photos in the DMV image database. Photo matches exceeding a configured threshold (numerical scores not within configured limits) are flagged and added to a secondary screening case list that requires further investigation within our Biometric Investigative Workstation (BIW).

The FRS is designed for very easy integration into any IT environment. Its design advantages are described below.

Facial Recognition System (FRS) Design Advantages

Gemalto's FRS has the distinct advantage of being modular in design. The "case creation" processes have been isolated from the "investigation tools" by a layer we call the Biometric Deduplication System (BDS). This allows any biometric (or non-biometric) process to be used to generate potentially fraudulent cases. It also allows multi-biometric processes to be utilized together for case creation. Simply put, this approach allows any case generating process to be used as long as it follows simple guidelines pertaining to case creation. Once a case is created, regardless if it was created from facial recognition or anything else, an investigator has all the tools required to resolve the case.

The system currently supports mulit-modal biometrics, facial recognition, fingerprint matching and iris matching. As new biometrics become more accepted, they can easily be added. Scores can also be created using a compound matching score, Biometric Fusion.

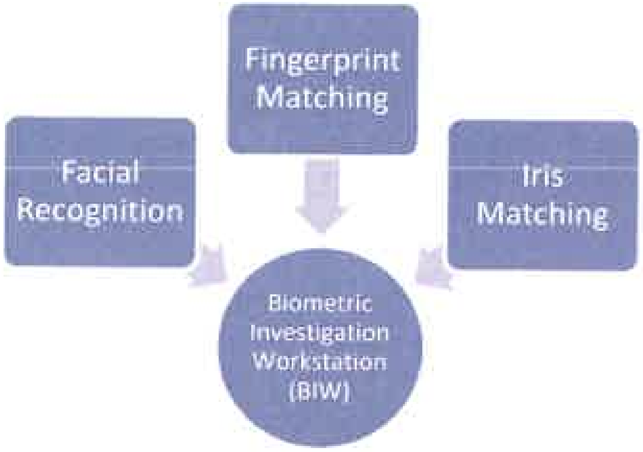


FIGURE 41:FRS SYSTEM DESIGN

Standard Case Creation Process (Nightly 1-N Batch)

The Gemalto case creation process is built upon industry-leading matching algorithms. These serve as the building blocks for an extremely robust FRS. Although most FRS case creation processes are very similar, there are always subtle differences required by each customer. Gemalto will never try to "shoe-horn" a solution into a customer's program. We will take the time to define and design a custom tailored solution specifically for West Virginia. We also understand that the case creation process must be fine-tuned over the initial months of the program, to work as expected. Gemalto will work closely with the DMV to refine this process until it functions as desired.

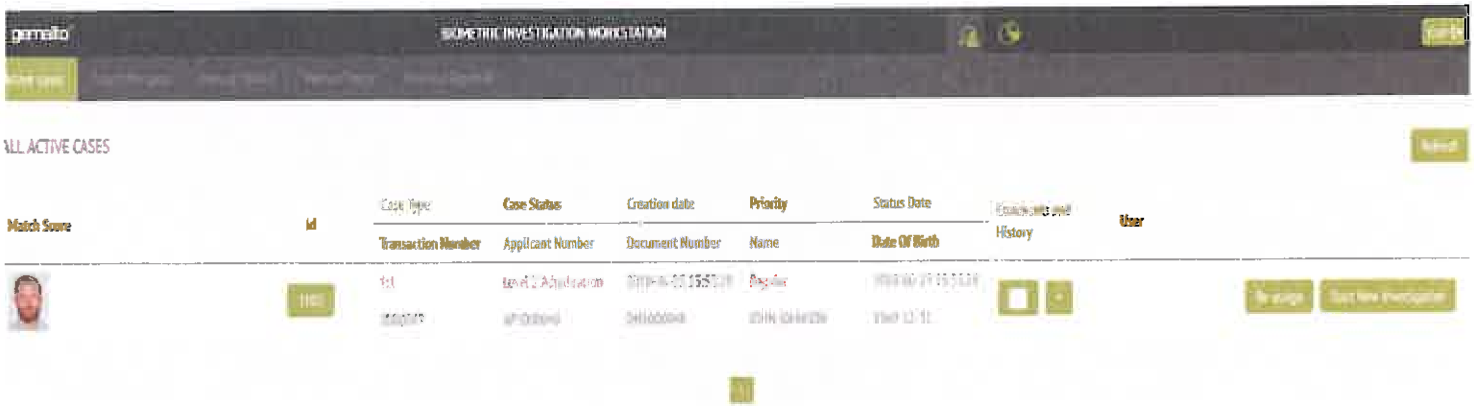
Biometric Investigation Workstation (BIW)

The BIW is an advanced, fully functioned, web-enabled toolbox containing all functionality needed to investigate and adjudicate all possible fraudulent applicants. The BIW is only available to authorized personnel, from authorized workstations. In addition to providing case management and workflow queueing tools, the BIW provides team members the ability to investigate potential cases of fraud.

Case Management

Gemalto's BIW generates "match lists" as required by the DMV. These are automatically created and displayed as the default view, in descending match percent order, when a case is opened. Match list filtering and sorting may be performed against any data captured by our solution i.e. sort by capture date, location, etc. Gemalto will work with the DMV during the planning phase to clearly define all requirements related to separate and priority workflows, case views, sorting and assignment (Users with Supervisor roles are able to assign and reassign cases to team operators, it is also possible to have the

Supervisor receive cases inspected by their team for the purposes of quality and vetting new team members). We have included an example screenshot of the default view for new cases below.



ALL ACTIVE CASES

Match Score	Id	Case Type Transaction Number	Case Status Applicant Number	Creation date Document Number	Priority Name	Status Date Date Of Birth	Comments and History	User
	[illegible]	1:1 [illegible]	Level 2 Adjudication [illegible]	[illegible] [illegible]	Regular [illegible]	[illegible] [illegible]		

FIGURE 42: BIOMETRIC INVESTIGATIVE WORKSTATION - CASE LIST

** Please note that the above screenshot is a sample of a previously delivered solution and the final user interface design will be specified during project specification workshops.*

Investigative Tools

Gemalto's Facial Recognition System (FRS) and accompanying Biometric Investigative Workstation (BIW) include many tools for investigators to assist in confirmation of potential matches. Cases may be examined using several different tools as illustrated and described below.

In this example, the two images are fused together across an adjustable line. Differences in facial structure become very apparent i.e. the lengths of the noses may be different between the individuals. Images may be fused vertically, horizontally, or even diagonally. In the below example, you can see two siblings. While they share many similar traits, the investigative tools highlight subtle differences like facial structure and eye color.

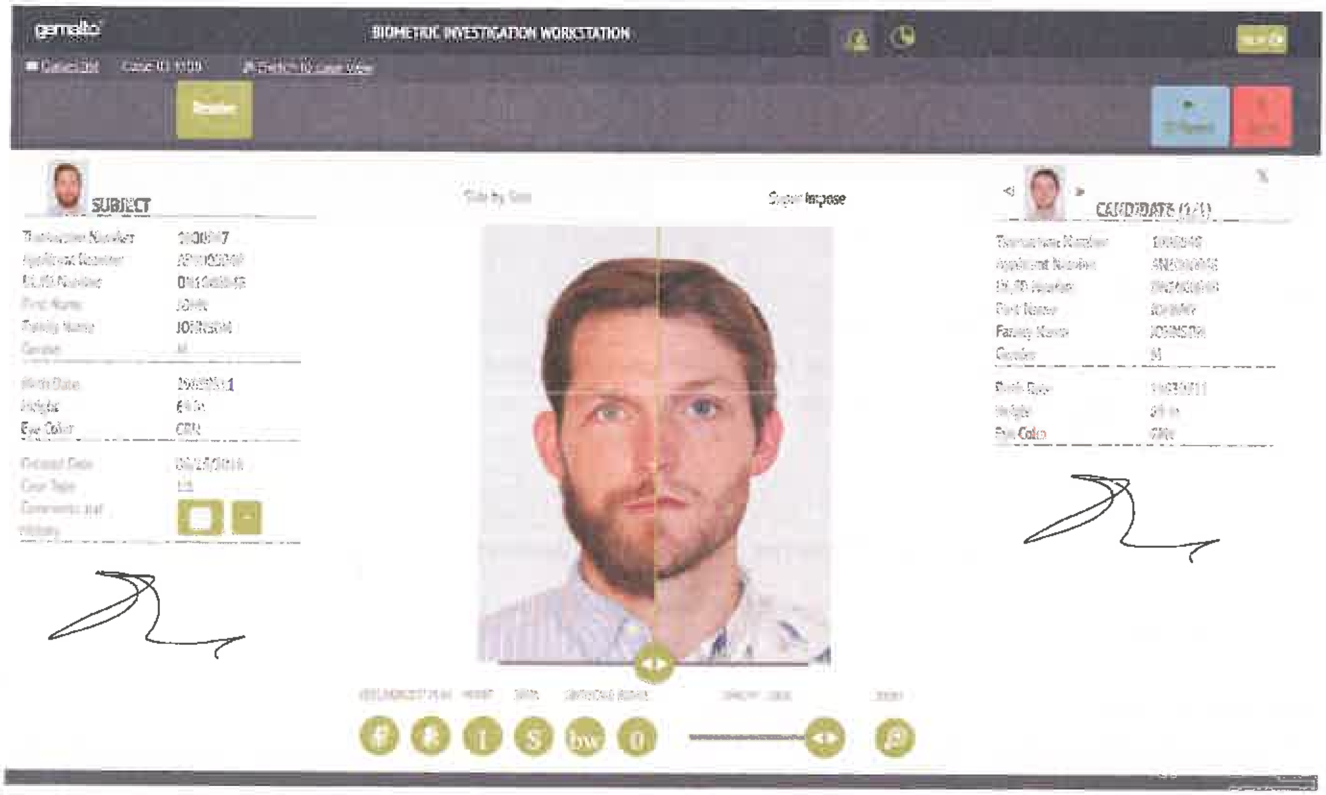


FIGURE 43: BIOMETRIC INVESTIGATIVE WORKSTATION - INVESTIGATOR VIEW

** Please note that the above screenshot is a sample of a previously delivered solution and the final user interface design will be specified during project specification workshops.*

In the above view, the following additional tools are available by clicking the corresponding icon:
Horizontal/Vertical View. Displays the split images vertically (default) or horizontally. Split the images vertically and the bar moves from left to right. Split the images horizontally and the bar moves from top to bottom.

- **1st Plan.** Swaps images left to right and right to left.
- **Invert.** Inverts the images to negative color.
- **Sepia.** Applies a sepia tone to the images.
- **Greyscale.** Applies a greyscale tone to the images.
- **Rotate.** Rotates the images as selected.
- **Opacity.** Applies an opaque filter to images as selected. Set opacity to 0 and the subject photo is fully transparent. Set it to 100 and the candidate photo is fully transparent.
- **Zoom.** Launches a magnified window of the images.

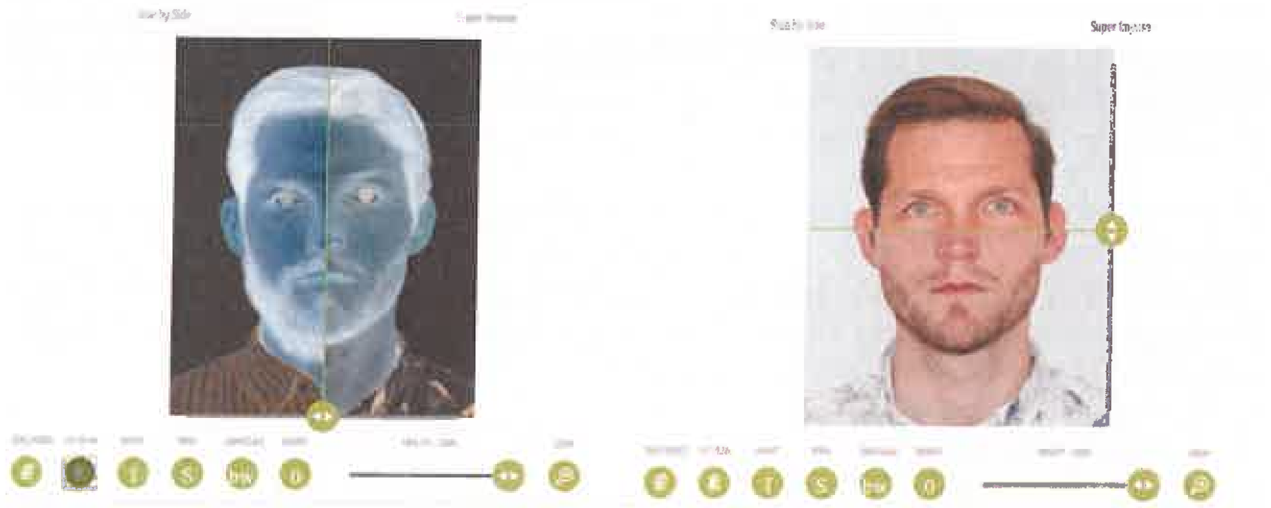


FIGURE 44: BIOMETRIC INVESTIGATIVE WORKSTATION - INVERTED AND ROTATED FUSE

** Please note that the above screenshot is a sample of a previously delivered solution and the final user interface design will be specified during project specification workshops.*

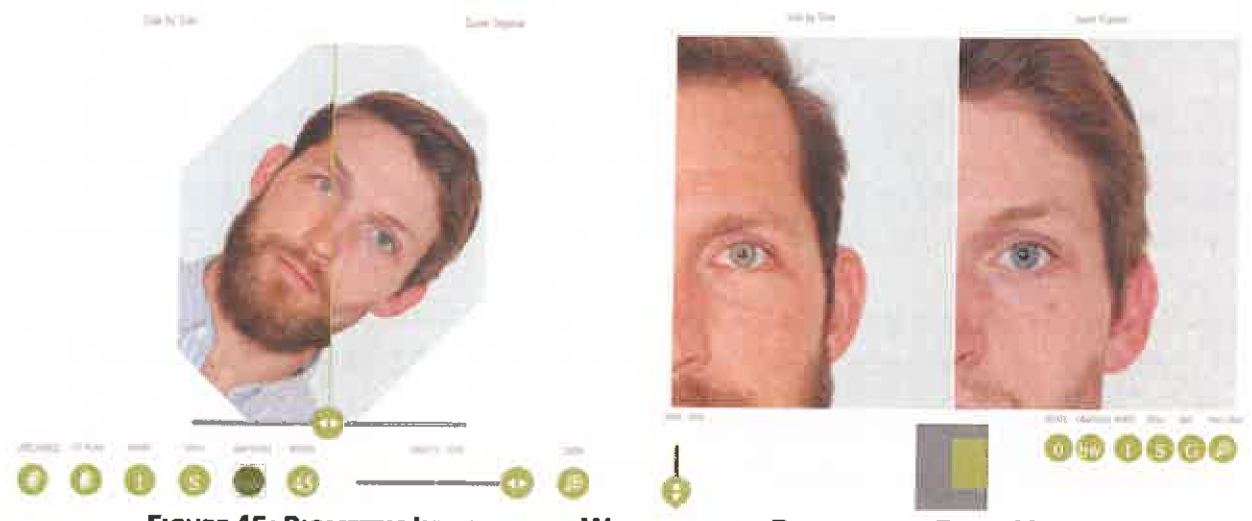


FIGURE 45: BIOMETRIC INVESTIGATIVE WORKSTATION - ROTATED AND ZOOM VIEWS

** Please note that the above screenshot is a sample of a previously delivered solution and the final user interface design will be specified during project specification workshops.*

BIW Reporting

Reporting specific to the BIW and FRS may be performed in two locations within Gemalto's solution. Standard and ad-hoc reports for all components of the solution may be viewed and run within the Web Reporting System (WRS) as described in the response to Appendix I.

In addition to the WRS, reporting and search functionality specific to cases and case management are conveniently located within the BIW. This functionality allows supervisors to view details and statistics about specific cases or operators in addition to allowing the supervisor to review cases that have been open too long or to re assign cases. Our BIW also includes a supervisor dashboard allowing managers to view the status of operations in real time including:

- Number of open cases
- Average time to solve a case
- Average of resolved cases per day
- Duplicates count
- Duplicates percentage

4.12.3.1 How the solution can provide a multi-tiered workflow for the manual review of match and non-match records, including priority queues,

VENDOR RESPONSE:

Gemalto's Biometric Investigative Workstation (BIW) can populate separate candidate review lists for user adjudication for 1:1, 1:N, and any other flagged transactions. Our solution allows for multiple workflows that can be configured to meet the business rules and requirements of the DMV including priority queues to ensure that expedited transactions are cleared in time for timely card production.

Records which have been manually or automatically flagged for secondary review are held in an "under review" state until the flag is removed or forwarded to senior investigations/supervisors for further investigation (depending on DMV processes and business rules). All business processes, within our BIW and overall solution, are configurable and will be defined with DMV during the planning phase of the project along with all required interfaces with State systems.

It should be noted that we have implemented a process in other jurisdictions that allow a designated person(s) to quickly review cases to ensure that investigators are spending their time on cases that truly require their attention. We can review this step/process with the DMV during our planning phase.

4.12.3.2 How all expedited records that have matches can go to a separate priority queue for same day manual review.

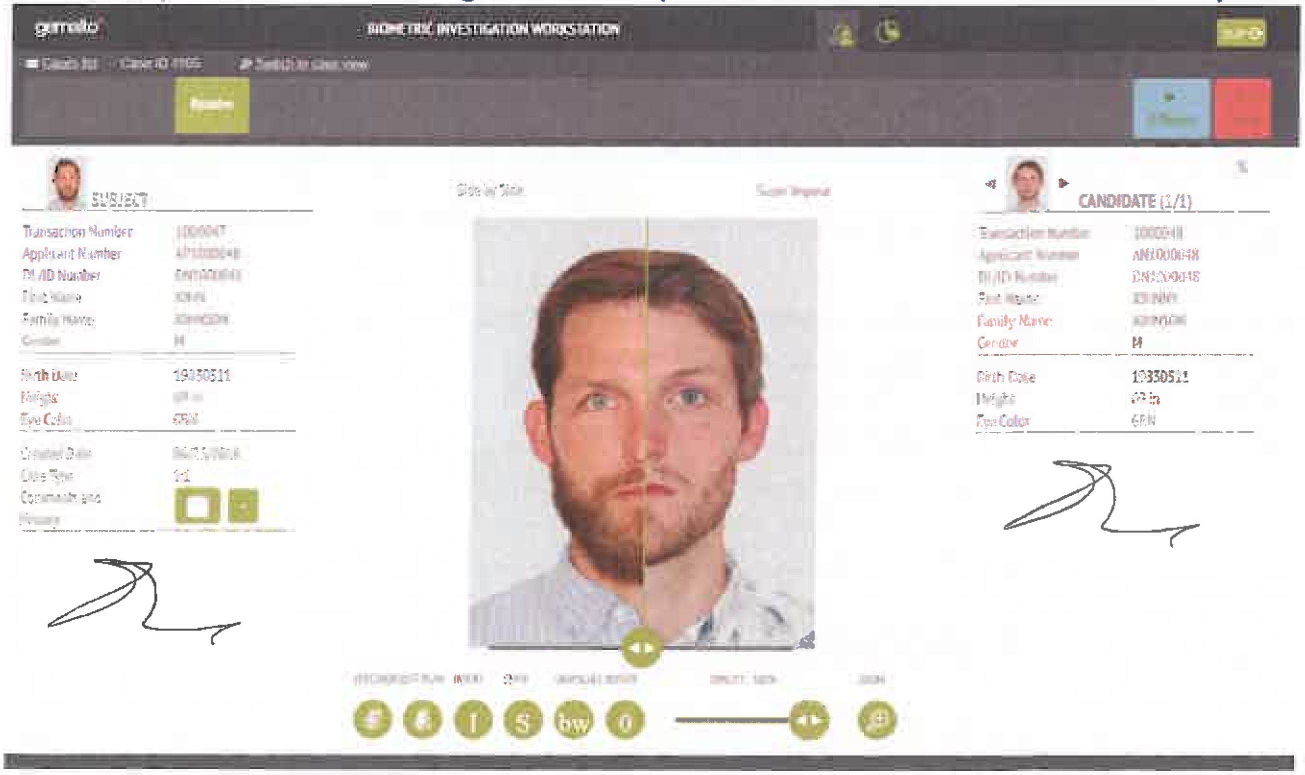
VENDOR RESPONSE:

Gemalto confirms that, as described above, expedited or priority queues and workflows are supported within our Biometric Investigative Workstation. All business processes, within our BIW and overall solution, are configurable and will be defined with DMV during the planning phase of the project along with all required interfaces with State systems.

4.12.3.3 How all match and non-match records can display the facial image, signature and demographic information formatted in such a way as to highlight the differences in data between the records.

VENDOR RESPONSE:

Gemalto confirms that both match and non-match records are displayed in a manner that allows investigators to easily compare facial image, signature and demographic data. Our Biometric Investigative Workstation (BIW) includes and advanced tools display portraits and demographic data in an intuitive layout that allows investigators to clearly see the differences between the two subjects.



SUBJECT

Transaction Number	1000047
Applicant Number	[illegible]
DL/ID Number	[illegible]
First Name	JOHN
Family Name	JOHNSON
Gender	M
Birth Date	19330511
Height	[illegible]
Eye Color	GRN
Created Date	[illegible]
Case Type	1:1
Comments and History	

CANDIDATE (1/1)

Transaction Number	1000048
Applicant Number	AN1000048
DL/ID Number	DN1000048
First Name	JOHN
Family Name	JOHNSON
Gender	M
Birth Date	19330521
Height	62 in
Eye Color	GRN

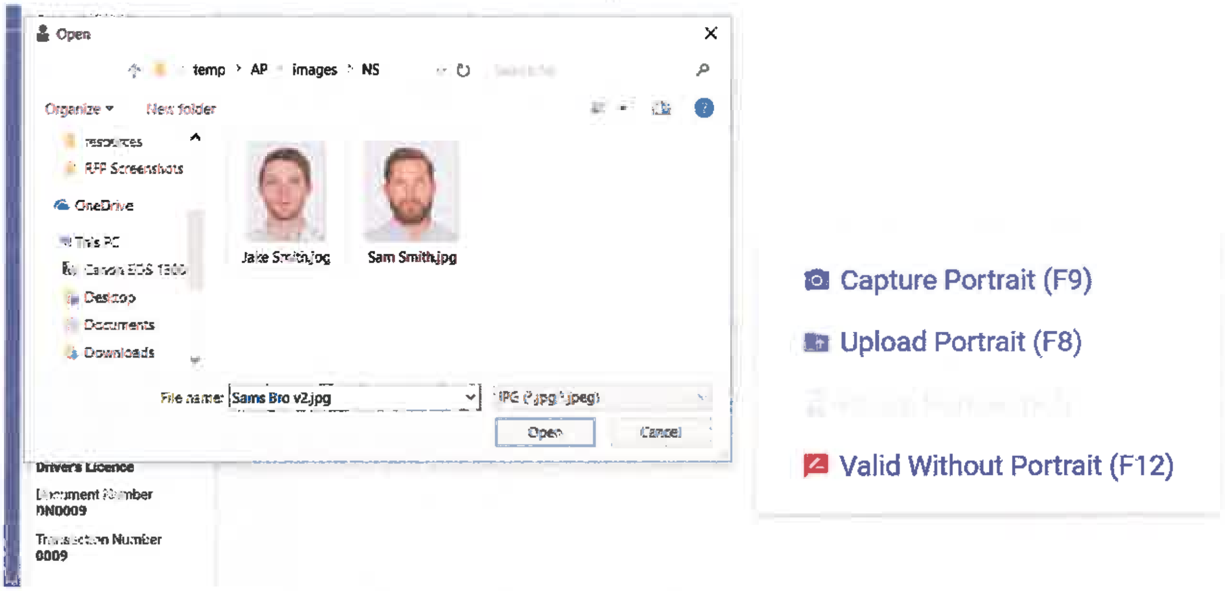
FIGURE 46: BIOMETRIC INVESTIGATIVE WORKSTATION - INVESTIGATOR VIEW

** Please note that the above screenshot is a sample of a previously delivered solution and the final user interface design will be specified during project specification workshops.*

Section 4, Subsection 4.12.4 - Vendor should describe how the proposed solution will manage manual image enrollment applications. This description should include:

VENDOR RESPONSE:

Gemalto confirms that our solution is able to manually upload images that were not captured by the Image Capture Workstation (ICW) as illustrated below or within our Biometric Investigative Workstation (BIW) for fraud investigation purposes. Please note that manually uploaded images within our ICW are still subject to ICAO and 1:1/1:N checks by default within our solution.



File name: Sams Bro v2.jpg

Driver's Licence

Document Number
DN0009

Transaction Number
0009

FIGURE 47: IMAGE CAPTURE WORKSTATION - MANUAL UPLOAD

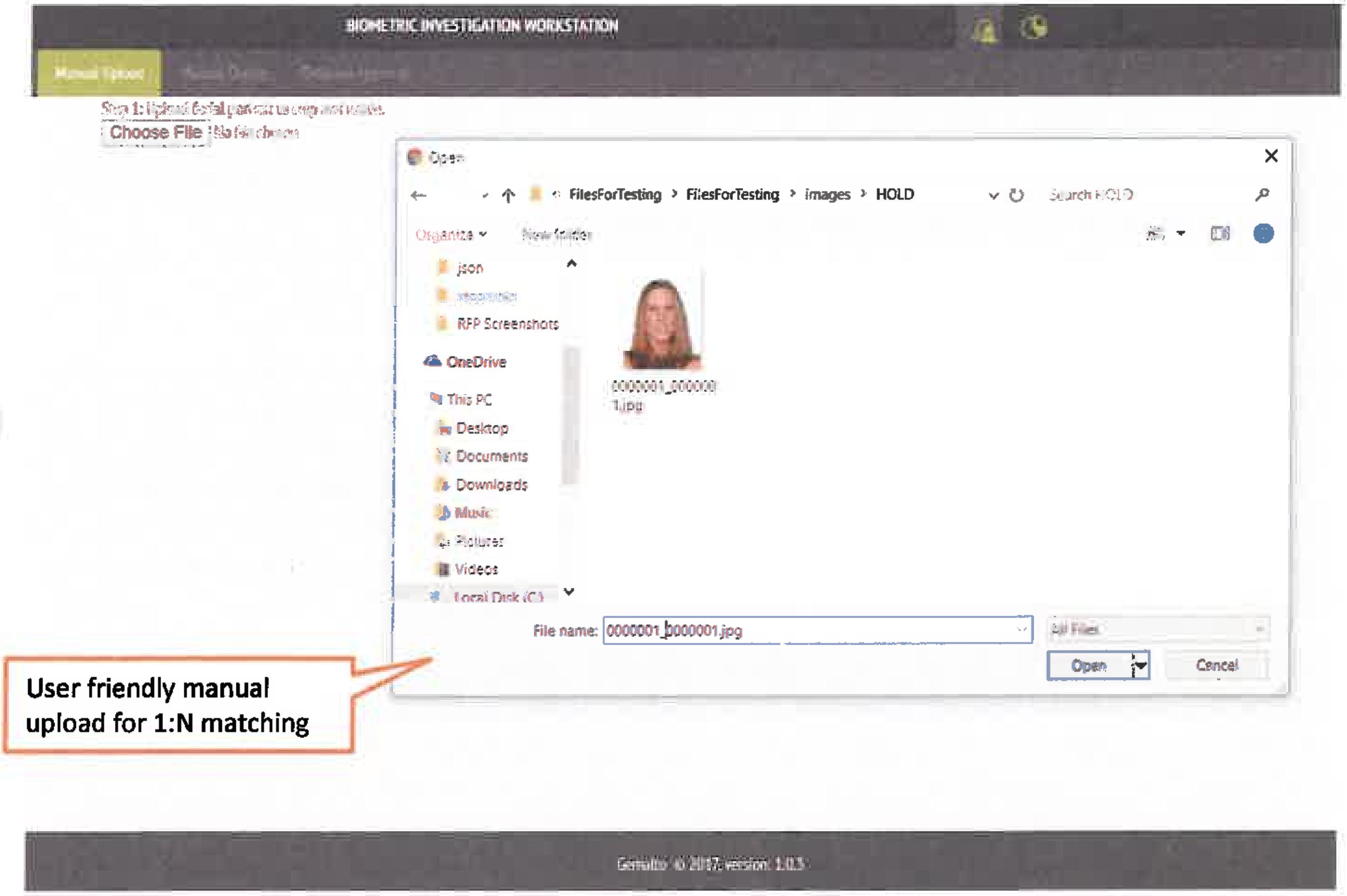
** Please note that the above screenshot is a sample of a previously delivered solution and the final user interface design will be specified during project specification workshops.*

It should be noted that our ICW supports manual uploading of images for special scenarios like deployed soldiers or priority issuances. This feature may be disabled or restricted to priority users if required by the State.

4.12.4.1 How the Vendor solution will allow images that were not captured by the image and signature capture workstation to be uploaded to the system for comparison against images in the database.

VENDOR RESPONSE:

As described above, Gemalto confirms that images may be manually uploaded to our Biometric Investigative Workstation (BIW) in order to perform manual 1:N biometric comparisons as illustrated below:



User friendly manual upload for 1:N matching

Figure 48: Biometric Investigative Workstation - Manual Upload / Search

* *Please note that the above screenshot is a sample of a previously delivered solution and the final user interface design will be specified during project specification workshops.*

4.12.4.2 How the system will allow images of various file types to be uploaded into the manual enrollment application, including JPG, GIF, TIF, PNG, and BMP.

VENDOR RESPONSE:

Our solution has designed to be flexible in nature and we use standardized and common file formations whenever possible. Gemalto confirms that our solution currently supports manual uploading and enrollment of the following image file types:

- JPG,
- GIF,
- TIF,
- PNG,
- And BMP.

4.12.4.3 How the system will allow user to choose to keep uploaded images permanently enrolled in the facial recognition system with appropriate demographic data.

VENDOR RESPONSE:

Gemalto confirms that manually uploaded images may be permanently enrolled into the facial recognition system with any appropriate demographic data. After a user has uploaded an image into the Biometric Investigative Workstation (BIW), they can save the enrolled image into an alias that resides in the Facial Recognition System (FRS). After enrollment into the FRS, all citizens enrolled into the ICW are compared against the manually enrolled alias in addition to all other portraits in the FRS. Flags and matches behave in the same manner for manually enrolled images as they do for images enrolled through the ICW.

This functionality can also be integrated with a photo first process in our Image Capture Workstation through our photo first "Watch List" feature which is currently being implemented for the State of Colorado. If an applicant enters a DMV location and the operator believes the applicant to be suspect, the operator can immediately and quickly place the applicant on the Watch List. Placing an applicant on the Watch List will automatically push the photo and relevant information to all Photo First stations across the State to provide protection in the event that the applicant tries to visit other offices.

Section 4, Subsection 4.12.5 - Vendor should describe the applications reporting capabilities, including description and examples of all standard system reports. This description should also include:

VENDOR RESPONSE:

Gemalto's Web Reporting System Interface (WRS is based on SQL Server Reporting Services) provides easy access to standardized reports and live embedded, interactive dashboards. This provides a high level dashboard for any events DMV wishes to track whether monitoring customer processing times or tracking Gemalto's performance vis a vis SLA's. Gemalto's Central Server (CS) solution logs a comprehensive set of application/user activity event data encompassing the entire card issuance process. CS is responsible for the secure storage (i.e., integrity of the application and user activity log data and access rights/restrictions), and query and reporting functionality of this data.

The system currently contains many reports that are standard for most jurisdictions. During the planning phase of the project, Gemalto will work with the DMV to jointly define all custom reports required for the State of West Virginia. By default, Gemalto's Web Reporting System (WRS) provides a very rich set of search and query functionality (i.e., search and ad-hoc reporting functionality) in addition to running scheduled "standard" or "canned" reports as part of the Central Server offering. There are a variety of output formats available to DMV for each report including DOC, PDF, XML, CSV, and HTML.

Microsoft's SSRS has been included within this offer to provide the required reporting functionality. Due to the varying technical requirements, our system has been designed to remain agnostic towards reporting engines but we have had experience with multiple engines including Crystal Reports and Tableau. Business Intelligence requirements may be explored in more detail during the planning phase.

Gemalto will work with DMV during the planning phase of the project to refine the data and actions that should be stored and accessible within our Web Reporting System (WRS). Events are logged by each application and then stored in Gemalto's Central Server. Each user event contains at a minimum:

- the UserID of the user logged in to the application,
- timestamp of the event,
- the workstation identifier/name (as reported by the application or web browser), the application identifier,
- the System action identifier,
- and any action-specific data consisting of a customer identifier (e.g. customer number) and/or
- Issuance or Production Record ID

Central Server logs entries for the following subsystems:

- Image Capture Workstation (user enrollment)
- Biometric Investigation Workstation / Facial Recognition System (facial recognition and case management)
- Central Server (the issuance workflow engine and management application)
- Production Manager (production management for central issuance)

Please note that additional logging and reporting may be included based on the Requirement Specifications (RQS) submitted to DMV for approval by Gemalto during the planning phase of the project. For example, we can also log activity within our Web Reporting System (WRS)

During the design phase of your program, Gemalto will work with the DMV to jointly define a specific number of custom standard reports required for the State of West Virginia including the following at a minimum:

- Activity logs/daily transactions;
- Reconciliation reports;
- Image reports for failed images;
- Cards issued;
- Credentials flagged for additional review;
- Statistical analyses; and
- Standard pre-defined management reports.

4.12.5.1 How, in addition to any standard reports the solution offers, proposal should allow Agency to add a determined number of custom reports at no additional charge over the life of the contract.

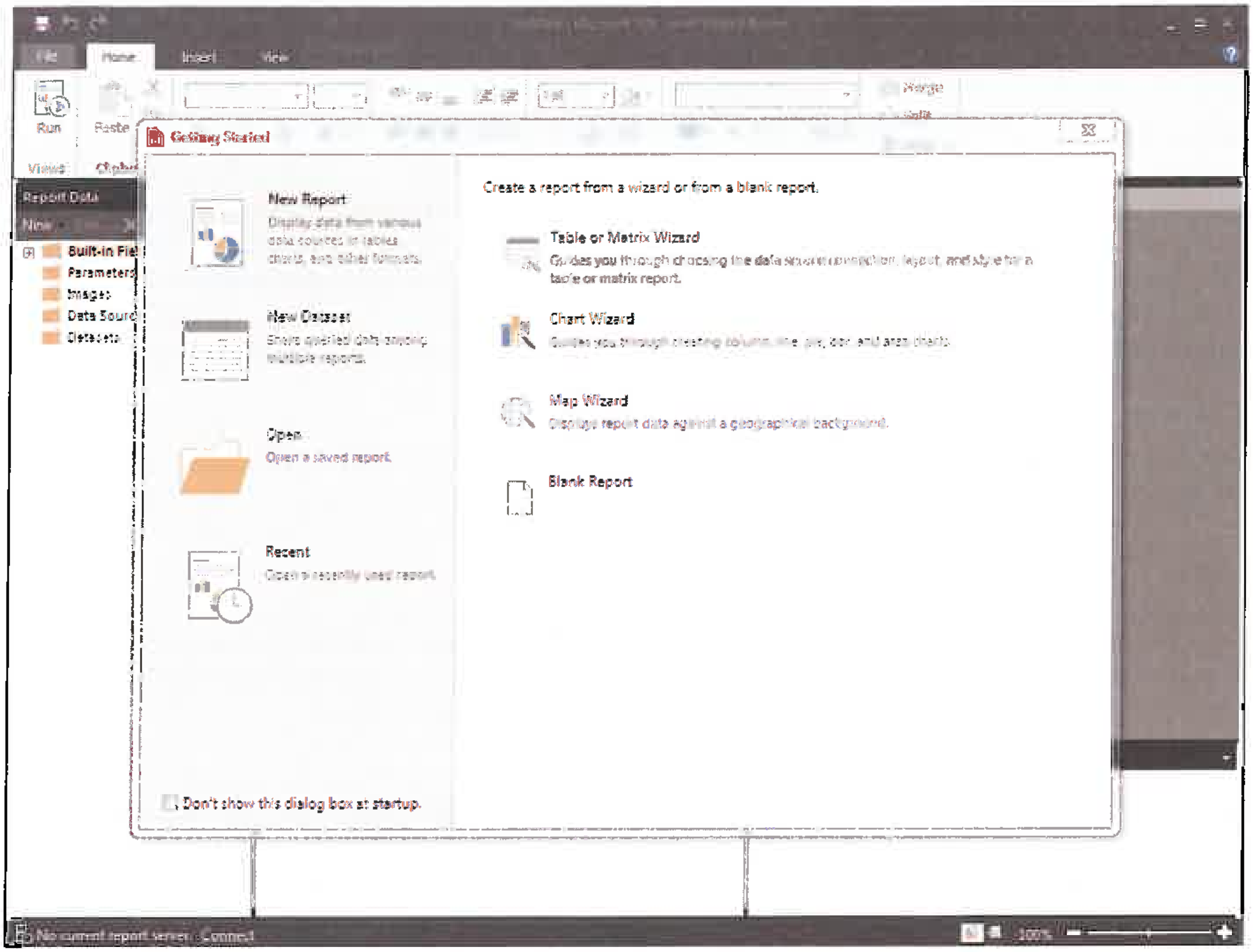
VENDOR RESPONSE:

During the design phase of your program, Gemalto will work with the DMV to jointly define 50 custom standard reports required for the State of West Virginia. In addition, we have included an additional 5 reports per year at **no cost** to the State. This will be managed as "free" change requests and should follow the change request process.

4.12.5.2 How can the Agency generate custom ad hoc reports?

VENDOR RESPONSE:

As described above, Microsoft's SSRS has been proposed within this offer to provide the required reporting functionality. Included with this is Microsoft Report Builder. Report Builder is a tool for authoring paginated reports. When you design a paginated report, you're creating a report definition that specifies where to get the data, which data to get, and how to display the data. When you run the report, the report processor takes the report definition you have specified, retrieves the data, and combines it with the report layout to generate the report.



Getting Started

New Report
Display data from various data sources in tables, charts, and other formats.

New Dataset
Share queried data among multiple reports.

Open
Open a saved report.

Recent
Open a recently used report.

□ Don't show this dialog box at startup.

Create a report from a wizard or from a blank report.

Table or Matrix Wizard
Guides you through choosing the data source connection, layout, and style for a table or matrix report.

Chart Wizard
Guides you through creating column, line, pie, bar, and area charts.

Map Wizard
Displays report data against a geographical background.

Blank Report

FIGURE 49: SSRS REPORT BUILDER

Gemalto has also included in our proposal Microsoft SSRS training for four (qty. 4) WV DMV staff to ensure that the DMV is able to effectively capitalize on their reporting functionality.

4.12.5.3 How reports displayed for view on the screen can be printable and properly formatted.

VENDOR RESPONSE:

Microsoft SSRS Report Building is designed to create both interactive and paginated reports which help to ensure that the custom(ad-hoc) or standard (canned) reports are properly formatted for their intended use (printed or web based). . Formats include HTML, MHTML, PDF, XML, CSV, TIFF, Word, and Excel.

4.12.5.4 How the report data can be displayed on screen in such a way as to limit the need to navigate through multiple pages.

VENDOR RESPONSE:

Reports with Gemalto's Web Reporting System (WRS) are designed to scroll so that there is no need to navigate through multiple pages. In addition, Gemalto designs our reports with layout and functionality in mind so that the appropriate data is included but they are not unnecessarily long or hard to read. Gemalto will work with the DMV during project delivery to clearly define report content and layouts and submit our 60 standard reports to the DMV for approval to ensure the State's requirements are met.

Section 4, Subsection 4.12.6 - Vendor should return a confirmation file to the Agency upon receipt of the standard production print files.

VENDOR RESPONSE:

Gemalto confirms that our solution will return a confirmation file to the Agency upon receipt of the standard production print files. Gemalto will work with the agency during the planning phase of the project to clearly define the confirmation file format and method of transition.

Section 4, Subsection 4.12.7 - Confirmation files should include the number of print requests received for validation by the Agency against the number of print requests sent.

VENDOR RESPONSE:

Gemalto confirms that the confirmation file returned to the Agency will include the number of print requests received for validation by the agency against the number of print requests sent. Gemalto also recommends the use of a cryptographic signature or check-sum during the transmission of the production requests. This helps ensure that no only were the correct number of records received but it also allows us to ensure that files were not altered or intercepted during transmission.

SYSTEM ADMINISTRATION

Section 4, Subsection 4.13 - User Account Management

Section 4, Subsection 4.13.1 - Vendor should describe the account management functions as part of their system administration module. This description should include:

VENDOR RESPONSE:

User sign-on profiles and status are kept on the Gemalto Central Server (CS) and are typically integrated with State active directories. This allows us to control simultaneous login capabilities. Additionally, these profiles can be updated from a single location as needed. Integration with the State's active directory helps deter users from sharing accounts as there is not a separate username and password to remember and there are not separate steps involved in logging into the system and system login is as simple as signing into windows and does not add any extra time to the process.

Login integration is done in accordance with West Virginia IT policies and will be defined during the planning phase of the project plan. In addition, by integrating with the State's active directory, we are able to maintain password policies, auto-logoff times, or any other IT security policies defined by the State. If integration with the State's Active Directory is not possible, a separate Active Directory can be provided by Gemalto.

4.13.1.1 How you may view last login date/time for each user.

VENDOR RESPONSE:

Gemalto's Central Server (CS) solution logs a comprehensive set of application/user activity event data encompassing the entire card issuance process. CS is responsible for the secure storage (i.e., integrity of the application and user activity log data and access rights/restrictions), and query and reporting functionality of this data. This data is viewable thought Gemalto's Web Reporting System (WRS)

4.13.1.2 How to manage user permissions.

VENDOR RESPONSE:

Gemalto confirms that access to certain components of our solution may be restricted through Active Directory. This is typically managed by various groups so that the DMV can manage access or revoke users if they leave their job or do not have the appropriate security clearance. Application permissions are Active Directory role based and configured through Central Server.

4.13.1.3 How the ability to view partial or full SSN data in all applications will be achieved based on permissions or role.

VENDOR RESPONSE:

Gemalto confirms that our solution can let users view partial or full SSN data dependent on the user's permissions (Granular Permission) or role (Windows AD Group). Access restrictions are managed within Active Directory user groups as described above. If this data is to be stored within our solution hosted at WVOT, we would recommend that it is secured with column level encryption within the database to ensure that additional permissions are required to access this data.

Section 4, Subsection 4.14 - System Usage Dashboard

Section 4, Subsection 4.14.1 - Vendor should describe how the system administration module may display the current view of system usage including items such as:

VENDOR RESPONSE:

As described in the above response to "Section 4, Subsection 4.12.5", Gemalto's Web Reporting System (WRS) provides easy access to standardized reports and **live embedded, interactive dashboards.** This provides a high level dashboard for any events DMV wishes to track whether monitoring customer processing times or tracking Gemalto's performance vis a vis SLA's. Gemalto's Central Server (CS) solution logs a comprehensive set of application/user activity event data encompassing the entire card issuance process. CS is responsible for the secure storage (i.e., integrity of the application and user activity log data and access rights/restrictions), and query and reporting functionality of this data.

Gemalto will work with the DMV during the planning phase of the project to clearly define and deliver customized dashboards to the State displaying key system usage statistics.

4.14.1.1 Number of users currently logged into FRS & ICW applications

VENDOR RESPONSE:

Gemalto confirms that our WRS Dashboard can display the number of users currently logged into the FRS (Biometric Investigative Workstation /BIW) and the Image Capture Workstation (ICW) application. Gemalto will work with the DMV during the planning phase of the project to clearly define and deliver customized dashboards to the State displaying the number of users currently logged in the FRS (Biometric Investigative Workstation/BIW) and ICW applications.

4.14.1.2 Number of records pending in all queues in FRS

VENDOR RESPONSE:

Gemalto confirms that our WRS Dashboard can display the number of records pending in all queries in the FRS (Biometric Investigative Workstation /BIW). Gemalto will work with the DMV during the planning phase of the project to clearly define and deliver customized dashboards to the State displaying the number of records pending in all queues in the FRS (BIW).

This information is also displayed within our BIW as illustrated below.

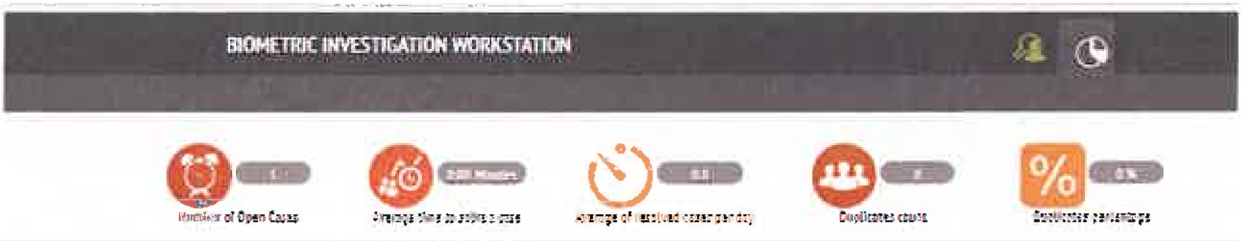

BIOMETRIC INVESTIGATION WORKSTATION
Number of Open Cases
Average time to solve a case
Average of resolved cases per day
Duplicates count
Duplicates percentage

FIGURE 50: BIOMETRIC INVESTIGATIVE WORKSTATION - STATUS DASHBOARD

** Please note that the above screenshot is a sample of a previously delivered solution and the final user interface design will be specified during project specification workshops.*

4.14.1.3 Central production facility statistics.

VENDOR RESPONSE:

Gemalto confirms that our WRS can display central production facility statistics. Card production reports is a common requirement and standard feature of our WRS. Our WRS and dashboards can include various breakdowns and drill downs of card production volumes including production by card type, date, "For Federal" vs non-Real ID, DL vs. ID, etc.

Section 4, Subsection 4.15 - Management of Central Issuance Records

Section 4, Subsection 4.15.1 - Vendor solution should allow for status queries on individual card print records.

VENDOR RESPONSE:

Gemalto's Web Reporting System (WRS) allows users to easily query the status of any credential transaction in real time. Transaction records may be queried and filtered by applicant name, address, transaction ID, dates, field office location, or any other field required by the DMV. We can provide a status bar within the query page of our WRS or provide a separate dashboard if required. An example of a status bar is provide below (please note this status bar indicates progress through the enrollment process). Our WRS also supports colorful and interactive dashboards which will be customized to meet the requirements of the DMV. Gemalto will provide a dashboard within our WRS with query functionality that allows the view of the status of any transaction as it moves through the DMV's required gates on to production. Gemalto will work with the DMV during the planning phase of the project to define all reporting and dashboard requirements.

Section 4, Subsection 4.15.2 - Vendor solution should allow for holds to be placed on individual card print records prior to the start of processing.

VENDOR RESPONSE:

Gemalto confirms that our solution allows for holds to be placed on individual card print requests prior to the start of processing. This is managed within the administration module of Central Server (CS). Users must search for the individual record and then select the record and flag the record for hold.

Section 4, Subsection 4.15.3 - Vendor solution should allow for priority flags to be set on individual card print records which must trigger expedited processing.

VENDOR RESPONSE:

Gemalto confirms that our solution allows for priority flags to be set on individual card print records to trigger expedited processing. This can be achieved through two ways. First, priority/expedited processing flags may be selected during the enrollment process within our Image Capture Workstation (ICW). Priority statuses may also be updated after the enrollment has already been completed through the administration module of Central Server (CS). Users must search for the individual record and then select the record and update the priority of the individual card print record.

Section 4, Subsection 4.15.4 - Vendor solution should allow for tracking information, to be available for expedited print request records.

VENDOR RESPONSE:

Gemalto confirms that our solution allows for tracking information to be made available for expedited print request records. Our solution is flexible with regards to communications and notifications and we can pass this information back to the DMV through methods including secure web services, Application Programming Interfaces (API's), or even email notifications if the DMV would like to pass this information on to the customer. This information can also be made available within the administration module of Central Server (CS). We are also able to handle tracking information in the same manner for "For Federal" DL/IDs.

Section 4, Subsection 4.16 - Reports

Section 4, Subsection 4.16.1 - Vendor solution should capture audit data for all images, data captured, and temporary DLs produced and made available in detail and summary reports.

VENDOR RESPONSE:

Gemalto confirms that Central Server captures audit data for all images, data captures, and temporary DL's produced. This information can be made available within our Web Reporting System (WRS) in detail and summary reports and can also be included in dashboards.

Gemalto's Central Server (CS) solution logs a comprehensive set of application/user activity event data encompassing the entire card issuance process. CS is responsible for the secure storage (i.e., integrity of the application and user activity log data and access rights/restrictions), and query and reporting functionality of this data.

Section 4, Subsection 4.16.2 - Vendor solution should produce daily reconciliation reports.

VENDOR RESPONSE:

Gemalto confirms that our solution is able to produce daily reconciliation reports. For inventory related reconciliation reports, reports can be made within our Web Reporting System (WRS) or within our Inventory Management System (IMS) where we have the functionality for perform inventory audits and reconciliation to ensure that stocks match what is in the system of for secure temporary documents within field offices or stocks of secure cardstock and consumables for the emergency OTC printer location.

Section 4, Subsection 4.16.3 - Vendor solution should be able to request reports for specific date or date ranges.

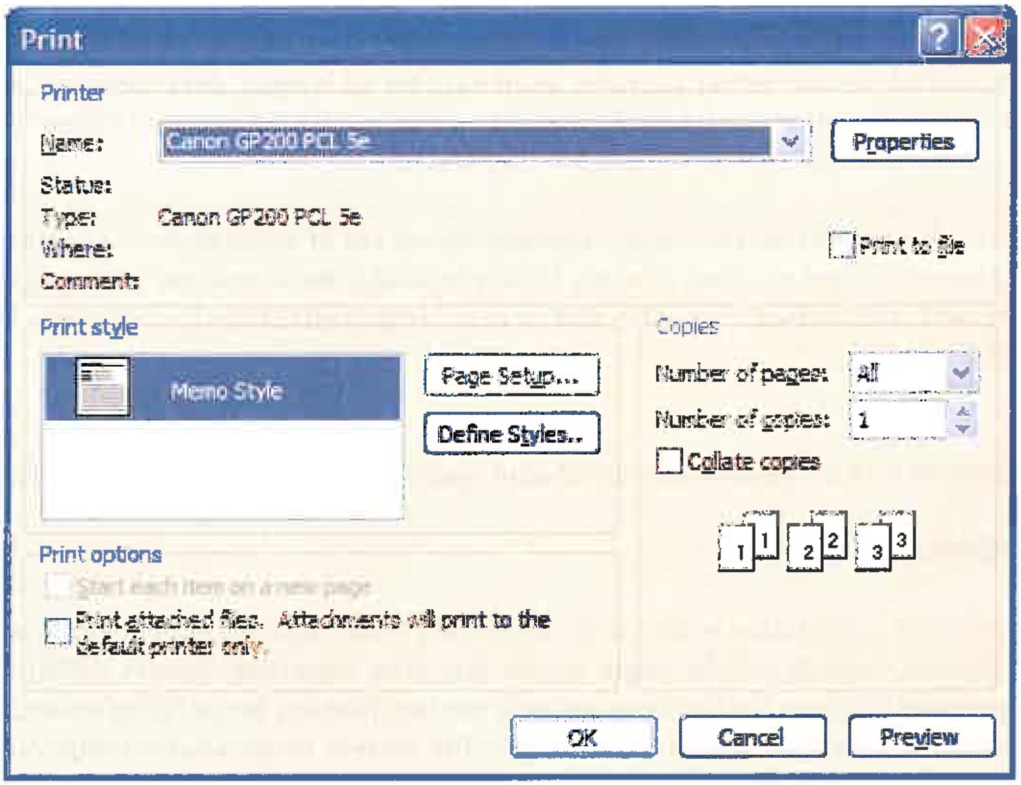
VENDOR RESPONSE:

Gemalto confirms that reports may be requested for a specific data or date range. This is a standard feature within or Web Reporting System (WRS) and is included for all applicable reports.

Section 4, Subsection 4.16.4 - Vendor solution should print to Agency network printers.

VENDOR RESPONSE:

Gemalto confirms that our solution supports printing to Agency network printers. Our Web Reporting System (WRS) and SSRS Report Builder print through the standard Microsoft Print Dialog (how web pages, Word documents, Excel files, and other documents are normally printed through Windows) so the DMV is able to print to any Agency network printer as long as the workstation used to print the report has the appropriate printer installed.



Print

Printer

Name: Canon GP200 PCL 5e

Status:

Type: Canon GP200 PCL 5e

Where:

Comments:

□ Print to file

Print style

Memo Style

Copies

Number of pages: All

Number of copies: 1

□ Collate copies

Print options

□ Start each item on a new page

□ Print attached files. Attachments will print to the default printer only.

FIGURE 51: STANDARD MICROSOFT PRINT DIALOG BOX

Section 4, Subsection 4.17 - Controlled Use

Section 4, Subsection 4.17.1 - Vendor solution should be able to log unauthorized attempts to access the system software.

VENDOR RESPONSE:

Gemalto confirms that our solution is able to log unauthorized attempts to access the system software. This is tracked within our Central Server (CS) and may be viewed along with other audit data within the Central Server (CS) administration module.

Section 4, Subsection 4.18 - Protection

Section 4, Subsection 4.18.1 - Vendor solution should have security protection to prevent unauthorized access.

VENDOR RESPONSE:

Gemalto confirms that our solution has security protection to prevent unauthorized access to the system. This is managed through a few different ways. First, login is password protected through Active Directory where we can manage access rules like login attempts, logout after a certain amount of inactive time, etc. We can also provide multiple levels of access and restrictions for various user groups. If we integrate with the State's Active Directory, we are able to push the State's IT policy and rules to our solution.

Section 4, Subsection 4.19 - Data Management

Section 4, Subsection 4.19.1 - The system administration module should include data management functions. Describe how these data management functions will address:

VENDOR RESPONSE:

Gemalto's Central Server is administered through a web browser and allows the DMV to manage user groups, rights, and permissions. It also allows the DMV to adjust configurations of the Gemalto Capture Suite Image Capture Workstation allowing for example the DMV to change which ICAO checks are performed. This administration module is also where audit data is accessed and managed.

4.19.1.1 Removing records with data or image errors

VENDOR RESPONSE:

Gemalto confirms that our Central Server (CS) administration module supports data reconciliation and removing records with data or image errors. Due to the sensitive nature of the data held within our solution, Gemalto will work with the DMV to clearly define and implement all business rules and uses cases for data cleansing and deletion. We can also track all of the records that were modified or deleted within our solution for audit purposes.

4.19.1.2 Marking records that are to be used for testing purposes

VENDOR RESPONSE:

Gemalto confirms that our solution supports test records and these may be managed within our Central Server (CS) administration module. Our solution can use fixed "Dummy Data" that can be passed through all of the gates all the way through card production. If the State wishes to use this test data to make test cards, we highly recommend adding "Sample Card" or similar verbiage to ensure that these test records do not pose a security risk to the overall solution. Gemalto will work with the DMV during the planning phase of the project.

4.19.1.3 Access to system audit logs

VENDOR RESPONSE:

Gemalto's solution is capable of logging all user actions/operations at the transaction level in audits and investigation activities. Application log data provides the "who, what, where and when" of all of the critical business actions throughout the Gemalto Solution. This Audit Data is searchable and is also available for ad-hoc queries. Audit data may also be restricted to user groups so that only approved DMV users can access certain data.

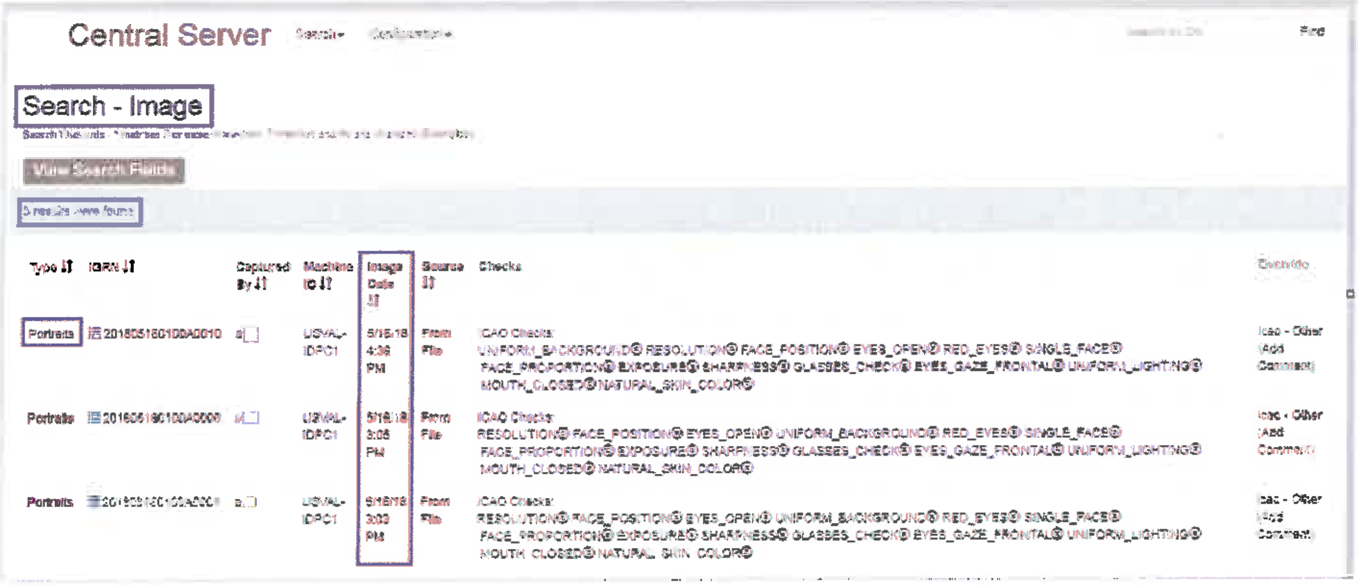
In our experience, audit data requirements vary slightly from jurisdiction to jurisdiction regarding what specific data and actions that must be logged. However, most jurisdictions share the high level requirement of tracking actions and activity within their solution and then presenting that data through a user interface allowing users to query data which is restricted by user group. Because of this, our solution has been designed to be flexible regarding audit and logging requirements. These requirements are specified between DMV and Gemalto during workshops at the beginning of the planning phase of the project.

Section 4, Subsection 4.20 - Audit functions

Section 4, Subsection 4.20.1 - Vendors solution should store the username for every transaction completed on the image and signature capture workstation. Re-authentication upon the printing of each temporary driver's license may be needed and should be configurable.

VENDOR RESPONSE:

Gemalto confirms that our solution logs the username of the operator for every transaction performed on our Image Capture Workstations. We are also able to log every action and override performed within our Image Capture Workstation (ICW) in addition to every other module of our solution including the Biometric Investigative Workstation. Audit data is security stored in our Central Server (CS) solution and is only accessible to authorized employees.



Type	IGRN	Captured By	Machine ID	Image Date	Source	Checks	Override
Portraits	201805160100A0010	a	USVAL-IDPC1	5/16/18 4:36 PM	From File	ICAO Checks: UNIFORM_BACKGROUND RESOLUTION FACE_POSITION EYES_OPEN RED_EYES SINGLE_FACE FACE_PROPORTION EXPOSURE SHARPNESS GLASSES_CHECK EYES_GAZE_FRONTAL UNIFORM_LIGHTING MOUTH_CLOSED NATURAL_SKIN_COLOR	Icao - Other (Add Comment)
Portraits	201805160100A0009	a	USVAL-IDPC1	5/16/18 3:05 PM	From File	ICAO Checks: RESOLUTION FACE_POSITION EYES_OPEN UNIFORM_BACKGROUND RED_EYES SINGLE_FACE FACE_PROPORTION EXPOSURE SHARPNESS GLASSES_CHECK EYES_GAZE_FRONTAL UNIFORM_LIGHTING MOUTH_CLOSED NATURAL_SKIN_COLOR	Icao - Other (Add Comment)
Portraits	[illegible]	a	USVAL-IDPC1	5/16/18 3:03 PM	From File	ICAO Checks: RESOLUTION FACE_POSITION EYES_OPEN UNIFORM_BACKGROUND RED_EYES SINGLE_FACE FACE_PROPORTION EXPOSURE SHARPNESS GLASSES_CHECK EYES_GAZE_FRONTAL UNIFORM_LIGHTING MOUTH_CLOSED NATURAL_SKIN_COLOR	Icao - Other (Add Comment)

FIGURE 52: EXAMPLE IMAGE SEARCH ICAO CHECKS OVERRIDE AUDIT

** Please note that the above screenshot is a sample of a previously delivered solution and the final user interface design will be specified during project specification workshops.*

Section 4, Subsection 4.21 - Equipment installation

Section 4, Subsection 4.21.1 - To minimize clutter, prevent damage, and prevent easy removal, the Vendors solution should consist of only the workstation components that are necessary for capturing the applicant's image, validating DL credentials and signature.

VENDOR RESPONSE:

Gemalto has always made it a priority to not only minimize the required counter space needed for our systems, but ensure that the desk layout is as ergonomic as possible to ensure the interaction between the equipment and operator is as efficient as possible. We also securely fasten and mount hardware whenever possible to reduce the potential for damage or theft of equipment. To minimize the amount of counter space required, Gemalto suggests placing as much equipment as possible under the counter, or on side counters. We can start by dividing the equipment into the following three categories:

1. Customer facing countertop
2. Side countertop
3. Below counters

Customer Facing Countertop

Some equipment must be placed on top of the customer-facing counter. This includes at a minimum, the camera system, signature tablet, monitor, keyboard and mouse.

Helpful Design Decisions

We understand this space is at a premium, therefore we have made some design decisions that help conserve as much counter space as possible. For instance, our current camera system is designed to have a minimal footprint. The signature tablet is small, lightweight and rugged.

Ergonomic and Easy-to-Use

The camera system also requires virtually no adjustments by the user, ever. It captures an image of the complete backdrop. As long as the applicant is in front of the backdrop, no adjustments are required. Once the image is captured, the system automatically locates, crops and provides color correction of the finished photo. All with no user intervention.

The signature tablet is small, lightweight and rugged. It is tethered to the workstation by the USB cable, allowing adequate length to easily support wheelchair applicants. Its' design also supports right and left-hand applicant comfortably.

Side Countertop

Other equipment must be handy, but could reside on a side countertop. This includes devices such as the temporary DL/ID printers.

Below Counters

Equipment that is not used throughout the day can be located under the counter. This includes the computer and all power supplies and cabling. For the State of New Hampshire, we mounted workstations under desks to provide additional counter space.

Cabling

All cabling and power supplies will be located under the counter whenever possible. They will be affixed off the floor and out of the way of the users' normal movements. All associated cabling will be tie-wrapped to keep it away from the user, cleaning crews, etc.

Cabling that must exist on the countertop will be tie-wrapped and run in areas that are non-intrusive.

Office Design Plan

Prior to implementation, Gemalto will conduct site surveys and provide office layout plans as an output to the DMV. This plan will include a layout of all equipment and cabling required for the workstations.

CARD DESIGN AND SECURITY FEATURES REQUIREMENTS

Section 4, Subsection 4.22 - Secure Temporary Driver's License and ID's

Section 4, Subsection 4.22.1 - Vendor should explain how their solution will produce a secure temporary driving credential for applicant use while waiting for the card to be printed at the secure central production facility; including any secure consumables, such as laminate, and/or paper, and recommended printing equipment.

VENDOR RESPONSE:

As described in the above response to "Section 4, Subsection 4.9.1 "Gemalto confirms that a secure temporary driver's license will be produced by our Image Capture Workstation (ICW). Our solution uses a laser printer and a secure paper stock, detailed below, to produce Secure Temporary Driver's License and ID's that are resistant to alteration and forgery.

Temporary Driver's License - Security Features

The following security features are unique to the paper substrate of the Temporary Driver's License which has been included with our offer.

- **UV Fibers** - fibers are visible when put under a UV light source **(Illustrated Below).**
- **Toner Retention/Fusion** – this allows the toner to penetrate the paper deeply making it difficult to change.
- **Chemically Reactive Stains**– this causes the stock to stain if bleach or other chemicals are used.
- **Microtext** – This text is printed on the substrate and requires magnification to read with the naked eye.

FIGURE 53: UV FIBERS

Temporary Driver's License – Personalization and Use

The letter area and the interim document itself are personalized using a laser. **Please note that the interim document may be peeled from the carrier and folded into a card as detailed below.**

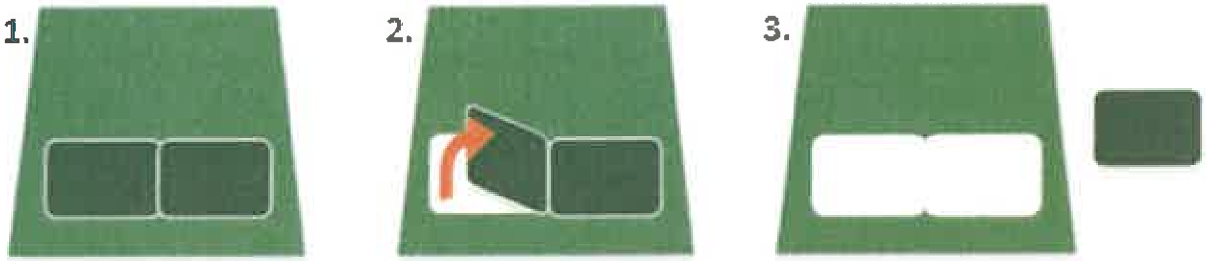


FIGURE 54: TEMPORARY DOCUMENT USAGE

Temporary Driver's License - Specifications:

Security Paper

- 28lb Bond
- Invisible blue security fibers that glow under UV Light. (green/yellow fluorescing fibers are available as an option)
- Chemical stains that react with: Oxidants, Polar Solvents, and, Non Polar Solvents
- Toner Retention/Fusion treatment – our supplier has taken steps to develop a toner retention treatment that not only performs well on high-speed laser printers, but also addresses fusion issues on low-heat laser printers.
- We contracted with one of our major paper suppliers to enhance the properties of our toner retention to meet this dual need.

Clean Release Adhesive

This adhesive was developed by our supplier and serves the following functions:

- Holds the cards firmly in place on the liner during laser throughput.
- Releases the card from the liner without tearing the cards.
- Leaves little to no residue on other documents after the cards are released from the liner.

Liner Material

The liner that is married to the base sheet was decided on after months of trials and it serves the following functions:

- Reacts favorably with the adhesive to hold the cards in place.
- Reacts favorably with the adhesive, when exposed to laser heat, so as not to compromise the way the cards release.
- Throughputs well on laser printers without causing a tenting effect.

Section 4, Subsection 4.23 - Card Design Changes

Section 4, Subsection 4.23.1 - Vendor should describe how they propose handling security format changes to cards made post-implementation, based on reported or identified security gaps.

VENDOR RESPONSE:

Having Gemalto as your vendor is important to staying on top of any new standards well ahead of its implementation. Gemalto works with the standards team at AAMVA to share our experience and recommendations towards making North American Driver Licenses more secure and interoperable with today's security threats and challenges. We keep our customers informed of changes and the road map of any upcoming standards to determine the best plan to implement enhancements.

Adapting and modifying solutions to remain in compliance with applicable laws, rules, and regulations is a common requirement for jurisdictions in the driver license space. Gemalto addresses this through the following:

- We have continuously adapted our solution and processes to meet national, federal and international laws, rules, regulations and acknowledged industry best practices.
- During the planning phase of the project, we discuss expected change that will occur throughout the project so that we can plan and customize our solution to easily adapt whenever possible. For example, we have some jurisdictions that must regularly update data on the personalized cards such as Governor's or Director's names and signatures.
- During the Planning Phase of the project we also establish clearly defined processes and procedures for managing changes not only during the initial project delivery but also throughout the life of the project. This typically includes a Communication Plan, Change Management Plan, and Testing and Acceptance Plans.

Gemalto has been providing secure documents to our customers for decades and have found a proven means to assure that your next generation documents are impossible to reproduce and very difficult to simulate; exceed the intended security standards; and represent the jurisdiction artistically through creative design and high-end security planning. If Gemalto ever determines that a security feature needs to be enhanced or an AAMVA requirement changes, we will immediately analyze the impact of the change to your documents and recommend an implementation plan.

PROJECT MANAGEMENT

Section 4, Subsection 4.24

Section 4, Subsection 4.24 - The Vendor project manager should be involved in every detail of the project from start to finish. High level oversight will not be acceptable.

VENDOR RESPONSE:

Gemalto confirms that our proposed, PMP certified project manager, Tony Wallette, will be involved in every detail of the project from start to finish. The project manager will be on site on a regular basis and available for in person and conference call meetings throughout the duration of the project. The project manager is responsible for managing all day to day activities including project planning, communications (regular project status reports), and hardware and software delivery.

Section 4, Subsection 4.25

Section 4, Subsection 4.25 - The Vendor project manager should follow project phases from project initiation through acceptance, including requirements gathering and analysis. The Vendor project manager should be prepared and capable of facilitating requirements gathering meetings with the Agency staff.

VENDOR RESPONSE:

Gemalto confirms that our proposed, PMP certified project manager, Tony Wallette, will be involved with and follow all project phases from project initiation through acceptance, including requirements gathering and analysis. Our project manager is prepared and capable of facilitating requirements gathering (Requirements Specifications/RQS and Requirements Workshops). He has a Master's degree in Computer Information Systems and over 18 years of experience in state government. He has worked as a Project Manager for five different state Driver's License programs with a proven track record of customer service. He has also worked with West Virginia on a proposed DL/ID solution and is familiar with their current system.

Our project manager will be involved with and follow all project phases of our project plan which are listed below:

- Monitoring Phase (throughout the duration of the project)
- Initiating Phase
- Planning Phase
- Executing Phase
- Closing Phase

Section 4, Subsection 4.26

Section 4, Subsection 4.26 - The Vendor project manager should be involved in the technical details of the design, development, and testing phases of the project, and should not expect the Vendor technical lead to fully manage those activities.

VENDOR RESPONSE:

Gemalto confirms that our proposed, PMP certified project manager, Tony Wallette, will be involved in the technical details of the design, development, and testing phases of the project, and does not expect the WV DMV to technical lead to fully manage those activities. As described above, our proposed project manager has a Master's degree in Computer Information Systems and over 18 years of experience in state government. He has worked as a Project Manager for five different state Driver's License programs with a proven track record of customer service. He has also worked with West Virginia on a proposed DL/ID solution and is familiar with their current system.

Section 4, Subsection 4.27 - Communication

Section 4, Subsection 4.27.1 - The Vendor project manager should manage the work by establishing and maintaining communications with all groups related to the project. The activities of the Vendor's project team should be directed, coordinated, and communicated with the Agency Project Manager to ensure that the project progresses per the project work plan and is completed on schedule.

VENDOR RESPONSE:

Your success in every way is our success. We know that the key to delivering a successful project is ensuring that our people truly understand your needs and make your priorities their own. With this in mind, Gemalto confirms that our proposed, PMP certified project manager, Tony Wallette, will be involved in every detail of the project from start to finish. Tony will serve as your advocate and trusted partner throughout the duration of the project, ensuring that business objectives are regularly reviewed and assessed against current performance.The project manager will be on site on a regular basis and available for in person and conference call meetings throughout the duration of the project. The project manager isresponsible for managing all day to day activities including project planning, communications (regular project status reports), and hardware and software delivery.

Section 4, Subsection 4.27.2 - The Vendor project manager should communicate with the Agency project manager daily for resolution of issues, decisions, or just to report project status.

VENDOR RESPONSE:

Gemalto confirms that our proposed, PMP certified project manager, Tony Wallette, will be involved with and follow all project phases from project initiation through acceptance, including requirements gathering and analysis. Our project manager is prepared and capable of facilitating requirements gathering (Requirements Specifications/RQS and Requirements Workshops). He has a Master's degree in Computer Information Systems and over 18 years of experience in state government. He has worked as a Project Manager for five different state Driver's License programs, successfully serving and advocating for his customers, and building strong relationships along the way. He has also worked with West Virginia on a proposed DL/ID solution and is familiar with their current system.

Section 4, Subsection 4.28 - Status Reporting

Section 4, Subsection 4.28.1 - During project design and implementation, Vendor's Project Manager should facilitate weekly project status reviews to ensure measurable progress is being achieved and the Vendor's project team is following the agreed upon work plan.

VENDOR RESPONSE:

We are dedicated to listening and collaborating with our customers at every step of the way. Customer feedback is greatly valued and utilized as fuel for fully realizing our customer's vision. Our PMP pledges to guide your team, utilizing extensive experience and lessons learned, paired with consistent and productive collobartion and listening exercises. Therefore, Gemalto can confirm that our project manager will facilitate weekly project status reviews to ensure measured process is being achieved and the Gemalto project team is following the agreed upon work plan. As described above, **Gemalto will provide a Project Communications Plan to document how project and Project information should be communicated to all parties and includes the method of communication.** It describes why, what, when, and where items will be communicated and also indicates who is responsible for each item.

The following items are standard channels that we typically follow in our projects:

- A contact list, including Project Team Members, Sub-Contractors, related Projects, DMV Key Staff and sponsor contact information, is developed and stored in the appropriate project repository. Distribution and control of this list will be documented and approved.
- The Project Manager will facilitate the Project Team meetings and manage action items, issues and risk logs for the Project.
- Executive Project Steering Committee Meeting held between Senior Management from both organizations occurs on an as needed basis via in person or conference call. Agenda/Minutes distributed by email and stored in a project repository.
- Project Steering Committee Meeting held between the Project Manager, Executive Sponsors, DMV, and relevant team members to review status, issues, or risks that cannot be resolved by the Project Team. Frequency of meeting is typically on a monthly basis or as needed. Agenda/Minutes distributed by email and stored in a project repository.
- Project Status Report, which is an executive level status of the project including risks, is distributed by the Project Manager to DMV and Gemalto Executives. This can be held in person or via conference call and is typically done bi-weekly. Agenda/Minutes distributed by email and stored in a project repository.

- Change Control Board Meeting to review, evaluate, approve, reject, and prioritize change requests. The meeting is held between the Project Manager and the DMV either in person or via conference call. The frequency is typically bi-weekly. Agenda/Minutes distributed by email and stored in a project repository.
- Risk Review Board Meeting is held on a bi-weekly basis between the Project Manager and the DMV to review and manage project risks. Agenda/Minutes distributed by email and stored in a project repository.
- Acceptance or approval of decisions or other requests may occur via e-mail as long as the e-mail includes a definition of what is being accepted or approved and comes directly from the party accepting or approving. Instant messages or transcripts of chat sessions are not acceptable for this purpose.

Section 4, Subsection 4.28.2 - Additional meetings should be scheduled as required by the Agency Project Manager or the Vendor. The Vendor's Project Manager and personnel should be available to provide information, reports, or audits as required by the Agency Project Manager.

VENDOR RESPONSE:

Gemalto confirms that additional meetings will be scheduled, if required, either by the Agency Project Manager or the Gemalto project manager. Gemalto's project manager and project team will be available for additional meetings and to provide any additional information, reports, or audits as required by the Agency Project Manager to ensure the overall success of the project.

Section 4, Subsection 4.28.3 - The following deliverables should be included prior to each status meetings:

VENDOR RESPONSE:

Gemalto confirms that the following deliverables will be included prior to each status meeting as required by the Agency. In addition, these deliverables will be included as part of our Project Communications Plan as described above.

- Updated project work plan
- Status of all tasks that have fallen behind schedule
- Summarization of all risks and problems
  - Action and person(s) responsible for mitigating the risk and resolving the issue
  - Impact to the project schedule

4.28.3.1 Updated project work plan indicating progress for each task

VENDOR RESPONSE:

Gemalto confirms that an updated project work plan indicating progress for each task will included prior to each status meeting as required by the DMV. This is a standard component of our Project Communications Plan and Project Status Report.

4.28.3.2 Identify and report the status of all tasks that have fallen behind schedule, the reason for the delay, the projected completion date and project impact

VENDOR RESPONSE:

Gemalto confirms that our project manager will identify and report the status of all tasks that have fallen behind schedule, the reason for the delay, the projected completion date and project impact prior to each status meeting as required by the DMV. This is a standard component of our **Risk and Issue Management Plan, Project Communications Plan and Project Status Reports**.

4.28.3.3 Identify and summarize all risks and problems identified by the Vendor, which may affect the project:

VENDOR RESPONSE:

Gemalto confirms that our project manager will identify and report all risks and problems identified by the Vendor, which may affect the project prior to each status meeting as required by the DMV. This is a standard component of our **Project Communications Plan and Project Status Report**. As part of our overall Project Plan, Gemalto will provide a formal **Risk and Issue Management Plan** to the DMV as a deliverable to clearly define how we will identify significant project risks and indicate the likelihood, impact, and response strategy with each risk in an effort to mitigate or avoid the risk. These actions will be performed and monitored during the project.

Risk management is conducted throughout all phases of the project. The objective is either to identify potential risks in advance, provide a mitigation plan in the event the risk occurs, and to provide an approach to manage non-forecasted risks. Risk assessment is conducted at the Project kick-off, at the end of each major phase, and periodically as risks may be identified during the project.

4.28.3.3.1 For each risk and issue, identify the action and person(s) responsible for mitigating the risk and resolving the issue, and the time required to implement avoidance and/or mitigation actions.

VENDOR RESPONSE:

Gemalto confirms that our project manager will identify the action and person(s) responsible for mitigating each risk and resolving the issue, and the time required to implement avoidance and/or mitigation actions for each risk prior to each status meeting as required by the DMV. This is a standard component of our **Risk and Issue Management Plan, Project Communications Plan and Project Status Reports**.

4.28.3.3.2 For each risk and issue identified, state the impact to the project schedule discuss and identify all personnel, equipment, facilities, and resources of the Agency that will be required for the Vendor to perform the project work plan tasks at least two (2) weeks in advance of the need.

VENDOR RESPONSE:

Gemalto confirms that our project manager will state the impact to the project schedule discuss and identify all personnel, equipment, facilities, and resources of the Agency that will be required for the Vendor to perform the project work plan tasks at least two (2) weeks in advance of the need for each risk and issue identified as required by the DMV. This requirement will be added to our **Risk and Issue Management Plan, Project Communications Plan and Project Status Reports**.

Section 4, Subsection 4.29 - Project Work Plan Objective

Section 4, Subsection 4.29.1 - The Vendor should describe in the response a draft project work plan that includes project phases and milestones required from project initiation through full implementation (i.e. planning, analysis, design, development, testing, deployment, and operations).

VENDOR RESPONSE:

A high level project overview can be found in the pages below and a detailed breakdown of each phase we will follow towards the end of the project plan.

- Monitoring Phase
- Initiating Phase
- Planning Phase
- Executing Phase
- Closing Phase

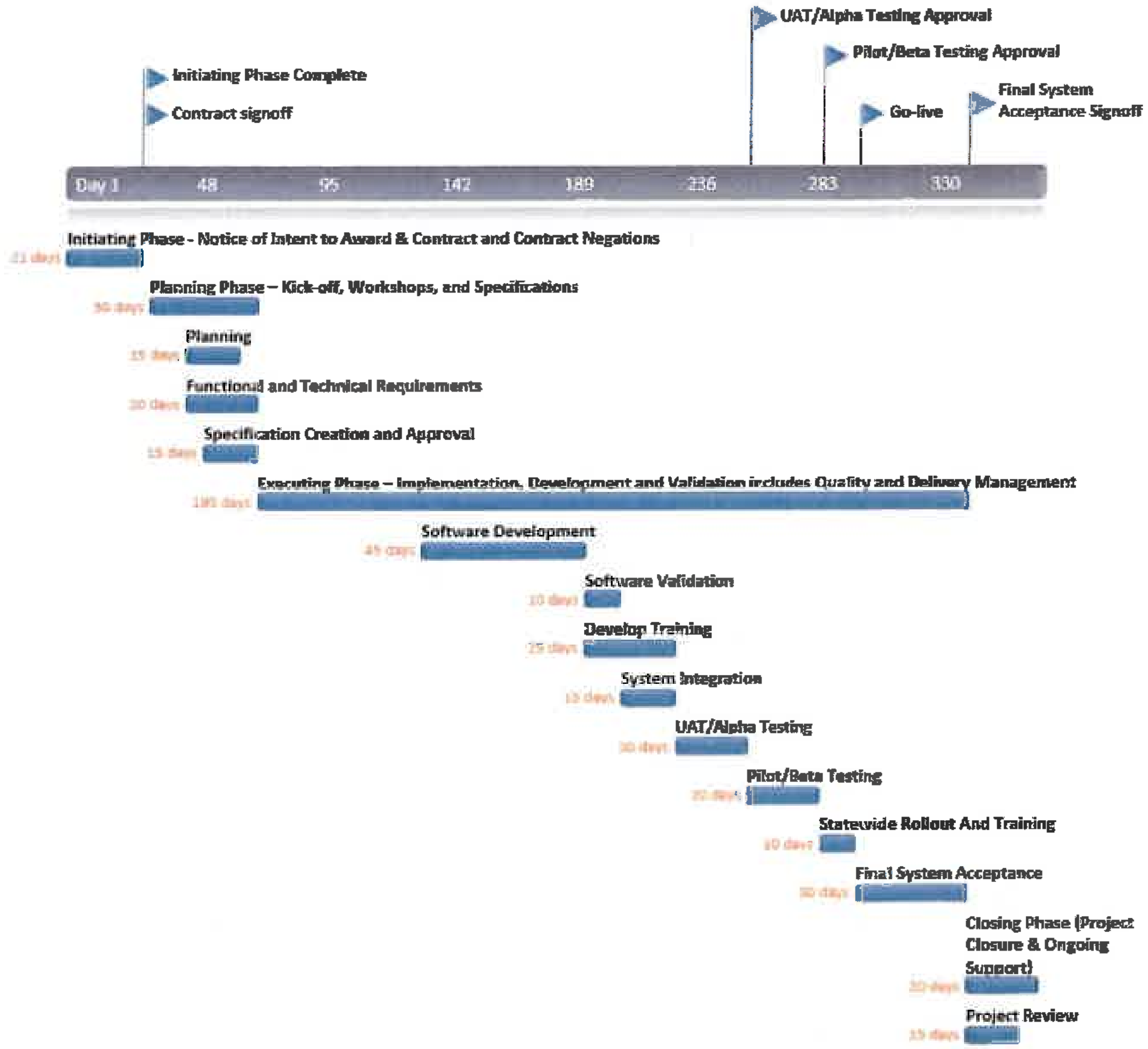


FIGURE 55: HIGH LEVEL PROJECT OVERVIEW

Monitoring Phase:

Our goal of the monitoring phase is to collect, measure, and disseminate performance information, and assess measurements and trends to effect process improvements. This phase occurs throughout the duration of project.

This phase includes the following plans and activities:

- **Project Control** - The roles, responsibilities, and obligations of the Project Team, Team Leaders, Quality Representatives, and Stakeholders
- **Change Control** -Changes to the baseline approved plan must be tracked, managed and recorded through a formal Change Control Process under a Change Control Board (CCB)
- **Issue Management** -A real-time process put into place to increase performance of the project.
- **Risk Management** -Objective is either to identify potential risks in advance, provide a mitigation plan in the event the risk occurs, and to provide an approach to manage non-forecasted risks.
- **Quality Management** -It defines Project Quality, the processes for managing quality claims, assesses quality compliance, and creates quality awareness
- **Project Communication** - A plan will be developed that documents how Gemalto will ensure proper and timely communication of all Project-relevant information.

Initiating Phase:

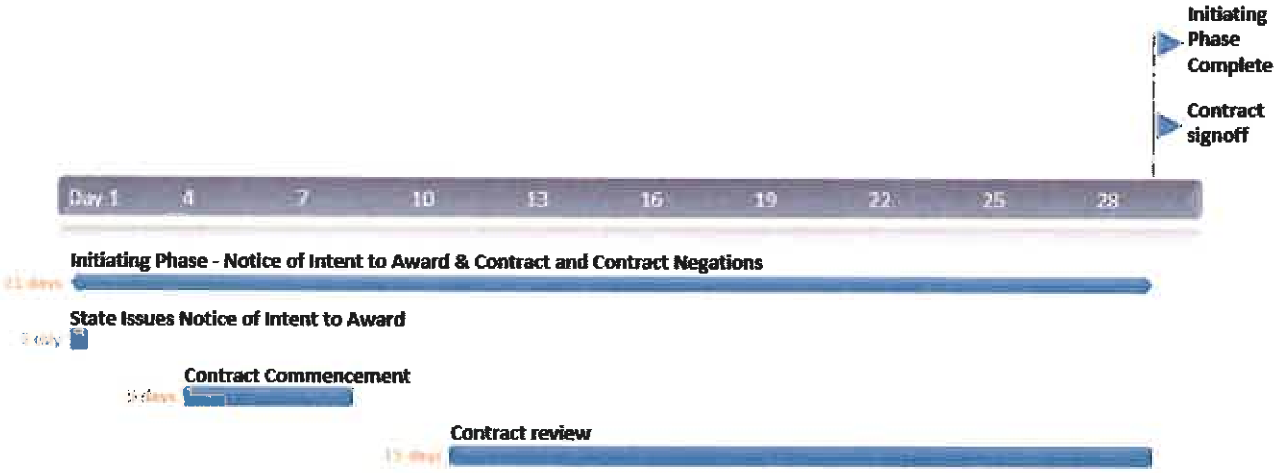


FIGURE 56: INITIATING PHASE OVERVIEW

During the Project Initiation phase, Gemalto will mobilize the necessary resources required to support the final contract negotiation process in order to start the project as soon as possible. These resources will include Legal and/or Finance as required.

During Contract Review, Gemalto will make key individuals available to visit the State of West Virginia and review or answer questions regarding the submission. We anticipate that the Executives, Project Director, Project Manager, and Account Manager will be made available during this period in addition to any additional required resources.

Planning Phase:

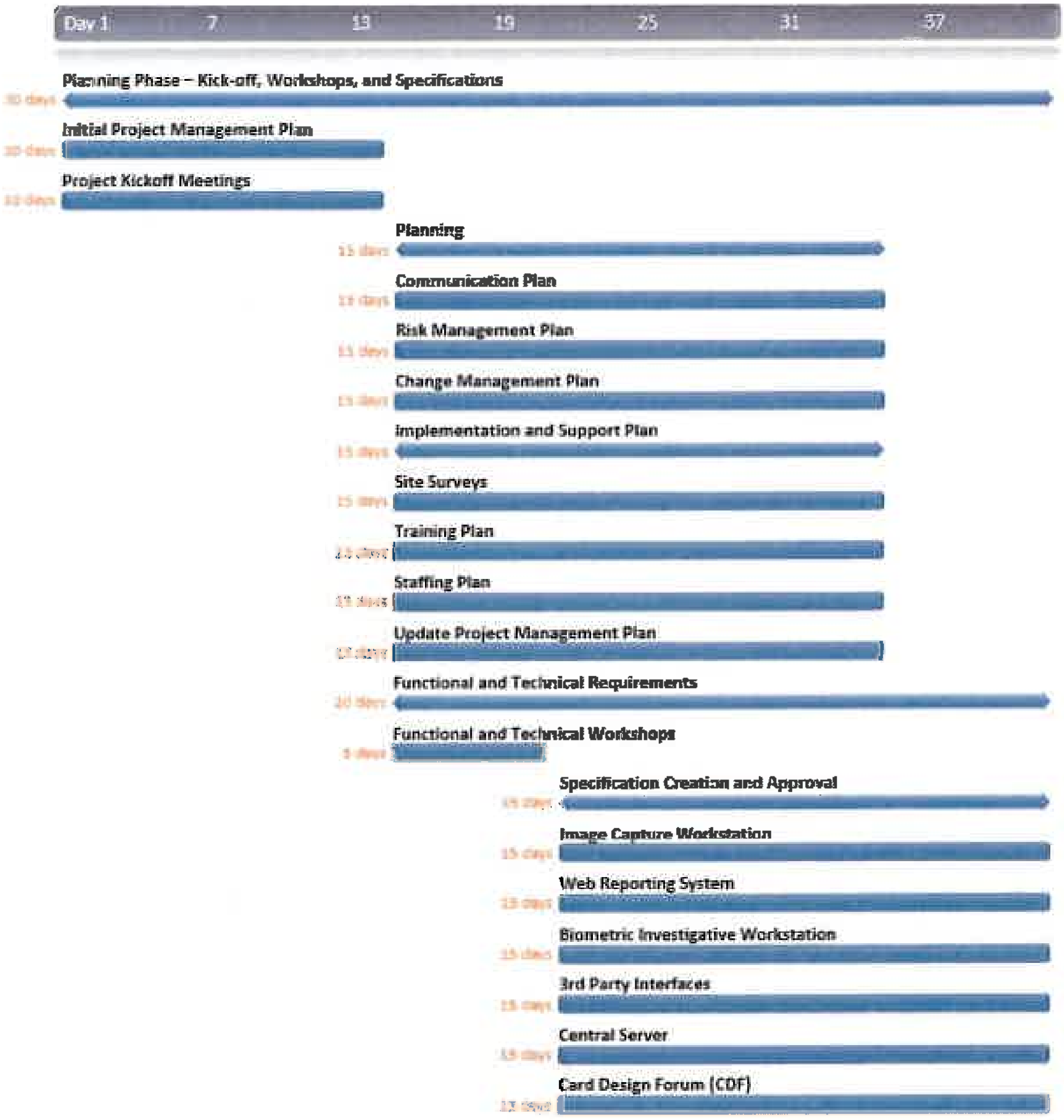


FIGURE 57: PLANNING PHASE OVERVIEW

The first part of the Planning Phase is typically the Project Kickoff. In this compressed timeline, Gemalto will include the Project Kickoff at the very beginning of the Requirements (RQS) Workshops described below. Kickoff meetings are held to discuss the **upcoming requirements and to layout the upcoming milestones, timelines, and schedules for each of the work packages listed below.** In addition, we will quickly mobilize resources to meet the delivery requirements for the ICW, Central Issuance, Central Server Solution, and plans required by the DMV.

In addition to the RQS for each work package and key documents required by the DMV, the following plans will be:

- **Project Work Plan** – the baseline agreed upon by the both parties during the contract negotiations and the latest updates during project preparation. This document is an active document which will be updated on a weekly basis and agreed by the Gemalto Project Manager and the DMV Project Managers. This document contains the list of activities, tasks, and resources required for successful project implementation. This will become the basis for the Final Implementation Plan.
- **Communication Management Plan** – captures all required communication and documentation that will be exchanged with the DMV, the required frequency of distribution, the method of communication, and the distribution list. Other areas of communication may include updates to the Project Status Report and Project Plan, project status meetings, and steering committee meetings.
- **Change Control Management Plan** – describes the change management process as well as the associated escalation process. It determines, at the beginning of the project, how changes will be identified, qualified, analyzed, and submitted to the State prior to implementation. This plan also identifies potential changes that could occur during the life of the project.
- **Risk and Issue Management Plan** – identifies significant project risks and indicates the likelihood, impact, and response strategy with each risk in an effort to mitigate or avoid the risk. These actions will be performed and monitored during the project.

In addition to the above project management deliverables, Gemalto will provide the following plans to the DMV in conjunction with or immediately following the Requirements Workshop:

- **Testing Plan** - Testing is the execution or evaluation of software and its data to verify conformance to the approved specifications or to identify the discrepancies between the expected results and the actual results. Typically this is developed after the creation of the State's Solution Requirements Specification so that Gemalto has a clear understanding of the requirements to be validated. Of course this can be adjusted according to the DMV's requirements.
- **Acceptance Test Plan (ATP)** – the test plan that will be agreed to by both the State and Gemalto staff to determine the success or need for re-test of the solution as evaluated during each of the UAT, Pilot and Field UAT Review periods.

Gemalto will also provide the following Plans to the DMV.

- **Quality Assurance Plan (QAP) –** describes the measures taken throughout the beginning of the project to the successful completion of the project. It ensures that all of the deliverables and processes meet the agreed upon quality levels. This plan typically covers the quality standards that will be followed, the controls, tools, and the plan for reporting any issues. For Gemalto, the Quality Plan will summarize all of the inputs to the project. It will also list all of the major milestones, required deliverables, rules, and processes that need to be followed in order to establish agreement and acceptance.
- **Staffing Plan** - involves the confirmation of the allocation of the appropriate resources for the project along with their percentage of allocation toward this project. The scope of this plan not only defines the availability of Gemalto resources but also includes the availability of the State's resources as well. In addition, the Staffing Plan will be used as a foundation for the Implementation Plan.
- **Site Survey / Facilities Plan –** defines the list of sites that require visits by Gemalto and will list the intended dates for each visit. Upon completion of the site visits, this plan will also identify the resources, hardware, equipment, and software required to successfully integrate the solution at each site during deployment.
- **Data Conversion Plan--** covers the migration of existing data within DMV's legacy system into their new system. This plan is typically developed during the creation of the workshops in the planning phase because the migration strategy is heavily dependent on the specifications of the existing and future systems. Of course a plan can be provided earlier to the DMV if necessary but based on past experience, Gemalto recommends developing this plan after specifications of the existing and future systems are complete. **As Gemalto is the incumbent vendor, we can guarantee 100% of existing records will be migrated.**
- **Final Implementation Plan** - The items covered under this plan such as the delivery and rollout of the overall solution is typically covered under the Project Work Plan but can be provided as a separate sub-plan if required by the State. Typically, the field installation portion of this plan is updated after the completion and review of the Site Surveys.
- **Preventative Maintenance Plan –** will cover the frequency and methods used to maintain all hardware provided by Gemalto. This is provided as part of the overall maintenance plan will cover in State support, backup parts and equipment, anticipated response and resolution times, maintenance reporting requirements, and remedial maintenance.
- **Disaster Preparedness Plan (Disaster Recovery Plan)** - This Disaster Recovery Plan is designed to ensure the continuation of vital business processes in the event that a disaster occurs at any of the DMV sites including the datacenter and central issuance facility. This plan is an on-going process of planning, developing, testing and implementing Disaster Recovery management procedures and processes to ensure the efficient and effective resumption of critical business functions in the event of an unscheduled interruption.

Acceptance Test Plans (ATP)

With results of Requirements Workshops and with approved RQS, Gemalto will develop acceptance test plans for all work packages. These will be submitted to the DMV for review and approval. The ATP's will be used as the basis for Gemalto Factory Acceptance Tests (FAT) performed before final software release, and User Acceptance Tests (UAT) performed at customer UAT sites, and Site Acceptance Tests (SAT) performed during installation of all Field offices.

Testing is the execution or evaluation of software and its data to verify conformance to the approved specifications or to identify the discrepancies between the expected results and the actual results. The internal Validation Test Plan gives the list of tests to be performed before we move to acceptance. The logical order of the tests and all the details of those tests are described in the **Acceptance Test Plan (ATP).** It should be noted that State resources will be required for the acceptance of all testing and validation to confirm that all requirements have been met.

Typically, the logical order of the tests is outlined below. However, we will work with the State on the details of the test plan approach:

- **Unit Tests** - performed for each sub-system and custom developed component. These tests verify the behavior of a component against their detailed technical specifications. They are internal tests and performed in Gemalto labs in Austin on test platforms.
- **Factory Acceptance Tests (FAT)** - the sub-system components are integrated together during these tests. During this period, we focus on data and event exchange between systems through their technical interfaces. These tests are internal and performed in Gemalto labs in Austin, TX on test bed platforms. We encourage State participation during this testing process because it will give the State an early glimpse of the software for review. Colorado, Idaho, Quebec, Maryland, Idaho, New Hampshire, and all four Atlantic Provinces have all gone through this step.
- **User Acceptance Tests (UAT)** - during the integration test phase, the final production environment is installed, tested, and ready for real production. Commissioning Tests ensure real-environment trouble-free operations. At this stage, the solution is still working with test data and producing test driving licenses (test cards).These will cover the UAT Compliance Review.
- **Site Acceptance Tests (SAT)** - will cover the testing for Field offices that will be performed prior to site acceptance. Pilot Compliance Reviews (for the Central Server Site, Production Site, and Field offices) as well as State -wide rollout will be covered under these tests.

For all the Tests described above, a Test Strategy, a Test Plan, and an Acceptance Plan will be designed and communicated for information and/or approval, depending on the type of test, to the State project teams before executing the tests.

Execution Phase:

The purpose of the Executing Phase is to implement the solution based on what both Gemalto and the State agreed is required for this project. We have provided an overview of executing phase activities for each of the proposed work packages. This will include the following high level activities:

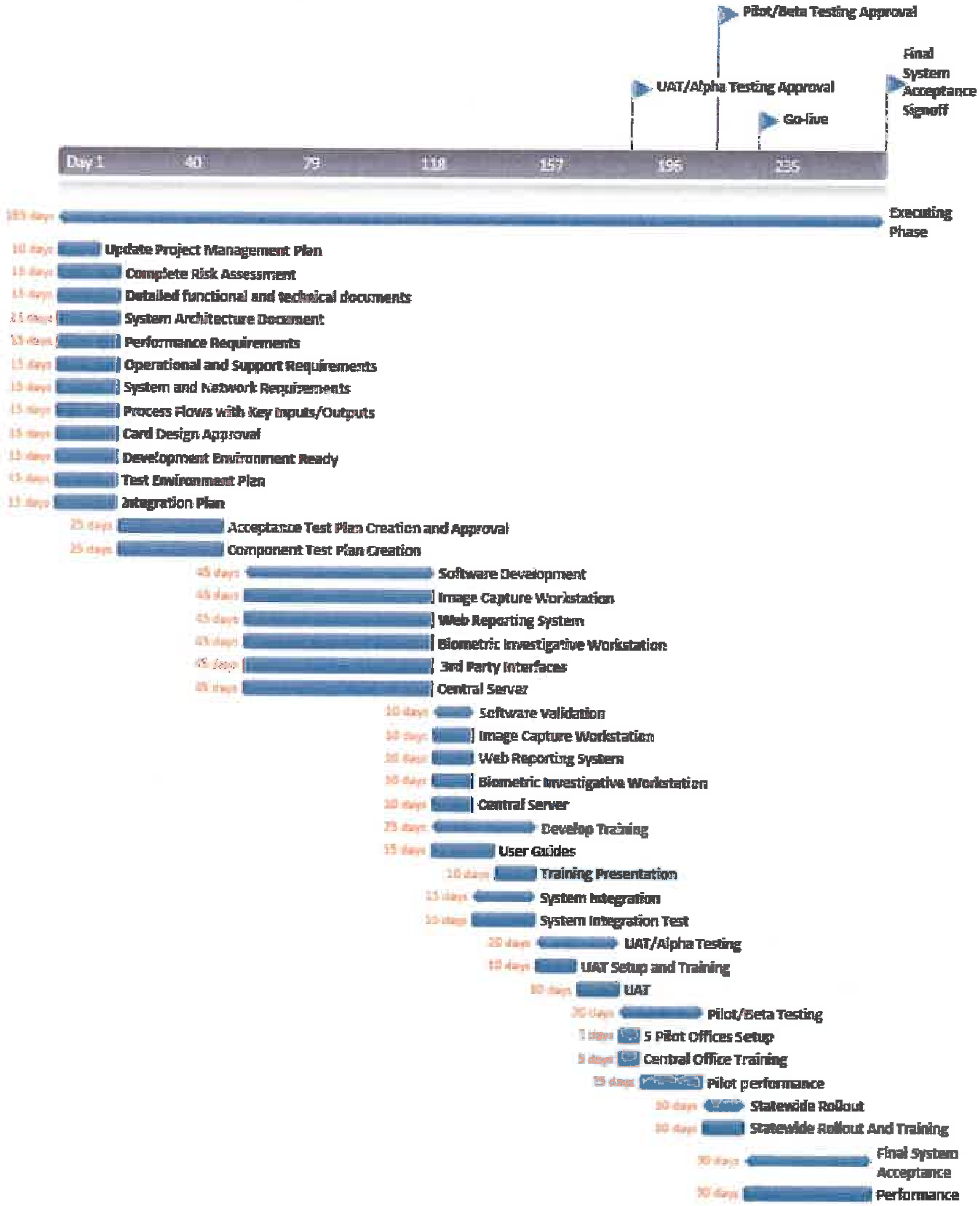


FIGURE 58: EXECUTING PHASE OVERVIEW

Procure Hardware

Given that we will have spent time with the DMV during Requirements Workshops and we have received approvals at this point, Gemalto will commence with procuring hardware. This is an activity that does not require input from the DMV once we have agreed to the specifications. This hardware procurement will include all of the equipment required for the offices.

Server Hardware and Network Configuration

These tasks mainly focus on installing, configuring, and testing the main production and backup servers. This is an activity that does not require DMV involvement.

Gemalto Support Portal and Call Center

These tasks mainly focus on setting up and modifying the Support Portal software and establishing the call center dedicated toll-free number which will be provided to the DMV. It also involves setting up a test database. Once the test database is setup, we will perform unit tests, quality assurance and prepare it for pilot testing. This is an activity that does not require DMV involvement.

Card Production and Reporting

For this activity, Gemalto will modify/update its existing software platform to accommodate the interface with DMV system as well as the proposed hardware. We will run testing for batches, sample print tests, and will prepare it for UAT Compliance Reviews. We will also look to integrate with the State's systems at this time.

Gemalto In-House Integration/System Testing

These set of tasks focus on bringing together the full solution and perform end-to-end testing in-house. We will test data input and storage, system performance, data storage stress, data retrieval and accuracy, in-house production, and reporting. The goal with this set of tasks is to prepare for UAT Compliance Review. This is an activity that does not require the State involvement. We will provide results of this Factory Acceptance Test (FAT) to the DMV for review. However, we welcome the State to view the testing if interested.

Install and User Acceptance Testing

We will require heavy State involvement during this period to witness and approve UATs'. These activities are discussed in further detail with Lab, Development, and User Acceptance Testing (UAT) Sites and UAT Compliance Review. Central Issuance Facility Integration and User Acceptance (UAT). UAT's will similarly be performed for Training Labs.

Training

We separate these tasks into headquarters training and field office training. Field office training will be linked to the field office rollout schedule.

Documentation

Gemalto will provide draft and production versions of Operations and Maintenance Manuals for all components of the schedule according the Final Implementation Plan.

Card Designs

Gemalto will provide card designs based on the specification previously gathered. Once the production system is operational, we will also provide production samples.

Production Material

This is a set of tasks for Gemalto to manufacture, order, and receive all of the necessary card production materials for the project. We expect no involvement from the DMV during these activities.

Card Durability Testing

Gemalto will provide card samples to an external lab for card durability testing.

Pilots

As described above, pilots will be performed in selected Field office Locations. This will validate successful operation of Gemalto solution prior to the final installation.

Solution Rollout

Following successful pilots, Gemalto will move to deploy the remaining sites with Final Installation Schedule and Installation Requirements.

Closing Phase

Once the project is completed, it is essential to draw lessons from what happened. This analysis is performed during a last Project debriefing meeting (post-mortem) involving all project stakeholders. Good practices or good behaviors are captured to be expanded to other projects. It is also important to capitalize on problems that were encountered, in order to understand the root causes and to implement corrective actions.

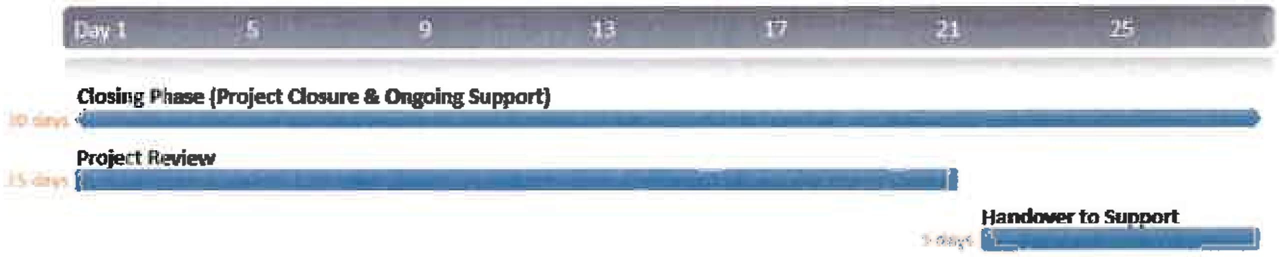


FIGURE 59: CLOSING PHASE OVERVIEW

The goal of the Post mortem is to:

- Collect strengths and weaknesses identified during the project (only ones with possible improvement action) from all project team members
- Rank and select the most significant one (weaknesses and strength - max 5 of each) during the Post Mortem meeting, define actions and actions owners, assigned a person to follow them and share results with others projects.

During the Closing Phase, we will also do the official handoff to Support. As stated previously, the Support Staff will be involved during the project so that we can have a smooth transition.

Project Work Plan and Work Packages (Milestones)

Within our project approach we organize our activities into Work Packages. We have found it is easier to communicate, track, and report on project status. We have listed the work packages and the deliverables associated with these work packages below:

Work Package 1 (WP1) Project Management Milestones
• **Project Management Plan**
✓ **Scope**
✓ **Planning**
✓ **Communication**
✓ **Deliverables**
✓ **Change Management**
✓ **Risk Management**

Work Package 2 (WP2) ID Card Design & Delivery Milestones
• **Workshop**
• **Graphical & Personalization Specification**
• **Temporary Document Specification**
• **Design- Card Design PDF**
• **Design- Epson Proof**
• **Color Proof**
• **Card Delivery**

Work Package 3 (WP3) Enrollment Software Milestones

- **Workshop**
- **ICW capture specification**
  - ✓ **Biometric Capture (Signature & Photo)**
  - ✓ **Document Capture**
- **Capture Acceptance Test Plan**
- **Factory Acceptance Test**
- **Capture Software Delivery**

Work Package 4 (WP4) Central Server Software Milestones

- **Workshop**
- **Central Server Specification**
- **Web Reporting Tool**
- **Central Server Acceptance Test Plan**
- **Factory Acceptance Test**
- **Central Server Software Delivery**

Work Package 5 (WP5) External Interfaces Milestones

- **Central Server Specification**
- **Law Enforcement**
- **Central Server Acceptance Test Plan**

Work Package 6 (WP6) Production Manager (Issuance Application) Milestones

- **Production Manager Specifications**
- **Quality Control Specifications**

Work Package 7 (WP7) IT & Security Milestones

- Workshop for DMV Solution and connectivity
- IT Specifications
  - ✓ ICW requirements- Supplied by DMV
  - ✓ ICW Peripherals- Supplied by Gemalto
  - ✓ Central Server -Supplied by DMV
  - ✓ Network Specs (VPN, Firewall)
  - ✓ Bandwidth
- ISP Connectivity
- IT Acceptance Test Plan
- ICW Workstations
- Central Server Equipment
- IT Delivery/ Installation / Validation / Integration

Work Package 8 (WP8) Data Migration Milestones

- Workshop
- Data Migration Specifications
- Data Migration Acceptance Test Plan
- Data Migration Delivery / Installation / Validation / Integration

Work Package 9 (WP9) Implementation &Training Milestones

- Implementation & Training Plan
- Installation in each site
- Training Materials
- User Guides

Work Package 10 (WP10) Support & Maintenance Milestones

- Workshop
- DMV Support:
  - ✓ Customer Portal
  - ✓ Change Management
  - ✓ Incident Management
  - ✓ Escalation Path
  - ✓ Disaster Recovery Plan
- Factory Acceptance Test Plan (Production / Support)
- Factory Acceptance Test (DR) If option is selected
- Support Active

Work Package 11 (WP11) UAT Milestones

- User Acceptance Test Plan
- ICW Workstations
- UAT Training Doc
- Training

Work Package 12 (WP11) Pilot Phase Milestones

- Pilot Plan
- User Acceptance Test Plan
- Pilot Training Doc
- Training

Work Package 13 (WP13) Transition Phase Milestones

- Transition Plan
- Site Acceptance Test Plan
- ICW workstation
- Enrollment Training
- UAT Training Doc
- Pilot Training Doc
- Enrollment User Guide
- Train DMV office staff
- Train DMV head office staff

Section 4, Subsection 4.30 - Test Plan Objective

Section 4, Subsection 4.30.1 - The Vendor should describe how they will develop, implement, and maintain a test plan, subject to the Agency's approval, in accordance with industry standards to manage testing and defect tracking for providing an efficient error correcting process to be used in system and user acceptance testing ("UAT").

VENDOR RESPONSE:

Gemalto will develop acceptance test plans for all work packages with results of Requirements Workshops and with approved Requirement Specifications (RQS). These will be submitted to the DMV for review and approval. The ATP's will be used as the basis for Gemalto Factory Acceptance Tests (FAT) performed before final software release, and User Acceptance Tests (UAT) performed at customer sites, and Site Acceptance Tests (SAT) performed during installation of all Field offices. Gemalto will plan the UAT and coordinate with the Agency as required.

Typically, the logical order of the tests is outlined below. However, we will work with the State on the details of the test plan approach:

- **Unit Tests**
  Performed for each sub-system and custom developed component. These tests verify the behavior of a component against their detailed technical specifications. They are internal tests and performed in Gemalto labs in Austin on test platforms.

- **Factory Acceptance Tests (FAT)**
  System tests and sub-system components are integrated together during these tests. During this period, we focus on data and event exchange between systems through their technical interfaces. These tests follow the approved test plans but they are internal and performed in Gemalto labs in Austin, TX on test bed platforms. We encourage State participation during this testing process because it will give the State an early glimpse of the software for review. Colorado, Idaho, Quebec, Maryland, Idaho, New Hampshire, and all four Atlantic Provinces have all gone through this step. At this stage, the systems and their interfaces are considered as Technically Acceptable within a test environment. This is a unique step offered by Gemalto and all of our customers who participated in it have clearly seen the value.

- **User Acceptance Test (UAT) – Alpha Testing**
  To move forward on the testing strategy, a testing (Staging) platform will be installed in the State's premises at DMV It is expected that this environment will be kept afterward for future release's testing, this will be known as the **DMV Staging Environment**.

  At this stage, the solution will be working with test data and producing test driving licenses (test cards).

- **Site Acceptance Tests (SAT) – Beta/Pilot Testing**
  Meanwhile, during the UAT phase, the final production platform environments are installed. Once UAT is successfully approved, the solution will be installed in the production environment. The systems are at this point installed, tested and ready for real production. The full solution will go through Commissioning Tests (Security validation, stress, performance, and failover) to ensure real-environment trouble-free operations.

  Five sites will have been identified in the Transition Plan to be switched over to the new solution with the co-operation of the State for a Pilot Phase operation. Each of the selected field office sites will be installed with the new solution components (Staff will have received prior training on the new solution), and a SAT will be conducted to ensure the solution deployment is functioning as required. The acceptance criteria for each site shall be defined in conjunction with the State. These sites will operate for a Pilot Phase period which will be determined with the DMV to ensure that the system is operating as designed, meets appropriate SLA's and performance is optimal.

  At this stage, the solution will be working with real data and producing real driving licenses (production cards).

- **Final System Acceptance**
  On successful completion of the Pilot Phase, a statewide rollout of the solution shall begin. Once the last deputy registrar office has completed its SAT, the solution will then run in production for 7 consecutive days, which will be heavily monitored and supported by Gemalto project and integration teams. After 30 days of operation and having any outstanding solution issues closed, the State is expected to issue Final Acceptance and receive handover of the solution.

For all the Tests described above, a Test Strategy, a Test Plan, and an Acceptance Plan will be designed and communicated for information and/or approval, depending on the type of test, to the State's project teams before executing the tests.

Section 4, Subsection 4.31 - Test Plan

Section 4, Subsection 4.31.1 - The test plan should include all the following:

VENDOR RESPONSE:

Gemalto confirm that our test plan will include the following:

- Unit testing
- Integration testing
- Usability testing
- Functional testing
- Performance testing
- Testing of external interfaces
- Continuous regression testing
- Backup and recovery testing

4.31.1.1 Unit testing - on-going development testing (Vendor)

VENDOR RESPONSE:

Gemalto confirms that our testing plan includes unit testing as required by the Agency. Unit Tests and performed for each sub-system and custom developed component. These tests verify the behavior of a component against their detailed technical specifications. They are internal tests and performed in Gemalto labs in Austin on test platforms.

4.31.1.2 Integration testing - all the pieces work together (Vendor and the Agency)

VENDOR RESPONSE:

Gemalto confirms that our testing plan includes integration testing (Factory Acceptance Tests) as required by the Agency. In out Factory Acceptance Tests (FAT), system tests and sub-system components are integrated together during these tests. During this period, we focus on data and event exchange between systems through their technical interfaces. These tests follow the approved test plans but they are internal and performed in Gemalto labs in Austin, TX on test bed platforms. We encourage State participation during this testing process because it will give the State an early glimpse of the software for review. Colorado, Idaho, Quebec, Maryland, Idaho, New Hampshire, and all four Atlantic Provinces have all gone through this step. At this stage, the systems and their interfaces are considered as Technically Acceptable within a test environment. This is a unique step offered by Gemalto and all of our customers who participated in it have clearly seen the value.

4.31.1.3 Usability testing - user friendly, intuitive application (Vendor and the Agency)

VENDOR RESPONSE:

Gemalto confirms that our testing plan includes usability testing as required by the Agency. Usability testing or User Experience (UX) testing is performed during all phases of the test plan from Unit Tests to Final System Acceptance. Enterprise level software is typically robust with features and functionality but the UX is often overlooked making it clunky or hard to use. We make things fast, simple, and efficient by reducing steps and keystrokes whenever possible to help keep customer processing times to a minimum. We design, develop, and test our software with UX in mind.

4.31.1.4 Functional testing - test scenarios against requirements (Vendor md the Agency)

VENDOR RESPONSE:

Gemalto confirms that our testing plan includes functional testing as required by the Agency. Functional testing is performed at every phase of the test plan to ensure that the software remains fully functional throughout the entire development and testing process through delivery.

4.31.1.5 Performance testing - stress and load (Vendor)

VENDOR RESPONSE:

Gemalto confirms that our testing plan includes performance testing as required by the Agency. We use Soap UI which is testing software which enables to test both functionality and performance in real world conditions. This is performed during User Acceptance Tests (UAT) and Site Acceptance Tests (SAT).

4.31.1.5.1 Vendor to provide mechanism to create load and stress conditions

VENDOR RESPONSE:

Gemalto confirms that we will provide a mechanism to create load and stress conditions. As described above, we use Soap UI which is testing software which enables to test both functionality and performance in real world conditions. This allows us to perform actions such as simulating transaction volumes and increasing them until the system breaks so we know the real works limits or simulate connections speeds between the primary and disaster recovery data center and various field offices (if the State was considering changing or upgrading infrastructure).

4.31.1.6 Testing of external interfaces - communication with other applications, databases, etc. (Vendor and the Agency)

VENDOR RESPONSE:

Gemalto confirms that we will test external interfaces and communications with applications, databases, and any other systems as required. Interface testing is performed during Site Acceptance Tests (SAT). Prior to the SAT, we simulate the external interfaces based on the provided communication specifications for each endpoint with test stubs. Test stubs are programs that simulate/emulate the behaviors of software components or external systems.

4.31.1.7 Continuous regression testing - on-going to determine impact of changes (Vendor and the Agency)

VENDOR RESPONSE:

Gemalto confirms that continuous regression testing is performed throughout the life of the contract for any changes made to the system software or hardware. This could be for the addition of a new model scanner for example, if the model initially provided becomes obsolete and must be replaced or it could be for the implementation of a change request that adds or modifies new functionality. We have a clearly defined Change Control and Configuration Management Process to ensure that any changes to the system will not adversely affection the functionality or performance of the system.

Change Control and Configuration Management Process

A change is defined as:

- an evolution of the definition of the services tendered
- an organizational modification at the customer's end
- a new constraint imposed by the customer

The Change Control Procedure, as well as the other relevant processes, will be formally detailed during the beginning of the project. However, the process will broadly follow the Gemalto process for Change Management and will use the Change Request Form (CRF) to effectively regulate, track and implement the change. The Change Request Form details the new requirements, the solution proposed by Gemalto, the impact in terms of cost and the delivery date.

If there is a change in requirements or new functionality introduced, we need to then follow the Change Request Process and potentially generate a new RQS. Either Gemalto or DMV staff may trigger activities regarding a change in functionality and these typically follow the below process (this applies to items which will have an impact to the Gemalto system):

- First, the request must go through a Change Request (CR) and signoff.
  - New Requirements (RQS) will be submitted to the DMV for review and approval.
- Development and then validation will be performed by Gemalto in Austin.

  - This will be performed on a Test platform and will include non-regression testing.
- Then new version will then be deployed into the staging environment in West Virginia
  - Non regression testing will also be performed here.
- Finally the maintenance will be rolled out to the State-wide system.

4.31.1.8 Backup and recovery testing - ability to conduct a local recovery and disaster recovery (Vendor and the Agency)

VENDOR RESPONSE:

Gemalto confirms that backup and recovery (Disaster Recovery) testing will be performed as required by the Agency. As part of our overall project plan, we have included a **Disaster Preparedness Plan (Disaster Recovery Plan)** as a deliverable. This Disaster Recovery Plan is designed to ensure the continuation of vital business processes in the event that a disaster occurs at any of the DMV sites including the datacenter and central issuance facility. This plan is an on-going process of planning, developing, testing and implementing Disaster Recovery management procedures and processes to ensure the efficient and effective resumption of critical business functions in the event of an unscheduled interruption.

Gemalto's Central Server solution is designed to be flexible and redundant in nature. The proposed solution will be hosted within West Virginia's primary and disaster recovery data centers. The storage systems provided by WVOT hosting Gemalto's Central Server (CS) solution will be configured for redundancy and backup to allow no data loss in the event of a hard drive failure.

Gemalto will work with the DMV and WVOT during the planning phase of the project to clearly define backup and recovery procedures and responsibilities. Typically, our solutions are designed to be used in an automated manner so they do not require manual backups and as such data is not lost due to manual procedures that were not followed.

Section 4, Subsection 4.31.2 - The test plan should include a schedule for when software or other changes will be deployed to the test system and testers must receive documentation of the changes.

VENDOR RESPONSE:

Gemalto confirms that tour test will include a schedule for when software or other changes will be deployed to the test system. Documentation will be updated and provided to the Agency for any changes to the system. Our change request process includes updating and distributing revised documentation including specifications, training materials, or any other applicable documents.

When updates are required, the Gemalto Service Coordinator will schedule updates on the dates proposed by the State, for example: 5am-10am every Sunday after the second Tuesday (i.e. Patch

Tuesday or the 2nd Tuesday of the month is when Microsoft releases security patches). Gemalto maintains a User Acceptance Test (UAT) IT environment where patches and updates will be tested prior to deployment. Testing will follow the agreed upon test plan to ensure updates do not negatively affect the system.

Section 4, Subsection 4.31.3 - The Agency requests a minimum of two (2) weeks' notice to schedule resources for UAT.

VENDOR RESPONSE:

Gemalto confirms that we will work with the Agency to schedule resources for UAT and will provide at least two weeks' notice so the Agency can ensure the appropriate resources are available. This will be managed and coordinated by the Gemalto project manager.

Section 4, Subsection 4.32 - Test Scripts

Section 4, Subsection 4.32.1 - The Vendor should provide and execute a test script, subject to the Agency approval, prior to the implementation of equipment, configuration changes and/or software to the UAT system. The Agency should conduct testing of new equipment and/or software in UAT before any such changes are installed in production.

VENDOR RESPONSE:

Gemalto confirms that we will provide and execute tests scripts prior to the implementation of equipment, configuration changes and/or software to the UAT environment. Test scripts will be provided to the Agency prior to implementation and testing and will be subject to Agency approval as required. Testing will be performed for all new hardware and software in the UAT environment before any changes are deployed to the production environment or in the field. UAT testing is a requirement for all change requests as part of our formal Change Request process and is part of our standard operating procedure.

Section 4, Subsection 4.32.2 - Full regression testing by the Vendor on the QA system should be completed before any change is deployed to the UAT system.

VENDOR RESPONSE:

Gemalto confirms that full regression (non-regression) testing will be performed on our QA system (internal testing environment) prior to deployment into the UAT system as described in the above response to "Requirement 4.31.1.7". It should be noted that we perform regression testing both in the QA system and UAT environment for all changes to the system. Gemalto has a clearly defined Change

Control and Configuration Management Process to ensure that any changes to the system will not adversely affection the functionality or performance of the system.

Change Control and Configuration Management Process

A change is defined as:

- an evolution of the definition of the services tendered
- an organizational modification at the customer's end
- a new constraint imposed by the customer

The Change Control Procedure, as well as the other relevant processes, will be formally detailed during the beginning of the project. However, the process will broadly follow the Gemalto process for Change Management and will use the Change Request Form (CRF) to effectively regulate, track and implement the change. The Change Request Form details the new requirements, the solution proposed by Gemalto, the impact in terms of cost and the delivery date.

If there is a change in requirements or new functionality introduced, we need to then follow the Change Request Process and potentially generate a new RQS. Either Gemalto or DMV staff may trigger activities regarding a change in functionality and these typically follow the below process (this applies to items which will have an impact to the Gemalto system):

- First, the request must go through a Change Request (CR) and signoff.
  - New Requirements (RQS) will be submitted to the DMV for review and approval.
- Development and then validation will be performed by Gemalto in Austin.
  - This will be performed on a Test platform and will include **non-regression testing.**
- Then new version will then be deployed into the staging environment in West Virginia
  - **Non regression testing will also be performed here.**
- Finally the maintenance will be rolled out to the State-wide system.

Section 4, Subsection 4.33 - Documentation for Testing

Section 4, Subsection 4.33.1 - Updated user, and/or administrator manuals should be supplied prior to the testing and acceptance phases of the project.

VENDOR RESPONSE:

Gemalto confirms that updated user guides and/or administrator manuals will be provided prior to the testing and acceptance phases. As part of our project plan and internal processes, documentation updates are made throughout the software development processes to ensure all documentation, including user guides, training materials, and specifications, are updated whenever changes are made to the system's software or hardware. Documentation updates are also included in our standard change request process.

As an output of the IT workshops, Gemalto will provide the DMV with specifications for all components of the solution which will be maintained and updated throughout the delivery of the project including:

- Requirement Specifications (RQS)
    - Image Capture Workstation (ICW) RQS
    - Biometric Investigative Workstation (BIW) RQS
    - Web Reporting System (WRS) RQS
    - Central Server RQS
    - Central Issuance RQS
    - Over the Counter Issuance RQS
    - Data Migration RQS
    - IT and Security RQS

These Requirement Specifications (RQS) will then be used to create the following Acceptance Test Plans (ATP) to ensure all the State's requirements are tested throughout the duration of the project.

- Acceptance Test Plans (ATP)
    - Image Capture Workstation (ICW) ATP
    - Biometric Investigative Workstation (BIW) ATP
    - Web Reporting System (WRS) ATP
    - Central Server ATP
    - Central Issuance ATP
    - Over the Counter Issuance ATP
    - Data Migration ATP
    - IT and Security ATP

Section 4, Subsection 4.33.2 - Vendor should supply written test cases for the Agency resources to use during UAT.

VENDOR RESPONSE:

Gemalto confirms that we will supply written test cases for the Agency resources to use during UAT. We develop test plans and test cases from the Requirement Specifications (RQS) which are an output of the Requirements Workshops. By using the specifications, which are submitted and approved by the Agency, to create the test plan and test cases, we are able to ensure that the requirements of the Agency are met throughout every phase of testing through Unit Tests, Factory Acceptance Tests, User Acceptance Tests, Site Acceptance Tests, Final Acceptance, and even Change Request.

Section 4, Subsection 4.34 - User Acceptance Testing

Section 4, Subsection 4.34.1 - The user acceptance testing (UAT) should be planned and coordinated jointly by the Vendor and the Agency project managers.

VENDOR RESPONSE:

Gemalto confirms that User Acceptance Testing (UAT) will be planned and coordinated by the Gemalto and Agency project managers as required. All project planning and coordination related to the project will be managed by the Gemalto project manager for the duration of the contract.

Section 4, Subsection 4.34.2 - The Vendor should use standard defect tracking tools to track all feedback from testers. Final UAT should end when the system has met the standard of performance for a period of seven (7) consecutive calendar days, as determined by the Agency Project Manager in conjunction with the Agency testers.

VENDOR RESPONSE:

Gemalto confirms that our software development processes includes standard software for defect tracking. We have tools that are used internally to manage these processes during software development, which we cover below. Gemalto confirms that Final System Acceptance (Final UAT) will end once the system has meet the standard of performance for seven (7) consecutive calendar days, as determined by the Agency Project Manager in conjunction with the Agency testers. This requirement will be integrated into our Acceptance and Test Plan and will be integrated into our overall Project Plan and Schedule. In the proposed work plan and project plan, we have accounted for additional time in case any issues or delays arise.

Issue Tracking

Gemalto uses Jira Software which enables our development team to plan, track, and release software updates. Jira Software is a powerful platform that combines issue collection and agile project management capabilities into a single application. Using Jira Software enables Gemalto to plan and organize tasks, workflows, and reports ultimately leading to more efficiently track and resolve issues

Section 4, Subsection 4.34.3 - Prior to final sign-off of user acceptance testing, all stated requirements for functionality should be in place, tested, and working free of bugs or defects, and all system performance testing must be complete and must meet required performance measures.

VENDOR RESPONSE:

Gemalto confirms that all stated requirements for functionality will be in place, tested, and working free of bugs or defects, prior to final acceptance/sign-off of User Acceptance Testing (UAT). This is a standard procedure and is integrated into our overall Acceptance and Test Plan and performed not only at UAT but at every stage of Testing including Unit Tests, Factory Acceptance Tests (FAT), User Acceptance Tests (UAT), Site Acceptance Tests (SAT), Final System Acceptance, and even in Change Request acceptance.

Section 4, Subsection 4.35 - Test Materials

Section 4, Subsection 4.35.1 - The Vendor should provide test materials at no additional cost to the Agency. This includes secure paper for testing production of the temporary DL and card materials for testing the end-to-end process through the central issuance facilities.

VENDOR RESPONSE:

Gemalto confirms that we will provide all required test materials at no additional cost to the Agency. As required, this includes secure paper for testing the temporary DL and card materials for testing end to end testing of enrollment through the issuance process.

Section 4, Subsection 4.36 - Test Systems

Section 4, Subsection 4.36.1 - The Vendor should describe how they will conduct Vendor Quality Assurance Testing.

VENDOR RESPONSE:

Gemalto confirms that we will provide Vendor Quality Assurance (QA) Testing as required by the Agency. It should be noted that our internal quality assurance processes include functional and usability testing throughout the entire Acceptance Test Plan (ATP) so QA testing in not performed at only one point or phase within the process. We internally QA test during the Unit Test phase which is performed for each sub-system and custom developed component. These tests verify the behavior of a component against their detailed technical specifications. They are internal tests and performed in Gemalto labs in Austin on test platforms.

The final, internal Vendor Quality Assurance Testing is performed during the Factory **Acceptance Tests (FAT)** prior to moving the User Acceptance Test phase. During the FAT, system tests and sub-system components are integrated together during these tests. During this period, we focus on data and event exchange between systems through their technical interfaces. These tests follow the approved test plans but they are internal and performed in Gemalto labs in Austin, TX on test bed platforms. We encourage State participation during this testing process because it will give the State an early glimpse of the software for review. Colorado, Idaho, Quebec, Maryland, Idaho, New Hampshire, and all four Atlantic Provinces have all gone through this step. At this stage, the systems and their interfaces are considered as Technically Acceptable within a test environment. This is a unique step offered by Gemalto and all of our customers who participated in it have clearly seen the value.

Section 4, Subsection 4.36.2 - The Vendor should describe how they propose to facilitate Agency User Acceptance Testing prior to full system implementation, and during the first two years of the contract period, as well as being available for on-going testing and training for the life of the contract.

VENDOR RESPONSE:

Gemalto confirms that we will facility Agency User Acceptance Testing (UAT) throughout the duration of the project and throughout the duration of the contract, for any necessary changes or updates to the system. The Gemalto project manager will coordinate and provide resources as necessary to support the State during the UAT and all phases of our overall Acceptance Test Plan (ATP) for the following test phases:

- **User Acceptance Test (UAT) – Alpha Testing**

  To move forward on the testing strategy, a testing (Staging) platform will be installed in the State's premises at DMV It is expected that this environment will be kept afterward for future release's testing, this will be known as the **DMV Staging Environment**.

  At this stage, the solution will be working with test data and producing test driving licenses (test cards).

- **Site Acceptance Tests (SAT) – Beta/Pilot Testing**

  Meanwhile, during the UAT phase, the final production platform environments are installed. Once UAT is successfully approved, the solution will be installed in the production environment. The systems are at this point installed, tested and ready for real production. The full solution will go through Commissioning Tests (Security validation, stress, performance, and failover) to ensure real-environment trouble-free operations.

  Five sites will have been identified in the Transition Plan to be switched over to the new solution with the co-operation of the State for a Pilot Phase operation. Each of the selected field office sites will be installed with the new solution components (Staff will have received prior training on the new solution), and a SAT will be conducted to ensure the solution deployment is functioning as required. The acceptance criteria for each site shall be defined in conjunction with the State. These sites will operate for a Pilot Phase period which will be determined with the DMV to ensure that the system is operating as designed, meets appropriate SLA's and performance is optimal.

  At this stage, the solution will be working with real data and producing real driving licenses (production cards).

- **Final System Acceptance**

  On successful completion of the Pilot Phase, a statewide rollout of the solution shall begin. Once the last deputy registrar office has completed its SAT, the solution will then run in production for

30 consecutive days, which will be heavily monitored and supported by Gemalto project and integration teams. After 7 days of operation and having any outstanding solution issues closed, the State is expected to issue Final Acceptance and receive handover of the solution.

Section 4, Subsection 4.37 - Training Plan Objective

Section 4, Subsection 4.37.1 - The Vendor should describe how they will develop and implement a training plan that specifies the approach and steps to be taken by the Vendor to ensure that the knowledge, skills, and abilities necessary to operate the proposed system are transferred to the Agency's Train-the-Trainers (approximately 75 employees).

VENDOR RESPONSE:

Gemalto will be including a user friendly and detailed training plan as part of our project management documentation. Gemalto recommends hands on just-in-time training to maximize the effectiveness of the training. Coursework and training materials will be provided and training sessions may be videotaped for later use.

Gemalto's training plan is integrated into the overall project and implementation plan by training users alongside solution deployment. Gemalto recommends synchronizing the deployment schedule with the training schedule so that users are trained to use their new solution. By taking this approach, users retain most of the training materials instead of forgetting information between training and using their new solution. Operators will also be able to attend nearby sessions the day before or the day after if they are aware of a scheduling conflict.

Gemalto offers multiple types of training to the DMV. Based on our previous experience deploying similar solutions in other jurisdictions, we have found the following approach to be the most effective methods for the topic and audience including the following:

- **Training manuals and user guides** for all components of the solution
- **Classroom training** for system administration and operations, and **"train the trainer"** classes for the Image Capture Workstation (ICW), Biometric Investigation Workstation (BIW), Web Reporting System (WRS), and Central Server Solution (CS) and system administration
- **Hands on training** in the field and onsite for the Image Capture Workstation (ICW), Biometric Investigation Workstation (BIW), Web Reporting System (WRS), and Central Server Solution (CS) and system administration

Training will be provided for the following components at a minimum:

- **Image Capture Workstation** -This course covers the overview and operation of the Image Capture Workstation. The course is intended to provide users with the skills required to capture applicant signatures, fingerprints and photos. Topics include the sequence of operations, cropping photos, image verification messages and corrective actions. Also covered is verification of application and the viewing of documents and basic trouble shooting.

- **Web Reporting System** -This course covers the overview and operation of the Web Reporting System. The course is intended to provide users with the knowledge required to use the Web Reporting System to generate reports, retrieve images, and access specifics on the status of applicant cards scheduled for production. This course also covers the overview and operation of the business operation solution. The course is intended to provide DMV users with an overview of the components of the business solution and the knowledge required to use the solution to generate useful statistics and repots.
- **Biometric Investigation Workstation** -This course covers the overview and operation of the Biometric Investigative Workstation. The course is intended to provide investigators with the knowledge to address applicant cases that have been flagged as potentially fraudulent. The course covers the methods to review prior applicant history and facial photo analysis techniques to help in the determination of the validity of applicant. Also covered are administrator and supervisor functions and the process for case assignment and management.
- **Central Server - System Management and Maintenance** -This course covers the overview and operation of the Gemalto solution. The course is intended to provide West Virginia's IT professionals with an overview of the components of the Gemalto solution and the inter-working of the components with the application software.

As part of the deliverables, Gemalto will deliver a Training Plan for review and approval. We will also provide draft Operations, Maintenance Manuals, and Trouble Shooting Guides for review and approval prior to release. Training manuals will be develop and provided for each specific part of the credential issuance process.

Gemalto confirms that our training plan and classes address the various types and levels of users within the solution. In addition to classes that cover basic operations for the Image Capture Workstation and Biometric Investigative Workstation, we offer more in-depth courses for the administrators and the management and maintenance of the overall solution.

We break down the types of training for the various audiences in the following table:

Course Target Audience	Image Capture Workstation	Web Reporting System	Biometric Investigative Workstation	•Central Server - System Management and Maintenance
DMV Front Office Personnel	Required	required		
DMV Administrative Personnel	Required	required	required	
DMV--Investigators			required	
DMV-IT	recommended	required	required	required
DMV Trainer	Required	required	required	recommended

We also include various sessions throughout the delivery of the project as described below. We offer different levels of classes for in intended audience and cover the solution in different levels in depth based on session and the audience. For example, we provide a high level training during UAT to give the DMV staff the option to view all of the components of the solution. This also gives the DMV the opportunity to provide feedback on our training so adjustments can be made if necessary. During the deployment of the solution, we offer three levels of training including Basic Operations for the Staff at headquarters, Administration which covers the solution in greater detail, and a separate technical training which is geared towards the DMV IT staff. Basic operations training is also performed in the field offices during the pilot phase and also as the solution is deployed and goes live state-wide.

Session	Planned Audience	Total hours	Courses	Delivery
UAT & Performance Testing	Operations staff designated by DMV	8	Image Capture Workstation, Web Reporting System, Biometric Investigation Workstation	DMV Classroom
Basic Operation - Front Office	DMV front office operation staff, Trainers	4	Image Capture Workstation	DMV Classroom
Administration - Front Office	DMV front office Administrators, Trainers	8	Image Capture Workstation, Web Reporting System, Biometric Investigation Workstation	DMV Classroom
Technical Training	System Management and Maintenance, Trainers	16	Central Server - System Operation, Management and Maintenance	DMV Classroom

The following are the planned sessions on Go Live day:

Session	Planned Audience	Total hours	Courses	Delivery
Basic Operation - Front Office	DMV operation staff	4 per site	Image Capture Workstation	On site

Section 4, Subsection 4.38 - Training Guide Objective

Section 4, Subsection 4.38.1 - The Vendor should describe how their training guide will be made available to all Agency employees.

VENDOR RESPONSE:

Gemalto will provide detailed documentation, user guides, manuals, and training materials during project delivery both in electronic format and hard copy as required for DMV approval. This is marked as a deliverable as part of our overall project plan. We provide drafts to the DMV for review during the Factory Acceptance Tests (FAT) and User Acceptance Tests (UAT) as the training materials are revised throughout project delivery.

Documentation will be maintained and updated throughout the life of the contract. Gemalto's change request process includes evaluation and revision of all applicable documentation and user guides. The following guides allow DMV staff members to make a comprehensive analysis of our hardware and software:

User Guides/Training Materials

- Image Capture Workstation (ICW) User Guide
- Biometric Investigation Workstation (BIW) User Guide
- Web Reporting System (WRS) User Guide
- System Administration and Management – Central Server (CS) User Guide
- IT Operations and Maintenance – Central Server (CS) User Guide

Draft Operations and Maintenance Manuals will be submitted to the DMV prior to the implementation of the solution will be updated prior to first use in the Pilot site training based on DMV feedback and any updated to the solution. All Operations and Maintenance Manual deliveries will be in the preferred format of the DMV.

The general content of the Guide(s) is expected to contain basic information

- Introduction to the system or subsystem
- Basic features
- Basic operations and functionality with step by step instructions
- Screenshots
- Workflows for each business process
- Basic troubleshooting
- Basic maintenance
- FAQs

Section 4, Subsection 4.39 - Training Guide

Section 4, Subsection 4.39.1 - The training guide should include

VENDOR RESPONSE:

Gemalto confirms that the User Guides and Training Materials will include all of the requirements listed below.

4.39.1.1 An introduction to the Digital Driver's License application systems

VENDOR RESPONSE:

Gemalto confirms that our User Guides and Training Materials will include an introduction to the Digital Driver's License application systems and an overview of the entire solution.

4.39.1.2 A layman's explanation of the function of each component of the system

VENDOR RESPONSE:

Gemalto confirms that our User Guides and Training Materials will include layman's explanations of the functions of each component of the system. The guide(s) will be written in practical and functional business use case manner with the anticipated audience to be familiar with working in a typical office environment and a beginner's level of understanding of Microsoft windows. The guide(s) will be sufficiently illustrated and contain relevant examples for all employees to quickly grasp the materials.

4.39.1.3 Systematic operating instructions for system components

VENDOR RESPONSE:

Gemalto confirms that our User Guides and Training Materials will include systematic operating instructions for system components. As described in the above response to "Section 4, Subsection 4.38.1", the materials will include basic operations and functionality with step by step instructions, screenshots, and workflows for each business process including all necessary operating instructions.

4.39.1.4 Procedures for system start-up, daily operation, and end-of-day transactions

VENDOR RESPONSE:

Gemalto confirms that our User Guides and Training Materials will include procedures for system start-up, daily operation, and end-of-day transactions. As described in the above response to "Section 4, Subsection 4.38.1", the materials will include basic operations and functionality with step by step instructions, screenshots, and workflows for each business process including all necessary operating instructions.

4.39.1.5 Guidelines for maintenance, problem solving, troubleshooting, back-up, and recovery

VENDOR RESPONSE:

Gemalto confirms that our User Guides and Training Materials will include procedures for system start-up, daily operation, and end-of-day transactions. As described in the above response to "Section 4, Subsection 4.38.1", the materials will include basic operations and functionality with step by step instructions, screenshots, and workflows for each business process including all necessary operating instructions.

Section 4, Subsection 4.40 - User Operations Manuals Objectives

Section 4, Subsection 4.40.1 - The Vendor should describe how they will provide documentation for functional specifications and user manuals for all system components.

VENDOR RESPONSE:

Gemalto confirms that we will provide documentation for the functional specifications and user manuals for all systems and components of the solution. As an output of the workshops, Gemalto will provide the DMV with specifications for all components of the solution which will be maintained and updated throughout the delivery of the project including:

- Requirement Specifications (RQS)
  - Image Capture Workstation (ICW) RQS
  - Biometric Investigative Workstation (BIW) RQS
  - Web Reporting System (WRS) RQS
  - Central Server RQS
  - Central Issuance RQS
  - Over the Counter Issuance RQS
  - Data Migration RQS
  - IT and Security RQS

- Acceptance Test Plans (ATP)
    - Image Capture Workstation (ICW) ATP
    - Biometric Investigative Workstation (BIW) ATP
    - Web Reporting System (WRS) ATP
    - Central Server ATP
    - Central Issuance ATP
    - Over the Counter Issuance ATP
    - Data Migration ATP
    - IT and Security ATP

In addition to the requirements and specifications, Gemalto will provide detailed documentation for all software and hardware provided as part of the solution. This will include user guides, manuals, and training materials that will be provided during project delivery. Documentation will be maintained and updated throughout the life of the contract. Gemalto's change request process includes evaluation and revision of all applicable documentation and user guides. The following guides allow DMV staff member make a comprehensive analysis and use of our hardware and software:

User Guides:

- Image Capture Workstation (ICW) User Guide
- Biometric Investigation Workstation (BIW) User Guide
- System Administration and Management – Central Server (CS) User Guide
- IT Operations and Maintenance – Central Server (CS) User Guide

This approach to providing a comprehensive set of specifications and documentation is a standard component of our project plan approach and has most recently been provided to all of Canada's Atlantic Provinces including Newfoundland and Labrador, Nora Scotia, New Brunswick, and Prince Edward Island.

Section 4, Subsection 4.40.2 - The Vendor should explain how user operations manuals will be made accessible as a reference document.

VENDOR RESPONSE:

Gemalto can provide user operations manuals and users guides in both printed and digital format. We are able to host the files so they are digitally accessible within our customer SharePoint site or we can provide the files to the DMV so they may be hosted internally.

Section 4, Subsection 4.41 - Technical Documentation Objective

Section 4, Subsection 4.41.1 - Vendor should explain how they will deliver and maintain technical documentation that describes the operation of all system components, including their interfaces to Agency or third-party systems. This documentation should include:

VENDOR RESPONSE:

As described above, Gemalto will provide and maintain technical documentation for all components of the overall solution that describes the operations of all system components including interfaces to Agency and third party systems. As an output of the IT workshops, Gemalto will provide the DMV with specifications for all components of the solution which will be maintained and updated throughout the delivery of the project including:

- Requirement Specifications (RQS)
    - Image Capture Workstation (ICW) RQS
    - Biometric Investigative Workstation (BIW) RQS
    - Web Reporting System (WRS) RQS
    - Central Server RQS
    - Central Issuance RQS
    - Over the Counter Issuance RQS
    - Data Migration RQS
    - IT and Security RQS

Our Project Management Processes all have documentation maintenance and updates integrated to ensure that whenever there is a change to the system, specifications, user guides, and training materials will be updated to reflect the change. This is also integrated into our Change Request Process to ensure that documentation does not become outdated throughout the life of the contact.

4.41.1.1 Complete Data Dictionary with all tables, fields, and values

VENDOR RESPONSE:

Gemalto confirms that a complete Data Dictionary with all tables, fields, and values will be included for all documentation. This a standard component of the documentation provided by Gemalto as part of overall project delivery and is typically included in the beginning or all Requirement Specifications, User Guides, Acceptance Test Plans, or Training Materials. .

4.41.1.2 System Architecture Diagrams

VENDOR RESPONSE:

Gemalto confirms that system architecture diagrams will be included and clearly defined as part of the specifications. This a standard component of the documentation provided as part of overall project delivery.

4.41.1.3 Communication Protocols

VENDOR RESPONSE:

Gemalto confirms that communication protocols will be included and clearly defined as part of the specifications. This a standard component of the documentation provided as part of overall project delivery.

4.41.1.4 Listing of all data center equipment with DNS and IP information, operating systems, and software information including versions

VENDOR RESPONSE:

Gemalto confirms that Listing of all data center equipment with DNS and IP information, operating systems, and software information including versions will be included. This a standard component of our documentation. As the solution will be hosting on infrastructure provided by the Agency in the State's primary and disaster recovery datacenter, some of this information will need to be provided by the Agency or other State IT staff. Gemalto will collaborate with WVOT to ensure that all required information is included within our documentation.

4.41.1.5 Functional Specifications for the interaction of all components

VENDOR RESPONSE:

Gemalto confirms that functional specifications for the interaction of all components will be included. This a standard component of the documentation provided as part of overall project delivery.

Section 4, Subsection 4.42 - Updates to Documentation Objective

Section 4, Subsection 4.42.1 - The Vendor should describe how they will supply and or update all training, operations, or troubleshooting manuals when a system is replaced, or software is upgraded creating a significant change to a process.

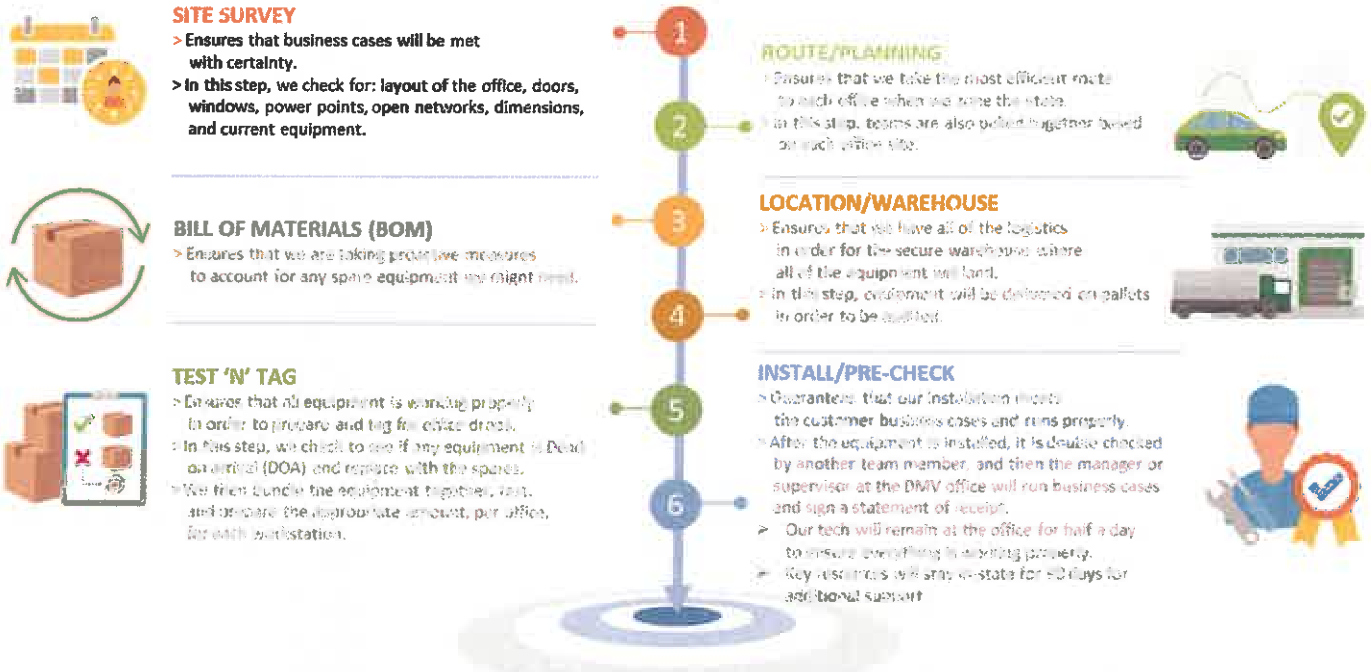
VENDOR RESPONSE:

Gemalto confirms that all training, operations, and troubleshooting manuals will be updated to reflect any changes or updates to our systems and software. Documentation will be maintained and updated throughout the life of the contract. Gemalto's change request process includes evaluation and revision of all applicable documentation and user guides.

Section 4, Subsection 4.43 - Implementation Plan Objective

Section 4, Subsection 4.43.1 - The Vendor should detail their implementation plan for every component of the system. The implementation plan should ensure all equipment and system components can be installed and functional prior to the target go live date of the system.

VENDOR RESPONSE:



SITE SURVEY

> Ensures that business cases will be met with certainty.

> In this step, we check for: layout of the office, doors, windows, power points, open networks, dimensions, and current equipment.

BILL OF MATERIALS (BOM)

> Ensures that we are taking proactive measures to account for any spare equipment we might need.

TEST 'N' TAG

> Ensures that all equipment is working properly in order to prepare and tag for office drops.

> In this step, we check to see if any equipment is Dead on arrival (DOA) and replace with the spares.

> We then bundle the equipment together, test, and prepare the appropriate amount, per office, for each workstation.

ROUTE/PLANNING

> Ensures that we take the most efficient route to each office when we zone the state.

> In this step, teams are also pulled together based on each office site.

LOCATION/WAREHOUSE

> Ensures that we have all of the logistics in order for the secure warehouse where all of the equipment will land.

> In this step, equipment will be delivered on pallets in order to be audited.

INSTALL/PRE-CHECK

> Guarantees that our installation meets the customer business cases and runs properly.

> After the equipment is installed, it is double checked by another team member, and then the manager or supervisor at the DMV office will run business cases and sign a statement of receipt.

- Our tech will remain at the office for half a day to ensure everything is working properly.
- Key resources will stay in-state for 30 days for additional support

FIGURE 60: IMPLEMENTATION & TRANSITION PLANNING KEY ELEMENTS

In our experience, thorough planning of all implementation and deployment activities help ensure the success of the overall project and deployment and we perform the following tasks:

- **Site Surveys** - To be able to perform a statewide deployment we setup state office surveys to better understand the requirement's ahead of time. The objective of a site survey is to document the current equipment layout and identify all electrical and network port locations that may serve for the future deployment. There will also be as part of the report 360 degree photos for visual reference, a 2D diagram with equipment position and legend along with any observations that may hinder or improve the deployment phase when it will be executed. Our approach has been much appreciated by our customers because it also provided visibility to areas where they wanted to invest in more workstations to meet a growing demand in specific field offices. Meetings will be held following the competition of the site surveys all reports will be shared with the state to be able discuss and confirm the relevant needs and impacts, followed by an action plan. All decisions will be communicated back to Gemalto's Project Manager who will then inform the relevant Stake Holders of the decisions.

- **Equipment Procurement and Inspection -** Prior to pilot all the needed devices will be purchased and tested and if required any updates applied. The objective is to ensure both the pilot and deployment go smoothly when it comes to device conformity. Once approved all device will be allocated as per required office quantity and stored ready for shipment.
- **Preparation for pilot and deployment –** A checklist will be compiled by Gemalto for the deployment team to follow as part of the installation. The check list will be executed prior to deployment on multiple occasions by different technicians. The objective is to ensure that there are no steps overlooked and establish a deployment timeline.
- **State deployment routes –** Meetings will be held with the state to discuss office workstation locations and possible state routes along with office hours if business and where possible which offices can be upgraded during the day. The objective is to optimize the deployment and reduce the amount of time it takes the state to move to the new solution.
- **State representatives per office –** Before the pilot phase, the state will be required to provide a list of all state office representatives along with their contact information and a backup contact. The objective will be that these staff will be receiving the deployment technicians at their office and will also be responsible for the Asset log sign offs and testing of the new solution once all installed.

Pilot Phase

Gemalto will identify a few sites with the DMV as part of the Transition Plan to be switched over to the new solution with the co-operation of the State for a Pilot Phase operation. Each of the selected field office sites will be installed with the new solution components (Staff will have received prior training on the new solution), and a SAT will be conducted to ensure the solution deployment is functioning as required. The acceptance criteria for each site shall be defined in conjunction with the State. These sites will operate for a Pilot Phase period which will be determined with the DMV to ensure that the system is operating as designed, meets appropriate SLA's and performance is optimal.

Statewide Deployment

Once the pilot offices are operational, we will begin to deploy to the other offices by region. We look for minimal support from the DMV during this period. We will need to get access to each of the offices on an agreed upon schedule. We may also need support during the testing of the offices once all is established. Once we have an office installed and ready for production, we will work with the staff in that location on the proper operation of the equipment and software. Again, we will work with the DMV on a schedule for minimum impact. We will provide a checklist (contents to be agreed by the DMV) upon successful implementation that ensures we have someone from the DMV verify that all was implemented according to the plans provided.

Section 4, Subsection 4.44 - On-site Training

Section 4, Subsection 4.44.1- As part of the Vendor's Training Plan, the Vendor should describe how they will conduct on-site Train-the-Trainer instruction. This should include duration, methods, materials provided by the Vendor, materials required of the Agency and number of trainers conducting the training.

VENDOR RESPONSE:

As described in the above response to "Requirement Section 4, Subsection 4.37.1" Gemalto will provided onsite training throughout the delivery of the project including Train the Trainer sessions. Our training plan and classes address the various types and levels of users within the solution. In addition to classes that cover basic operations for the Image Capture Workstation and Biometric Investigative Workstation, we offer more in-depth courses for the administrators and the management and maintenance of the overall solution which are ideal for training trainers at the DMV headquarters in addition to any other staff that require training.

We break down the types of training for the various audiences in the following table:

Course Target Audience	Image Capture Workstation	Web Reporting System	Biometric Investigative Workstation	•Central Server - System Management and Maintenance
DMV Front Office Personnel	Required	required		
DMV Administrative Personnel	Required	required	required	
DMV–Investigators			required	
DMV-IT	recommended	required	required	required
DMV Trainer	Required	required	required	recommended

We also include various sessions throughout the delivery of the project as described below. We offer different levels of classes for in intended audience and cover the solution in different levels in depth based on session and the audience. For example, we provide a high level training during UAT to give the DMV staff the option to view all of the components of the solution. This also gives the DMV the opportunity to provide feedback on our training so adjustments can be made if necessary. During the deployment of the solution, we offer three levels of training including Basic Operations for the Staff at headquarters, Administration which covers the solution in greater detail, and a separate technical training which is geared towards the DMV IT staff. Basic operations training is also performed in the field offices during the pilot phase and also as the solution is deployed and goes live state-wide.

Session	Planned Audience	Total hours	Courses	Delivery
UAT & Performance Testing	Operations staff designated by DMV	8	Image Capture Workstation, Web Reporting System, Biometric Investigation Workstation	DMV Classroom
Basic Operation - Front Office	DMV front office operation staff, Trainers	4	Image Capture Workstation	DMV Classroom
Administration - Front Office	DMV front office Administrators, Trainers	8	Image Capture Workstation, Web Reporting System, Biometric Investigation Workstation	DMV Classroom
Technical Training	System Management and Maintenance, Trainers	16	Central Server - System Operation, Management and Maintenance	DMV Classroom

The following are the planned sessions on Go Live day:

Session	Planned Audience	Total hours	Courses	Delivery
Basic Operation - Front Office	DMV operation staff	4 per site	Image Capture Workstation	On site

Section 4, Subsection 4.45 - Account Manager for Operations

Section 4, Subsection 4.45.1 - Vendor should provide the Agency one primary person who will be responsible for the long-term management of the contract and service level agreement. Explain the role the account manager will have in the escalation process for issues that cannot get resolved through normal processes and within agreed upon timelines.

VENDOR RESPONSE:

Gemalto confirms that we will provide the Agency with a primary person (Service Delivery Manager - SDM) who will be responsible for the long term management of the contract and service level agreement. The Gemalto Account Executive will serve as the primary point of contact for all business related issues for both pre and post deployment activities. We will also provide a Support & Maintenance Manager (Manager of SDM) who will oversee the process and quality aspects of all support activities for both preventative and remedial maintenance for the entire Gemalto solution. The Gemalto Account Executive will remain the primary point of contact for the Agency and will directly manage the escalation process for issues that cannot be resolved through normal processes and within agreed upon timelines.

SERVICE LEVEL AGREEMENT

Section 4, Subsection 4.46 - Replacement of Equipment / Inventory of Spares

Section 4, Subsection 4.46.1 - The Vendor should explain how their proposal will address chronic hardware issues. (Requires a support call and occurs three (3) or more times within a twelve (12) month period).

VENDOR RESPONSE:

Gemalto confirms that we will address any chronic hardware issues for any hardware which requires a support call and occurs three (3) or more times within a twelve (12) month period. Gemalto, as part of our Support Service Officer, allocates a Service Delivery Manager who will oversee all of our support operations. The staff will track and manage all issues including chronic hardware issues. We will also provide root cause analysis and provide updates to user guides and training materials if issues are resulting from operator error.

Section 4, Subsection 4.46.2 - If a repair or maintenance problem is systemic, i.e. occurring system wide, the Vendor should provide a system wide solution, which may include statewide upgrade or replacement of all units.

VENDOR RESPONSE:

For any systemic issues that may arise, Gemalto will provide a system wide solution, which may include upgrades or replacement of all units. Gemalto, as part of our Support Service Offer, allocates a Service Delivery Manager (SDM) who will oversee all of our support operations for your account The SDM will track and manage all issues that are unresolved including developing action plans, mitigating risks, and executing actions to address unresolved warranty and maintenance problems. We also have a clearly defined support escalation plan to address any unresolved or systemic incidents.

Section 4, Subsection 4.46.3 - The Vendor should explain how their proposal will address equipment to be used as replacement units, as needed for service calls.

VENDOR RESPONSE:

As part of our standard support process, we will provide standby spare equipment as needed for service calls, as we do today for the State of West Virginia .This spare equipment will be managed by our support technicians and if space is available, we will keep some spare units onsite like we do today enabling the state staff to quickly replace simple items like temporary DL/ID printers. This availability of standby spares ensures that any service downtime will be minimized or repaired in minutes (Simply removing the defective unit and replacing it for a working spare).

Section 4, Subsection 4.47 - Service Response Times

Section 4, Subsection 4.47.1 - The Vendor should detail their proposed service response plan for dealing with issues related to CIF, ICW, CIDS, CIS and FRS. This should include a response in the number of working hours expected after notification based on the component and severity of the fault.

VENDOR RESPONSE:

During the specifications phase of the project a Work Package is dedicated to defining a mutually agreed upon Service Level Agreement (SLA) in terms of providing assistance, warranty and support and system availability in collaboration with the State DMV.

The objective of the work package is to mutually define the specifics of the required support and detail the measures that will ensure Gemalto will meet (Certify) the expectations of the West Virginia DMV for service delivery.

Sample SLA

	Service	Description
Services Maintenance	Correction testing	Gemalto will perform any type of testing, including the non-regression and compatibility, on every Patch and Minor version before its delivery to the Licensee.
	Bug Fixing	Gemalto will deliver the remedies and workarounds for related Software Faults which may be in the form of a corrected copy of the Supplied Software or a temporary fix or patch until a New Version of the Supplied Software or final fix can be delivered and installed.
	SW Maintenance Release and New Release Notification	Gemalto will inform Licensee on forthcoming Maintenance and New Versions deliveries as soon as practicable.
	SW Corrective Release Delivery	Gemalto will provide to the Licensee Corrective Releases of the Gemalto Software, including related documentation and installation on Licensee system. Those Corrective Releases are delivered free of charge. It is under Licensee responsibility to install them on corresponding platforms.
	Preventive Maintenance	Preventive Maintenance guarantees to notify or alarm about all events related to the software that may have an impact on the services offered by the system or may have an impact on the performance level of the system as detailed in this Agreement. After every Preventive Maintenance, Gemalto will submit a report to the designated recipient of Licensee, with if applicable, the list of corrective actions and alarms (specific to each identified fault or problem) to be implemented. Gemalto will define the list of covered operations, periodicity and operating mode.
	Functional Test Environment Hold by Gemalto	Gemalto will create and maintain Licensee's image platform in Gemalto premises for investigation and testing purposes. The image will reproduce exhaustive Software versions and configuration. The specific data related to Production Environment will not be included, neither the Hardware configuration.
Services Support	On-line ticketing system	Gemalto provides web-based access to the internal Ticketing Application allowing Licensee to place and follow up any Customer Service Requests.
	Phone Assistance (8x5)	Technical Support Phone Assistance (Help Desk) is a service to enable Licensee to obtain a quick response to theirs Customer Service Requests. It should be used for every severe CSR. In all other cases it should be used only as a backup solution to On-line ticketing system. The access to this service is limited within 8x5 coverage and based on Gemalto local office capability business hours. In any case the calls received and answered outside this service window will be logged to On-line ticketing system the next business day.
	Remote Technical Support	Gemalto will deliver the technical Support and Maintenance services linked to the execution of the S&M Services Agreement based on Remote Access and phone communication with the Licensee.
	Documentation, Support Tools and Specifications Update	Gemalto delivers to Licensee, free of charge, the related Documentation and support Tools and guarantee to deliver any future updates of the Documentation and the Specifications.
	Collaborative Support for third Parties Software	Gemalto offers under this Support and Maintenance Agreement the Support services for embedded third party Software which are defined in the SLA agreement. For third party Software Gemalto will execute Support Level 1 and 2.
	Escalation Process	Gemalto delivers the access to the Licensee on escalation process which consists of providing the appropriate level of resources to resolve a request initiated by Licensee, when the contractual elements defined by the S&M Agreement are not met by Gemalto.
	Phone Assistance time coverage extension (24x7)	Technical Support Phone Assistance time coverage are extended to 7 days a week (7/7), 24 hours a day (24/24), 365 days a year. The extended time coverage shall be used by Licensee only for the Severe and Serious CSR.
Preventive Information, Meeting and Reporting	Customer Satisfaction Monitoring	Gemalto Customer Care team will conduct the surveys at such intervals as Gemalto may determine, to measure the Licensee satisfaction with the Support and Maintenance services provided. The results of this survey will be shared across the relevant Gemalto and Licensee teams in order to drive improvements for delivered service quality
	Regular Remote Technical Review	Gemalto will perform regular technical review of the CSR initiated by Licensee and general performance of Gemalto Platform covered by the S&M Agreement.
	Bi-Annual On-Site Technical Review	Gemalto will perform twice a year on-site technical review of the Software covered by the S&M Agreement and any other elements of the system which may influence the

		services offered by the system or may have an impact on the performance level of Gemalto services as detailed in the S&M Agreement. This Service is managed by Customer S&M Manager when applicable.
	Customer Service Requests Reports and Metrics	Gemalto will deliver to Licensee on monthly basis, a report containing: □ The total number of CSR opened and closed each month; □ The status on outstanding open CSR (incident short description, severity level, status) from the previous period (per month), if any.

Support SLA

We have included a sample SLA below. Gemalto will work with the DMV during the planning phase of the project to provide a clearly defined Support and Maintenance Plan including clear definitions of SLA's for all components of the system. This is included as its own deliverable and Work Package within our overall Project Plan.

Production	**SLA – Level of Commitment**		
	Response Time	**Restoration Time**	**Resolution Time**
Severity 1 (Major)	8 Hours	12 Hours	24 Hours
Severity 2 (Serious)	24 Hours	48 Hours	96 Hours
Severity 3 (Minor)	48 Hours	96 Hours	1440 Hours

Example SLA Commitment Table – This is for illustrative purposes only and does not constitute a commitment.

Section 4, Subsection 4.48 - Help Desk Support

Section 4, Subsection 4.48.1 - The Vendor should explain their Help Desk capabilities and responsibilities. This should include hours of operation, response times, remote access requirements, field service technician involvement, and escalation process.

VENDOR RESPONSE:

In Office Support

The in-office systems of computer software and peripherals (Camera towers and Signature Pads) are serviced by the Gemalto local technicians. Gemalto uses high quality peripherals to reduce both maintenance and repairs. Gemalto local technicians follow the quarterly maintenance cycles along with history data accumulated across Gemalto jurisdictions for service methods and intervals. **Gemalto will keep our current Field Office Technicians who currently support the State and are familiar with State staff, locations, and operations.**

For software updates and maintenance, Gemalto usually provides a fully automated method of pulling updates to our systems throughout the DMV Domain. We propose Microsoft System Center Configuration Manager (SCCM) a powerful tool allowing distribution of executable programs and ancillary files, distribution and execution of SQL scripts, registry updates, etc. Those systems are configurable to allow the update to be pulled to a single office, multiple offices, or all offices.

SCCM tracks all updates for each individual workstation. At any time, authorized users have the ability to centrally manage the current software versions throughout each of the West Virginia offices. The Automated Update System's main screen shows the office number, workstation number, software release mode (test, quality control, and production), current software version, and last update date/time. Please note that Gemalto can also capitalize on existing State SCCM installations for update distribution.

Gemalto uses both our on-site support team to address and monitor any issues being reported by the DMV and the ability to remotely connect to an office to view Windows performance logs and current system status. Using Windows built in resource monitoring and performance monitoring tools, Gemalto can quickly evaluate the health of a system and address any required updates, configurations or repairs required.

Gemalto has implemented additional monitoring software for remote access that is used internally for reporting, system monitoring, and performance alerts. Gemalto plans to integrate this as part of our on premise suite for customers and will utilize this approach for the DL/ID implementation.

Depending on the West Virginia IT domain constraints, Gemalto may also be able to use additional tools to further perform remote monitoring and access.

Central Server (CS) Support

Gemalto uses monitoring tools to track the system performance and health. This includes resource performance tracking of the physical servers in terms of memory and CPU utilization with alerts set for threshold conditions. Additionally, Gemalto monitors the network conditions for Gemalto local servers and infrastructure for both security and performance using a suite of tools from Quest and Sophos.

All of the server software is also set to be updated automatically as new software releases become available through the software vendors.

The storage systems are configured for redundancy and backup to allow no data loss in the event of a hard drive failure. The drives can be hot swapped without any impact on the system performance.

Central Issuance Facility

Gemalto's central issuance facility uses multiple, identical high volume/high reliability modular printers for production. Preventative maintenance is done on both a system level through general cleaning, calibration and adjustments and for each module depending the total card count. Gemalto uses in-house support personnel to perform the maintenance. Gemalto also continually monitors product output for quality and runs periodic quality control tests to exercise and verify all modules of the printing system

Toll Free Help Desk Line

Gemalto confirms toll free telephone support will be provided to the DMV as required. Gemalto will be capitalizing on a centralized, dedicated toll-free number, ticketing system, and distributed field technicians to ensure that calls are responded within the agreed upon SLA. This central number will serve as the first level of support, will manage the field technician dispatching, and will be staffed Monday through Friday 8 A.M. (EST) to 6 P.M. (EST), with helpdesk phone support extended for 24x7 support. In addition, Gemalto will provide an emergency call list for contacts (primary and secondary contacts) throughout the life of the contract.

Online Help

Gemalto will provide easy to access online computerized help through Gemalto's STiM (Support Ticketing Management) system. In addition to the call center and help desk, Gemalto will provide our support portal that is accessible via a web browser and provides the ability to sort based on specific data including location, time, date, severity and system component. Support tickets can be created by Gemalto Support Team or by the DMV for any verbal or electronic service requests.

The DMV and Gemalto Support Teams will have access to the system to enter a new ticket, search for an existing ticket, search for a solution, and to get statistics on ticket resolution. At any given time, the DMV and Gemalto Support Team can see the state of an open ticket in addition to track the resolution time compared to the SLA.

Gemalto has additional resources available if the first level of support cannot resolve an issue. Our support structure has multiple levels and a defined escalation process is described below. Please note that we have separate escalation processes to address business related issues.

Issue Resolution Process

Below is a high level description of the Support and Maintenance which includes issue resolution within 4 hours depending on the office as specified by the DMV:

Service Level 1: (Gemalto's helpdesk)

- DMV creates a ticket through Gemalto's STiM (Support Ticketing Management) system, or
- DMV places a call through the 1-800 number to Gemalto's service helpdesk.
- Gemalto Helpdesk service will assist by resolving the DMV issue remotely. If the issue cannot resolved by the help desk, the ticket will then be escalated to Service Level 2.

Service Level 2: (Gemalto's Technicians)

- Gemalto's helpdesk will escalate the ticket to Gemalto's technicians.
- Gemalto's technicians will assist in resolving the issue by phone, remote or setting up an estimated time of arrival to the DMV site.
- If Gemalto's technician is not able to find a solution to the issue within an agreed time between both parties, the technician will escalate the issue to Service Level 3.

Service Level 3: (Gemalto's Regional Manager of Operations)

- Gemalto's technicians will escalate the issue to Operations Manager.
- Gemalto's Operation Manager will assist in resolving issue by phone, remote or setting up an estimated time of arrival on an onsite visit to the DMV site

Section 4, Subsection 4.49 - Help Desk Reporting System

Section 4, Subsection 4.49.1 - Vendor should explain their help desk reporting system used to report, log, and track support issues, including the how the Agency will access the system, automatic tracking of issues and notification alerts, and report generation capabilities.

VENDOR RESPONSE:

Gemalto will provide easy to access online computerized help through Gemalto's STiM (Support Ticketing Management) system. In addition to the call center and help desk, Gemalto will provide our support portal that is accessible via a web browser and provides the ability to sort based on specific data including location, time, date, severity and system component. Support tickets can be created by Gemalto Support Team or by the DMV for any verbal or electronic service requests.

The DMV and Gemalto Support Teams will have access to the system to enter a new ticket, search for an existing ticket, search for a solution, and to get statistics on ticket resolution. At any given time, the DMV and Gemalto Support Team can see the state of an open ticket in addition to track the resolution time compared to the SLA.

Gemalto cam provide reports to fully explain system performance, maintenance actives, and downtime for system components. System performance reporting is a standard requirement and is currently provided to many of our customers. Gemalto will work with DMV during the planning phase and provide a Support and Maintenance Plan for DMV approval which will include all reporting requirements related to support. This will be managed by the Gemalto support manager throughout the duration of the contract and any extensions. Please note that Gemalto's STiM (Support Ticketing Management) system includes reporting capabilities so the DMV can look at system support activity and performance vs. SLA's at any point. We have included some sample support reports below:

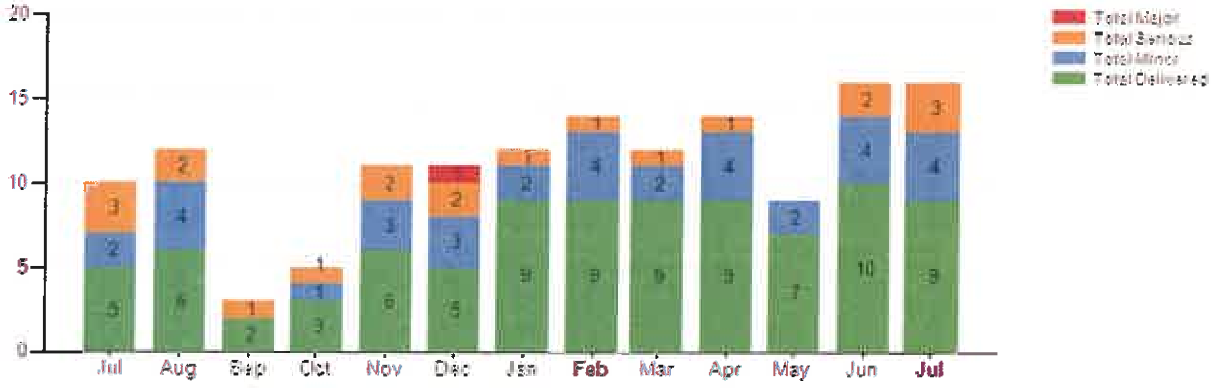
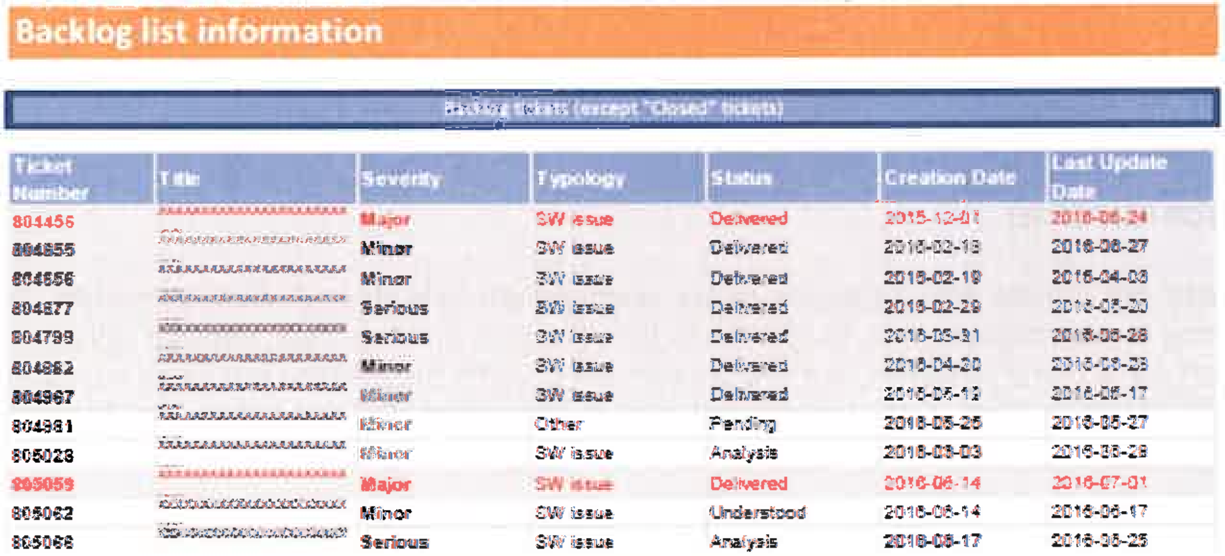


FIGURE 61: SAMPLE REPORT - BACKLOG ANALYSIS



Backlog list information

Backlog tickets (except "Closed" tickets)

Ticket Number	Title	Severity	Typology	Status	Creation Date	Last Update Date
804456	[illegible]	Major	SW issue	Delivered	2015-12-01	2016-06-24
804655	[illegible]	Minor	SW issue	Delivered	2016-02-18	2016-06-27
804656	[illegible]	Minor	SW issue	Delivered	2016-02-19	2016-04-08
804677	[illegible]	Serious	SW issue	Delivered	2016-02-29	2016-05-20
804799	[illegible]	Serious	SW issue	Delivered	2016-03-31	2016-06-28
804862	[illegible]	Minor	SW issue	Delivered	2016-04-20	2016-06-23
804967	[illegible]	Minor	SW issue	Delivered	2016-05-12	2016-06-17
804981	[illegible]	Minor	Other	Pending	2016-05-25	2016-05-27
805023	[illegible]	Minor	SW issue	Analysis	2016-06-03	2016-06-28
805059	[illegible]	Major	SW issue	Delivered	2016-06-14	2016-07-01
805062	[illegible]	Minor	SW issue	Understood	2016-06-14	2016-06-17
805066	[illegible]	Serious	SW issue	Analysis	2016-06-17	2016-06-25

FIGURE 62: SAMPLE REPORT - BACKLOG DETAIL

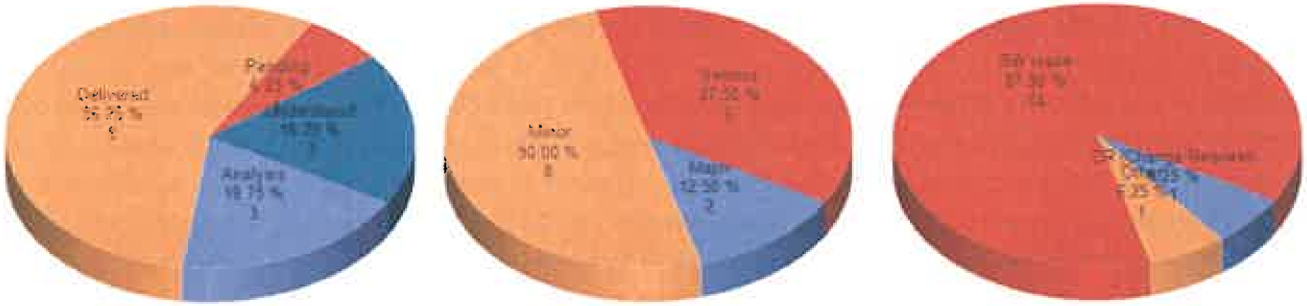


FIGURE 63: SAMPLE REPORT - BACKLOG STATUS, BACKLOG SEVERITY, AND BACKLOG TYPE

** Please note that the above screenshots are a sample of a previously delivered solution and the final user interface design will be specified during project specification workshops*

Section 4, Subsection 4.50 - Implementation Plan

Section 4, Subsection 4.50.1 - The implementation plan should include:

VENDOR RESPONSE:

Gemalto confirms that our final Implementation Plan will include the following as required by the State:

- Listing of the Vendor resources for each implementation task
- Plan for conducting site surveys
- Schedule including delivery and installation
- Plan for migrating data
- Plan for installation and deployment of all data center equipment and systems
- Plan for installation and deployment of all central issuance facility equipment

4.50.1.1 Listing of the Vendor resources for each implementation task

VENDOR RESPONSE:

Gemalto confirms that a listing of Gemalto staff will be provided for each implementation task as part of the finalized implementation plan.

4.50.1.2 Plan for conducting site surveys of all the Agency facilities

VENDOR RESPONSE:

As the current vendor, Gemalto is familiar with the Agencies facilities however we will still perform site surveys as part of our Implementation Play and deployment process. During the planning phase of the project a Site Survey work package is included as part of the Transition Plan. Gemalto conducts site surveys to better understand the processing requirements of each field office ahead of the deployment phase. The key objective of a site survey is to document the current equipment layout and identify all electrical and network port locations that may serve for the future deployment. There will also be as part of the report photos for visual reference, a 2D diagram with equipment position and legend along with any observations that may hinder or improve the deployment phase, including network infrastructure, when it will be executed.

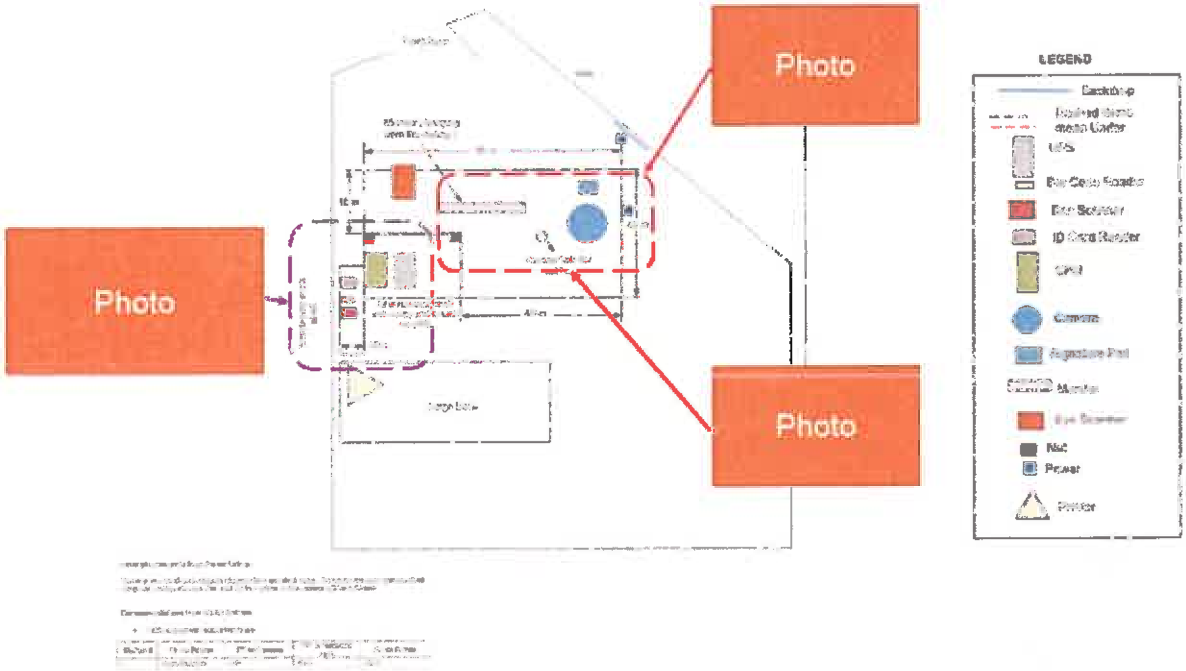


FIGURE 64: SAMPLE SITE SURVEY REPORT

Regular meetings will be held following the completion of the site surveys and all reports will be shared with the State to be able to discuss and confirm the relevant needs and impacts, followed by an action plan. All decisions will be communicated back to Gemalto's Project Manager who will then inform the relevant Stake Holders of the decisions.

4.50.1.3 Schedule including delivery and installation of equipment and training

VENDOR RESPONSE:

Gemalto confirms that a finalized delivery and installation schedule will be provided as part of the finalized implementation plan. We have included a samples rollout schedule in the below response to "Requirement 4.51.1.7". Typically delivery is managed from a central location then dropped off by our staff ahead of rollout.

4.50.1.4 Plan for migrating data from current image database

VENDOR RESPONSE:

As the State's current vendor, Gemalto can provide 100% data migration between systems. Typically, this is one of the more challenging tasks in migrating between driver's license systems however we fully understand the State's current image database and can easily migrate this to our new solution. Our data migration process typically follows the below process which we will follow to ensure and validate that all data has been successfully migrated.

Gemalto will ensure that the data identified as requiring migration during the Project Data Migration Workshop with the DMV will be cleansed and migrated following the Gemalto Data Migration Processes described below. The migration will be documented (Data Migration Plan) as part of the project implementation plan The criteria which constitutes the 100% successful migration will also be defined and mutually agreed upon in the Project Data Migration Workshop and documented in the Data Migration Plan which will be provided to the State, in addition to the final Data Migration Report post deployment of the solution across the State.

---------------------------------BEGIN Gemalto Trade Secret Information-------------------------------

Data Migration Planning - During planning we work together with the State's SME's (Subject Matter Experts) to clearly identify what data needs to be migrated over from the source system into the Gemalto system (target system).

Data Migration Testing - Gemalto's approach to designing migration testing strategies is to document the risk, the likelihood of occurrence, and then define the means to mitigate risk via testing where appropriate. In the case where demographic (e.g., Civil, Biometrics), audit and driving license data is migrated, significantly more upfront analysis is required to "best fit" the legacy data into the new Gemalto system. We have found that the best way of minimizing the occurrence of migration error is through testing prior to the actual production migration.

Pre-Data Migration Testing - Gemalto recommends as part of the process to sample some subset of the random legacy data to validate and inspect the selected content for conformity to known legacy specifications and reflection to the target system specifications. These tests occur early in the migration process, before any migration (even migration for testing purposes), is completed.

Data Migration Design Review – We will conduct a design review of the migration specification with the DMV when the pre-migration testing is near complete, or during the earliest stages of the migration tool configuration. The outcome of the design review will include a list of any open issues, the means to close each issue and approve the migration specification and a process to maintain the specification in sync with the migration tool configuration (from our experience this will continuously change until the production migration).Once the design review is approved a test sample of legacy data will be migrated into a "Staging Database" for testing. The Staging database is a secure and temporary working repository for the migration data where data can be tested and manipulated before moving/committing to UAT or Production systems.

Post-Data Migration Testing - Once a migration has been executed, additional end to end testing can be executed. We expect some errors to be identified during the initial test runs although these will have been minimized as during the pre-migration testing. Post-migration testing is typically performed in the Gemalto Staging Database (Test Environment).

Data Migration User Acceptance Testing - To measure success prior to production migration, Gemalto proposes to provide the user community of the DMV an opportunity to interact with the migrated legacy data in the new Gemalto solution. Functional subtleties related to the co-mingling of migrated data and data created in the Gemalto destination system may be difficult to identify early in the migration process. User acceptance testing provides an opportunity to test the data (through the image capture, biometric investigation applications, other system processes that rely on the migrated data e.g., downstream feeds such as reporting and interaction with external interfaces both legacy and new), to ensure that the data presented in the new system is valid, conforms to expectations and maintains data and business integrity across the desired solution landscape.

Production Migration – This includes all of the testing completed prior to the production migration aims to ensure that the production process will be completed without error. Depending on workshop planning and identification of data to be migrated the validation of the data migrated can be tested with minimal downtime. Data Migration Reports are continually sent to the Data Governance Board throughout the migration phase and a final Data Migration Report describing the success level of the migration is issued post deployment of the new solution across the State.

---------------------------------------END Gemalto Trade Secret Information------------------------------------

4.50.1.5 Plan for installation and deployment of all data center equipment and systems

VENDOR RESPONSE:

As clarified in the response to Vendor questions, installation and deployment of datacenter equipment and systems will be provided and managed by the State. Gemalto will work with the State to coordinate all backend data center requirements and will coordinate for the deployment and installation of the Central Server (CS) software and make all necessary technical staff available for this stage of implementation.

4.50.1.6 Plan for installation and deployment of all central issuance facility equipment and production procedures

VENDOR RESPONSE:

Gemalto's central issuance facility equipment and production equipment is currently installed and operational so no action needs to be taken for this plan. We will capitalize on the existing hardware used to personalize the driver's license for the State of West Virginia.

4.50.1.7 The Vendor should provide as a part of their proposal, a sample plan for the implementation and rollout of the solution to all locations, including timeline.

VENDOR RESPONSE:

Once the pilot offices are operational, we will begin to deploy to the other offices by region. We look for minimal support from the DMV during this period. We will need to get access to each of the offices on an agreed upon schedule. We may also need support during the testing of the offices once all is established. Once we have an office installed and ready for production, we will work with the staff in that location on the proper operation of the equipment and software. Again, we will work with the DMV on a schedule for minimum impact. We will provide a checklist (contents to be agreed by the DMV) upon successful implementation that ensures we have someone from the DMV verify that all was implemented according to the plans provided. We have included a sample installation schedule and timeline below:

Task Name	Duration	Start	Finish
Beckley – Field Office Installation and Training	1 days	9/3/2019	9/3/2019
Charles Town – Field Office Installation and Training	1 days	9/3/2019	9/3/2019
Clarksburg – Field Office Installation and Training	1 days	9/4/2019	9/4/2019
Elkins – Field Office Installation and Training	1 days	9/4/2019	9/4/2019
Flatwoods – Field Office Installation and Training	1 days	9/5/2019	9/5/2019
Franklin – Field Office Installation and Training	1 days	9/5/2019	9/5/2019
Huntington – Field Office Installation and Training	1 days	9/6/2019	9/6/2019
Kanawha City (Charleston) – Field Office Installation and Training	1 days	9/6/2019	9/6/2019
Lewisburg – Field Office Installation and Training	1 days	9/9/2019	9/9/2019
Logan – Field Office Installation and Training	1 days	9/9/2019	9/9/2019
Martinsburg – Field Office Installation and Training	1 days	9/10/2019	9/10/2019
Moorefield– Field Office Installation and Training	1 days	9/10/2019	9/10/2019
Morgantown – Field Office Installation and Training	1 days	9/11/2019	9/11/2019
Moundsville – Field Office Installation and Training	1 days	9/11/2019	9/11/2019
Parkersburg – Field Office Installation and Training	1 days	9/12/2019	9/12/2019
Point Pleasant– Field Office Installation and Training	1 days	9/12/2019	9/12/2019
Princeton– Field Office Installation and Training	1 days	9/13/2019	9/13/2019
Romney– Field Office Installation and Training	1 days	9/13/2019	9/13/2019
Spencer– Field Office Installation and Training	1 days	9/16/2019	9/16/2019
Summersville– Field Office Installation and Training	1 days	9/16/2019	9/16/2019
Weirton– Field Office Installation and Training	1 days	9/17/2019	9/17/2019
Welch– Field Office Installation and Training	1 days	9/17/2019	9/17/2019
Williamson– Field Office Installation and Training	1 days	9/18/2019	9/18/2019
Winfield– Field Office Installation and Training	1 days	9/18/2019	9/18/2019

Section 4, Subsection 4.51 - 14 Day Pre-Post Support Plan

Section 4, Subsection 4.51.1 - The Vendor should provide a comprehensive plan for product support that consists of a 7-day period prior to and a 7-day period immediately following implementation.

VENDOR RESPONSE:

Gemalto confirms that we will plan for product support that consists of a 7-day period prior to and a 7-day period immediately following implementation. We will have Project Managers, field technicians, and technical resources onsite to ensure that there is a smooth transition.

We also have a Closing Phase as part of our project plan to ensure that the project is successfully transitioned to an operational phase. Once the project is completed, it is essential to draw lessons from what happened. This analysis is performed during a last Project debriefing meeting (post-mortem) involving all project stakeholders. Good practices or good behaviors are captured to be expanded to other projects. It is also important to capitalize on problems that were encountered, in order to understand the root causes and to implement corrective actions.

The goal of the Post mortem is to:

- Collect strengths and weaknesses identified during the project (only ones with possible improvement action) from all project team members
- Rank and select the most significant one (weaknesses and strength - max 5 of each) during the Post Mortem meeting, define actions and actions owners, assigned a person to follow them and share results with others projects.

During the Closing Phase, we will also do the official handoff to Support. As stated previously, the Support Staff will be involved during the project so that we can have a smooth transition.

Section 4, Subsection 4.51.2 - Support should be available on-site at the agency headquarters in Kanawha City. Support should be available to installation technicians and the Agency staff during installation and configuration of any system component.

VENDOR RESPONSE:

Gemalto confirms that support will be available on-site at the agency headquarters in Kanawha City and to installation technicians and the Agency staff during installation and configuration of any system component. We plan to have a large number of staff onsite during this phase to coordinate, manage, and provide support as the solution is implemented.

Driver's License and Credential Issuance System
CRFP DMV1800000001

Appendix 01
Gemalto Facial Recognition Solution Press Release

Gemalto facial recognition solution excels at US Department of Homeland Security 2018 Biometric Rally

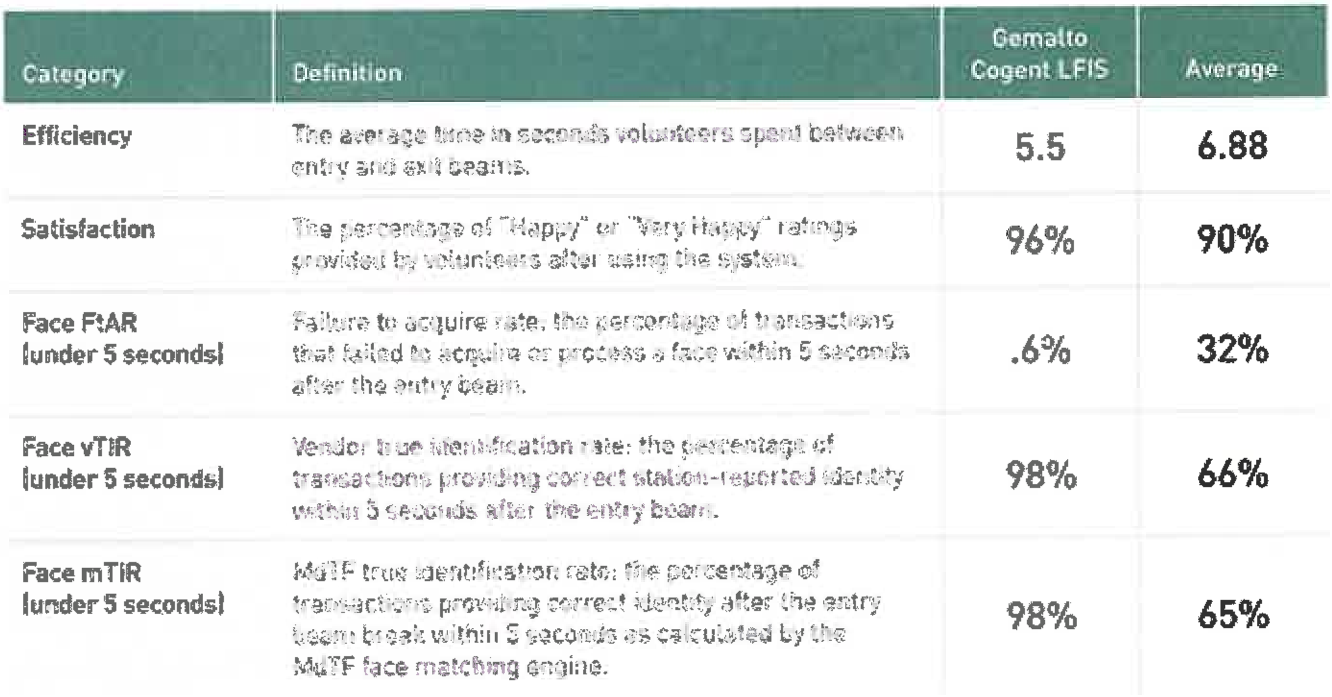
Innovative solution using Gemalto Live Face Identification System (LFIS) obtained a 99.44% acquisition rate under 5 seconds

Amsterdam, June13 , 2018 – Gemalto excelled at the 2018 biometrics rally, sponsored by the US Department of Homeland Security's (DHS) Science and Technology Directorate (S&T) in conjunction with the National Institute of Standards and Technology (NIST).

Twelve companies were chosen out of a pool of applicants to showcase their facial recognition technology to address the growing challenge of traveler identification and automated border control. Each company also had to meet several listed requirements such as time restraints, unmanned operation, and limited physical footprint. They were also evaluated in three categories: efficiency, satisfaction, and effectiveness. The 2018 rally was done at the Maryland Test Facility (MdTF) which provides a controlled environment for laboratory evaluation and operational scenario-based testing of various biometric entry and exit concepts of operation under simulated airport conditions.

Gemalto created a solution using Live Face Identification System (LFIS) as the core technology to meet the 2018 biometric rally requirements, and the solution outperformed the average range for most metrics in addition to a 99.44% successful acquisition rate in less than 5 seconds compared to the average of 65%.

Gemalto, also known as 'Castle' in the anonymized results shared by the sponsors performed exceptionally well. Gemalto's solution had the leading result for FtAR (see table) for both under 5 and 20 seconds and Face vTIR (see table) for under 5 and 20 seconds. Regarding Face mTIR (see table) and efficiency metrics Gemalto was one of only 2 vendors to meet the goal.



Category	Definition	Gemalto Cogent LFIS	Average
Efficiency	The average time in seconds volunteers spent between entry and exit beams.	5.5	6.88
Satisfaction	The percentage of "Happy" or "Very Happy" ratings provided by volunteers after using the system.	96%	90%
Face FtAR [under 5 seconds]	Failure to acquire rate, the percentage of transactions that failed to acquire or process a face within 5 seconds after the entry beam.	.6%	32%
Face vTIR [under 5 seconds]	Vendor true identification rate: the percentage of transactions providing correct station-reported identity within 5 seconds after the entry beam.	98%	66%
Face mTIR [under 5 seconds]	MdTF true identification rate: the percentage of transactions providing correct identity after the entry beam break within 5 seconds as calculated by the MdTF face matching engine.	98%	65%

Facial recognition is positioned to grow over 20% a year from 2016 to 2022[1] over a broad spectrum of use cases. In addition to security at the border, LFIS can improve the traveler's experience from curb to gate to curb by introducing self-service bag drop, speeding up security lines and even enabling biometric boarding. The technology is hardware and camera agnostic and can be used with enrolment and document verification as well. The technology can be used for other business cases where a biometric identity check is required to verify access to secure premises.

"We're thrilled with the outstanding results our solution achieved at the 2018 rally," said Neville Pattinson, senior vice president of Federal Government Sales for Gemalto. "Given the success of LFIS, we see this as a secure and efficient solution for government entities to interact with citizens. It can also revolutionize the air, land and sea passenger, international border, and security checkpoint experiences with increased security and added convenience to travelers."

[1] Source: Allied Market Research, "World Facial Recognition Market - Opportunities and Forecasts, 2015 - 2022.

Additional links
2018 Biometric Technology Rally
Original Gemalto Press Release

State of West Virginia

Division of Motor Vehicles

Driver's License and Credential Issuance System

CRFP DMV1800000001

Attachment B – Mandatory Specification Checklist

Gemalto, Inc.
9442 Capitol of Texas Hwy North
Plaza II, Suite 100
Austin, TX 78759 USA

gemalto
security to be free

Table of Contents

Confidentiality Disclaimer **6**

CENTRAL ISSUANCE **10**

Section 4, Subsection 4.1 - REAL ID Compliance Objectives........ 10

FACILITY IMAGE & SIGNATURE CAPTURE WORKSTATION (ICW) REQUIREMENTS **10**

Section 4, Subsection 5.1 10

Section 4, Subsection 5.2 - Functional - ICAO........ 10

Section 4, Subsection 5.3 - Functional - Interface with Agency Internal Systems 11

Section 4, Subsection 5.4. - Functional - Communication with Central Image/Demographic System 13

Section 4, Subsection 5.5 - Security - Remote Access 14

SYSTEM ADMINISTRATION REQUIREMENTS **14**

Section 4, Subsection 5.6. - User Interface........ 14

Section 4, Subsection 5.7 - User Account Management 15

Section 4, Subsection 5.8 - System Configuration 15

CENTRAL IMAGE/DEMOGRAPIDC SYSTEM ("CIDS") REQUIREMENTS **15**

Section 4, Subsection 5.9 - Hardware and Software 15

Section 4, Subsection 5.10 - Data Storage........ 17

Section 4, Subsection 5.11 - Ownership of Data 19

Section 4, Subsection 5.12. - Access to Data 19

Section 4, Subsection 5.13 - System Performance 20

Section 4, Subsection 5.14 - Software Optimization 20

Section 4, Subsection 5.15 - Image Migration and Volume 20

SECURE CENTRAL ISSUANCE FACILITY REQUIREMENTS. **22**

Section 4, Subsection 5.16 - Credential Issuance 22

Section 4, Subsection 5.17 - Communication with the Agency's Data Center - Transfer of Data........ 22

Section 4, Subsection 5.18 - Card Production Data Files........ 24

Section 4, Subsection 5.19 - Management of Central Issuance Facilities 24

Section 4, Subsection 5.20 - Standard Processing Time. 25

Section 4, Subsection 5.21 - Quality Assurance (QA) 26

Section 4, Subsection 5.22 - Card Mailing 26

Section 4, Subsection 5.23 - Card Volume........ 27

Section 4, Subsection 5.24 - Billing........ 27

CARD DESIGN AND SECURITY FEATURES REQUIREMENTS 29
Section 4, Subsection 5.25 - Data on Secure Temporary Driver's License and ID's 29
Section 4, Subsection 5.26 - Card Types 30
Section 4, Subsection 5.27 - Card Design 31
Section 4, Subsection 5.28 - Card Materials and Security Features 33
Section 4, Subsection 5.29 - Card Design Changes 38
Section 4, Subsection 5.30 - Consumables for Secure Temporary DL 39
COVERT SYSTEM REQUIREMENTS 39
MAINTENANCE AND SUPPORT. 39
PROJECT MANAGEMENT Responsibilities 41
Section 4, Subsection 5.36 - Project Work Plan 41
Section 4, Subsection 5.37 - Performance Testing 41
Section 4, Subsection 5.38 - Change Control Plan 42
Section 4, Subsection 5.39 - Change Orders 43
Section 4, Subsection 5.40 - Upgrades, Patches, Fixes, or Other System Updates 43
Section 4, Subsection 5.41 - Right to Reproduce and Distribute 44
Section 4, Subsection 5.42 - Training Plan 44
Section 4, Subsection 5.43 - Training Costs 45
Section 4, Subsection 5.44 - Implementation Plan 45
Section 4, Subsection 5.45 - Data Migration 45
SERVICE LEVEL AGREEMENT 47
Section 4, Subsection 5.46 - Preventive and Remedial Maintenance 47
Section 4, Subsection 5.47 - Service Response Times 48
Section 4, Subsection 5.48 - System Availability 49
Section 4, Subsection 5.49 - Help Desk Support 50
Section 4, Subsection 5.50 - Field Service Support 51
INFORMATION TECHNOLOGY REQUIREMENTS 51
Section 4, Subsection 5.51 - Communications 51
Section 4, Subsection 5.52 - Data Storage 51
Section 4, Subsection 5.53 - Software Updates 52
Section 4, Subsection 5.54 - Change to Production System 53
Section 4, Subsection 5.55 - 14 Day Pre-Post Support Plan 53

Section 4, Subsection 5.56 - End of Contract.. 53

Confidentiality Disclaimer

State of West Virginia
Purchasing Division
Request for Proposal (RFP)
To Provide Driver's License and ID Cards
CRFP 0802 DMV1800000001

Statement Concerning Trade Secret Information

Certain information herein qualifies as ***Trade Secret*** and is therefore exempt from disclosure under the West Virginia Freedom of Information Act, West Virginia Code §29B-1-1 *et seq*. (the "WV FOIA"). We respectfully submit this Statement Concerning Trade Secret Information and request that the State of West Virginia, Purchasing Division maintain its confidentiality.

With regard to the as ***Trade Secret*** information, such information includes formulae, plans, patterns, processes, tools, mechanisms, compounds, procedures, production data or compilations of information which are not patented and which are known only to certain individuals within Gemalto, Inc. ("Gemalto") who are using it to fabricate, produce or compound an article or trade a service or to locate minerals or other substances having commercial value, and which gives Gemalto an opportunity to obtain business advantage over competitors. (*W. VA Code §29B-1-4(a)(1))*

Document claiming a statutory exemption to the Freedom of Information Act	**Statutory exception of the Freedom of Information Act that applies**	**Explanation** (*Reason Code*) Manner in which the statutory exception to the Public Records Act applies
Attachment B - Section 4, Subsection 5.15.1	*W. VA Code §29B-1-4(a)(1)*	*6-Project Implementation Method and Process*
Attachment B - Section 4, Subsection 5.45.1	*W. VA Code §29B-1-4(a)(1)*	*6-Project Implementation Method and Process*

The beginning and end of confidential sections, which contain such trade secret information are marked as follows:

-------------------------------------BEGIN Gemalto Trade Secret Information-------------------------------

Trade Secret Information

-------------------------------------END Gemalto Trade Secret Information--------------------------------

Table of reason codes and descriptions

Reason code	Textual Description
1-Equipment Operation and Process Description	The information referenced describes the detailed operation of the equipment proposed and the processes that are to be implemented, including configuration and techniques employed to protect the security and integrity of the final solution. Protection of this proprietary, trade secret information is required to preclude the loss of competitive and economic advantage and to protect system and data integrity. This information is generally the subject of efforts to maintain its secrecy from competitors and the general public.
2-System Operation and Process Description	The information referenced describes the detailed operation of the system proposed and the processes that are to be implemented, including programs and methods employed to protect the security and integrity of the final solution. Protection of this proprietary, trade secret information is required to preclude the loss of competitive and economic advantage and to protect system and data integrity. This information is generally the subject of efforts to maintain its secrecy from competitors and the general public.
3-System Security Processes and Techniques	The information referenced describes the detailed techniques of system security of the system proposed and the processes that are to be implemented. This information includes programs, equipment, and methods employed to protect the security and integrity of the final solution. Protection of this proprietary, trade secret information is required to preclude the loss of competitive and economic advantage and to protect system and data integrity. This information is generally the subject of efforts to maintain its secrecy from competitors and the general public.

Reason code	Textual Description
4-Document Security Patterns and Techniques	The information referenced describes the detailed techniques and patterns of secure document design for the solution proposed. This information includes details of the methods employed to protect the security and integrity of the final secure identity documents. Protection of this proprietary, trade secret information is required to preclude the loss of competitive and economic advantage and to protect document and data integrity. This information is generally the subject of efforts to maintain its secrecy from competitors and the general public.
5-Document Production Processes and Techniques	The information referenced describes the detailed processes and techniques of document production of the solution proposed and the configuration of the facilities that are to be implemented. This information includes site designs, equipment, and methods employed to protect the security and integrity of the final solution. Protection of this proprietary, trade secret information is required to preclude the loss of competitive and economic advantage, and to protect system and data integrity. This information is generally the subject of efforts to maintain its secrecy from competitors and the general public.
6-Project Implementation Method and Process	The information referenced describes the detailed methods of project implementation of the system proposed and the project execution and control processes that are to be followed. Protection of this proprietary, trade secret information is required to preclude the loss of competitive and economic advantage. This information is generally the subject of efforts to maintain its secrecy from competitors and the general public.
7-Project Support Method and Process	The information referenced describes the detailed methods of project support of the system proposed and the operational support execution and control processes that are to be followed. Protection of this proprietary, trade secret information is required to preclude the loss of competitive and economic advantage. This information is generally the subject of efforts to maintain its secrecy from competitors and the general public.

Reason code	Textual Description
8-Facility Layout and Security Systems	The information referenced includes details of facility layouts, contents, and security systems and operations that, if compromised, will represent a real and immediate threat to the Security of the State. This information is generally the subject of efforts to maintain its secrecy from competitors and the general public.
9-Protected Sensitive Corporate Materials	The information referenced includes details of organization, personnel, corporate finance, clients, policies, and Corporate processes associated with corporate management and governance. Protection of this proprietary, trade secret information is required to preclude the loss of competitive and economic advantage. This information is generally the subject of efforts to maintain its secrecy from competitors and the general public.

CENTRAL ISSUANCE

Section 4, Subsection 4.1 - REAL ID Compliance Objectives

Section 4, Subsection 4.1.1 - Vendor should describe what specifications they would propose to address the REAL ID Act of 2005 standards, and how their solution will meet the initial "Photo First" requirements providing compliance with those standards. The Agency is requesting an in-depth description of how this can be handled in "real time", which should consist of a detailed system diagram illustrating server (physical/virtual) locations and on- site equipment at each Agency location.
Vendor Response:

Gemalto confirms that we will provide a Real ID compliant solution. We will continue to provide the State with a photo first workflow as described in "A-03-Attachment A-Vendor Response Sheet".

FACILITY IMAGE & SIGNATURE CAPTURE WORKSTATION (ICW) REQUIREMENTS

Section 4, Subsection 5.1

- Vendor must install digitized image capture workstations at each of the twenty-seven (27) locations as defined in Attachment D. At the time of installation, all equipment must be new and in good working order.
Vendor Response: WILL COMPLY

Gemalto confirms that it will install digitalized image capture workstations at each of the twenty-seven locations as defined in Attachment D. At the time of installation, all equipment will be new and in good working order (This is assured as we test and tag all the equipment before dispatching the equipment to sites for deployment to avoid any issues of faulty equipment at installation time).

Section 4, Subsection 5.2 - Functional - ICAO

Section 4, Subsection 5.2.1 - Image must meet ISO/IEC 19794-5:2011 Information Technology - Biometric Data Interchange Formats - Part 5: Face Image Data or current specifications. http://www.iso.org/iso/home/store/catalogue ics/catalogue detail ic5.htm?csnumber-50867
Vendor Response: WILL COMPLY

Gemalto Capture Suite - Image Capture Workstation ICAO Check Algorithm that ensures that all portrait images captured conform to the ISO/IEC 19794-5:2011 Information Technology - Biometric Data Interchange Formats – Part 5. Hence the state can be assured that we will be providing photo images in compliance with this standard.

Section 4, Subsection 5.2.2 The system must be capable of ICAO image quality checks.
Vendor Response: WILL COMPLY

Gemalto Capture Suite - Image Capture Workstation ICAO Check Algorithm performs the following checks:

- **Eyes Opened** – Ensure the applicant's eyes are opened, if possible
- **Uniform Background** – Ensure the white canvas covers the entire background area of the photo
- **Face Position** – Ensure the applicant's face is positioned correctly in the photo
- **Single Face** – Ensure no other persons are present in the photo
- **Glasses** – Ensure the applicant removes eyewear
- **Red Eyes** – Ensure camera settings are correct
- **Resolution** – Ensure the applicant is not standing too far from the camera
- **Mouth Closed** – Ensure the applicant's mouth is closed
- **Sharpness** – Ensure camera settings are correct
- **Face Proportion**
- **Uniform Lighting** – Ensure the applicant and camera are positioned correctly to allow uniform lighting
- **Exposure** – Ensure the flash settings are correct
- **Natural Skin Color** – Ensure the flash settings are correct
- **Eyes Gaze Frontal** – Ensure the applicant is looking directly at the camera

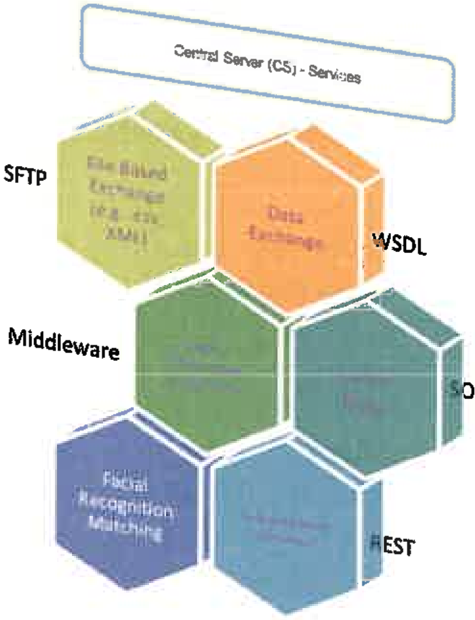
Section 4, Subsection 5.3 - Functional - Interface with Agency Internal Systems

Section 4, Subsection 5.3.1 - Must interface with the *dmv*FIRST Web Application, a component of *dmv*DRIVES, via a web service call. This interface ensures the appropriate fees are collected based on the type of credential issued.
Vendor Response: WILL COMPLY

We have performed integration to other systems across different platforms and using various services interfaces in every jurisdiction and will ensure a successful integration with the dmvFIRST Web Application, a via a web service call.

Within the n-tier design of our solution we have a Service Layer, built within Central Server for service integration. We have gained a wealth of integration experience integrating to a multitude of interfaces and are platform independent.

Some of our experiences include Legacy Mainframe Systems, Document Management Systems, Payment Gateways, State Board of Elections, Law Enforcement, Driver Testing, Secretary of State, Interfaces with approved government agencies for personal data verification and facilitating agency access to select contents, Authentication Engines.


Central Server (CS) - Services
SFTP
File Based Exchange (e.g. csv, XML)
Data Exchange
WSDL
Middleware
SOAP
Facial Recognition Matching
REST

Section 4, Subsection 5.3.2 - Must display voter registration questions on the signature pad and send the returned responses to the West Virginia Secretary of State's Office, to include applicant signature, required per West Virginia Code §3-2-1 1.
Vendor Response: WILL COMPLY

Gemalto confirms that the proposed signature pad will provide voter registration questions and capture a true representation of the applicant's written signature. Gemalto MIDS are already performing this integration in the current implementation with the state. With this experience already undertaken we are sure that we will successfully migrate our new solution and continue seamlessly to send the voter responses and applicant signature to the Secretary of State's office as required per West Virginia Code §3-2-1 1.

Section 4, Subsection 5.3.3 - Must interface with the State's mainframe system, that serves as the primary driver record, ensuring the applicants status and availability to receive a credential.
Vendor Response: WILL COMPLY

Gemalto confirms that we can continue to use the existing method of integration with the mainframe (AttachMate, BlueZone scrape to text file) with our new solution. In addition we confirm that we can move to alternative interface methods as required by the state. Our Central Server platform is a Service Orientated Archicture that can integrate to other systems across various platforms, messaging queues and interfaces.

Section 4, Subsection 5.3.4 - Must interface with the State's Automated Testing System, passing applicant demographic information.
Vendor Response: WILL COMPLY

Gemalto MIDS is currently providing this integration and assures the state that the new Gemalto Capture Suite Photo-First and ICW application will continue to send the applicant demographic to the State's Automated Testing System via Gemalto's Central Server SOA Platform.

Section 4, Subsection 5.3.5 - Must interface with West Virginia Interactive passing applicant demographic information related to multiple online solutions such as DL renewals, and employee ID applications.
Vendor Response: WILL COMPLY

Gemalto confirms that our Central Server SOA Platform will be able to interface with West Virginia Interactive passing applicant demographic information such that it can be used by multiple online solutions hosted by West Virginia Interactive such as DL renewals, and employee ID applications.

Section 4, Subsection 5.4. - Functional - Communication with Central Image/Demographic System

Section 4, Subsection 5.4.1 - The ICW must be capable of near real-time transfer (not just nightly batch) of demographic data and images to the central image/demographic system.
Vendor Response: WILL COMPLY

Gemalto confirms that the Gemalto Capture Suite ICW can perform near real-time transfer of demographic data and images to the central image/demographic system.

This is based on the assumption that the WVOT provided hosting services including platforms and networking can provide a suitable Network Throughput Quality (i.e. Bandwidth, RTT, Low Latency, QoS) between the WVOT data center and DMV office locations.

Section 4, Subsection 5.4.2 - All images and data captured must be transferred to the central image/demographic system for storage even if the transaction was cancelled or not completed.
5.4.2.1 If the applicant had to cancel or was not able to compete the transaction, Vendor's solution must provide for a verification match of the applicant's image and data against the central image/demographic system upon the applicant's return to any Agency Office for completion of the licensing process.
Vendor Response: WILL COMPLY

Gemalto confirms that all images and data captured will be transferred to the central image/demographic system for storage even if the transaction was cancelled or not completed.

If an application is resumed from a suspended state (e.g. cancelled, incomplete), the business logic applied to the ICW workflow will request a verification match of the applicants image (1:1 Verification) against the data stored at the central image/demographic system upon the applicant's return to any Agency Office for completion of the licensing process.

We will define the final workflow rules and process with the State during the workshops and specifications phase of the project.

Section 4, Subsection 5.4.3 - Images and data for incomplete transactions must be distinguishable from completed issuance records.
Vendor Response: WILL COMPLY

Gemalto confirms that image and data for incomplete transactions will be marked as "Incomplete", which will allow them to be distinguished from completed issuance records.

Section 4, Subsection 5.5 - Security - Remote Access

Section 4, Subsection 5.5.1 - Secure, remote access to Vendor staff for purposes of support will be allowed via the West Virginia Office of Technology Network Access Form (NAF) request process at no cost to the Vendor.
https://technology.wv.gov/SiteCollectionDocuments/Policies%20Issued%20by%20the%20CTO/2017/PO1021_AccountManage_Sept2017.pdf
Vendor Response: WILL COMPLY

Gemalto confirms that its support staff administrating the solution components hosted at the WVOT Data Center shall use the secure remote access provided by WVOT by completing the NAF and creating an account.

SYSTEM ADMINISTRATION REQUIREMENTS

Section 4, Subsection 5.6. - User Interface

Section 4, Subsection 5.6.1 - The solution must include a system administration module with a user interface for managing system settings.
Vendor Response: WILL COMPLY

Gemalto confirms that our solution will include a system administration module with a user interface for managing system settings. This is located within the Central Server (CS) administration module.

Section 4, Subsection 5.7 - User Account Management

Section 4, Subsection 5.7.1 - Vendor's solution must be compatible with Windows Active Directory protocol to utilize the agencies logon credentials, managed by the Office of Technology, to manage user roles.
Vendor Response: WILL COMPLY

Gemalto confirms that our solution is compatible with Windows Active Directory protocol to utilize the agencies logon credentials, managed by the Office of Technology, to manage user roles. This is our standard and preferred method for user account management and integration.

Section 4, Subsection 5.8 - System Configuration

Section 4, Subsection 5.8.1 - At a minimum, the Agency must be able to configure the following settings:
5.8.1.1 Thresholds for 1: N and 1:1 match or non-match results
5.8.1.2 Search limit thresholds for all applications
Vendor Response: WILL COMPLY

Gemalto confirms that thresholds for 1: N and 1:1 matches or non-match results and search limit thresholds for all applications are configurable within our solution. Thresholds for 1: N and 1:1 match or non-match results as configurable within the Central Server (CS) administration module. Search limit thresholds for all applications are configurable within each respective module i.e. manual search limits within the Biometric Investigative Workstation (BIW) are configurable within the BIW settings for that specific search. Search settings may also be globally configured within the CS administration module.

CENTRAL IMAGE/DEMOGRAPIDC SYSTEM ("CIDS") REQUIREMENTS

Section 4, Subsection 5.9 - Hardware and Software

Section 4, Subsection 5.9.1 - All software necessary for communication between the central image/demographic system and other Vendor or Agency systems, must be provided by the Vendor.
Vendor Response: WILL COMPLY

Gemalto confirms that all software necessary for communication between the central image/demographic system (Gemalto Central Server solution) and other Gemalto or Agency systems will be provided by Gemalto.

Section 4, Subsection 5.9.2 - All virtual servers necessary for the central image/demographic system shall be provided by and located in the West Virginia Office of Technology data center in Charleston, West Virginia.
Vendor Response: WILL COMPLY

Gemalto confirms that our solution has been designed to be virtualized and we will collaborate with WVOT to design the IT Infrastructure to ensure that all virtual servers for the central image/demographic system located in the West Virginia Office of Technology data center in Charleston, West Virginia will be able to operate flawlessly.

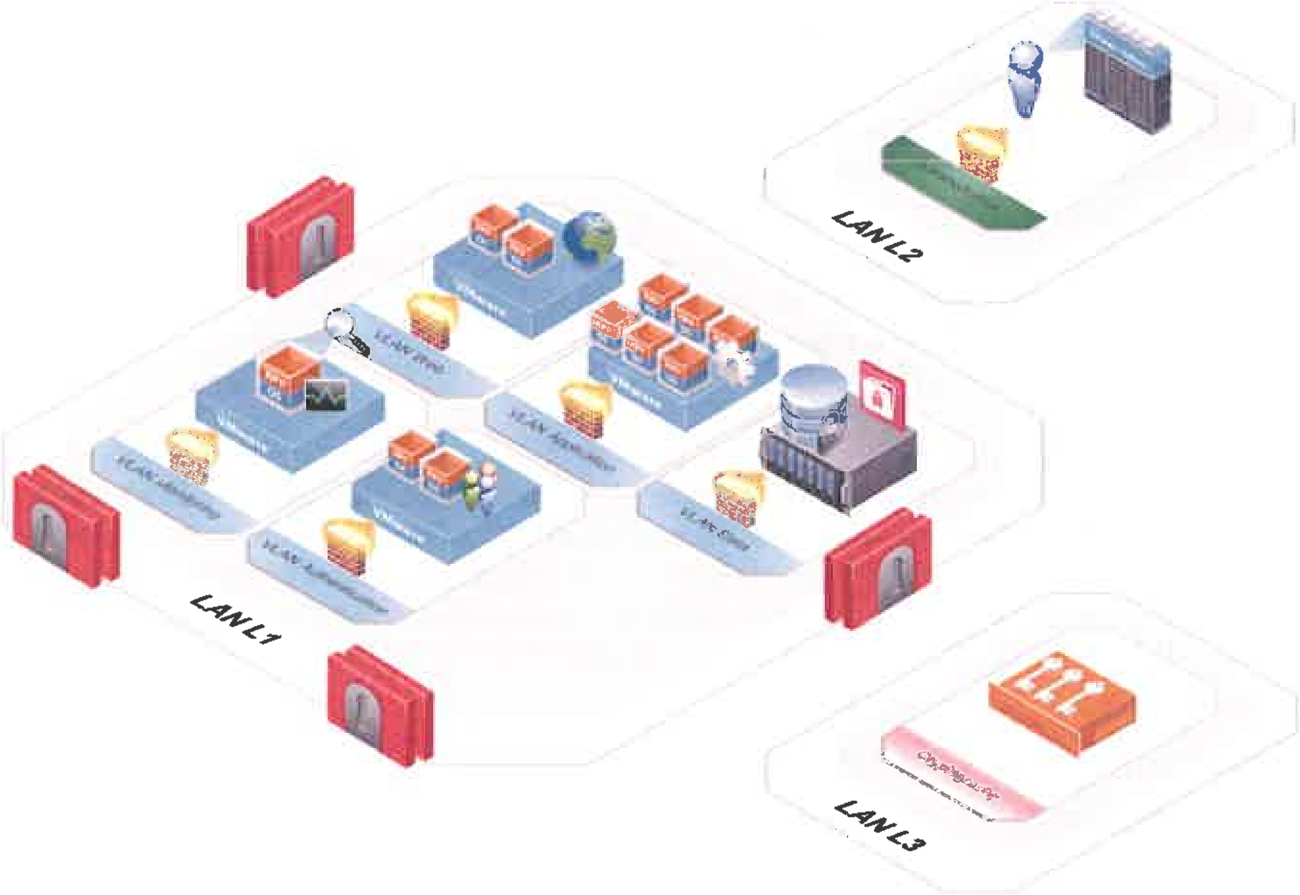


FIGURE 1 - PROPOSED FAULT TOLERANT VIRTUALIZED ENVIRONMENT

Our solution is designed to be hosted by virtualization with services in cluster, at both the Primary and DR (Disaster Recovery) sites, to offer high availability and rapid scalability. We will work with WVOT to ensure that the proposed supporting virtualized infrastructure is setup with fault tolerance by design to ensure that if an application server instance fails, another application server will be able to replace it.

Section 4, Subsection 5.9.3 - All data stores necessary for the central image/demographic system shall be provided by the Agency and located in the West Virginia Office of Technology data center in Charleston, West Virginia
Vendor Response: WILL COMPLY

Gemalto confirms that we accept that all data stores necessary for the central image/demographic system will be provided by the Agency and located in the West Virginia Office of Technology data center in Charleston, West Virginia as specified in this RFP.

Section 4, Subsection 5.10 - Data Storage

Section 4, Subsection 5.10.1 - Vendor's solution must meet all policy requirements regarding the collection, storage, usage, classification, transmission, backup, and retention of data as defined by the Office of Technology Policy number PO1001, PO1006, and PO1013. http://www.technology.wv.gov/security/Pages/policies-issued-by- the-cto.aspx
Vendor Response: WILL COMPLY

Gemalto confirms that our solution will meet all Office of Technology Policy requirements related to the collection, storage, usage, classification, transmission, backup, and retention of data including policy number PO1001, PO1006, and PO1013. Compliance with State IT policy is a common requirement and State IT policies will be included in our Requirement Specifications (RQS) to ensure all components of our solution meet the requirements of the Office of Technology and the State.

Our solution application architecture uses a layered approach that is designed and built in a way to respect the N-Tier architecture model that also naturally increases the security

Our N-Tier implementation has both desktop client and web clients connecting to the mid-tier servers for transactional data and business logic operations. The mid-tier servers then connect to a Microsoft SQL Server database for information retrieval or post operations. The mid-tier servers also connect to Hardware Security Modules (HSM), which are used to protect transactions, identities, and applications, as HSMs excel at securing cryptographic keys and provisioning encryption, decryption, authentication, and digital signing services for a wide range of applications. These logical layers are we be designed to be exclusive from each other by network segmentation firewalling.
Users and external systems are only connected to the presentation layer to access services and are kept away from logic and data layers. No direct communication is allowed between (n-2) or (n+2) nodes in each layer.

This 3-tier architecture provides defense in depth (A layering tactic, conceived by the National Security Agency (NSA) as a comprehensive approach to information and electronic security), because an infiltrator must pass through and compromise several firewalls to reach the back-end location of cryptographic keys and database.

We utilize the Microsoft IIS Application server to host our web interface components as it is a fast flexible runtime environment with enhanced reliability and resiliency that supports dynamic web applications requiring web tier clustering over multiple application server instances.

The solution database is based on Microsoft SQL Server technology, and we recommend to WVOT to include at the database level several security products to provide a highly secure and auditable environment for the database.

We recommend to WVOT to use a transparent and automated file-system level encryption for sensitive data residing in the solution.

We believe that having a homogenous security approach is essential for our customers, this is primarily due to the nature of sensitive demographic, personally identifying information (PII) and biometric data which are exchanged and stored within the solution.

Apart from recommending WVOT to provide firewalls and IPS (Intrusion Prevention System) appliances, we recommend to integrate a Vulnerability Assessment scanner to complement our stringent security design measures to ensure that we will meet or exceed the State's security expectations.

Employment of HSM (Hardware Security Modules, both physical and virtual) to manage secure storage of sensitive keys and certificates to support Transparent Data Encryption (TDE), Secure Socket Layer (SSL/https) communications hence providing to both infrastructure and applications encryption of data in transit and at rest is also highly recommended to be part of the WVOT hosting.

Section 4, Subsection 5.10.2 - The central image/demographic system must store the facial image files, signature image files, demographic data, and card issuance data for every transaction through the life of the contract. This must include specific card data that will be returned from the central issuance facility.
Vendor Response: WILL COMPLY

Gemalto confirms that our Central Sever (CS) solution (the central image/demographic system) will store the facial image files, signature image files, demographic data, and card issuance data for every transaction through the life of the contract included images of the personalized cards which will be sent from the Central Issuance Facility back to the Central Sever (CS) solution. Gemalto will work with the State during the planning phase of the project to clearly define and then implement all data retention policies.

Section 4, Subsection 5.10.3 - Facial image and signature files must be stored in JPEG 2000 for image compression, or standard that is an open (consensus) format, without proprietary wrappers, to ensure States can effectively use the image captures of other States as necessary. https://www.gpo.gov/fdsys/pkg/FR-2008-01-29/html/08-140.htm
Vendor Response: WILL COMPLY

Gemalto confirms that Facial image and signature files must be stored in JPEG 2000 for image compression or in any other format required by the State. We do not use proprietary file types to prevent our vendors from using their own data.

Section 4, Subsection 5.10.4- The system must log and store audit data for all types of system and data access including details of specific tasks performed and records accessed.
Vendor Response: WILL COMPLY

Gemalto confirms that our Central Server (CS) solution will log and store all required audit data for all systems and data including details of specific tasks and assessed records as required by the State. CS logs the "who, what, where and when" of all of the critical business actions throughout the Gemalto Solution. This Audit Data is searchable and is also available for ad-hoc queries. Audit data may also be restricted to user groups so that only approved users can access certain data.

Section 4, Subsection 5.11 - Ownership of Data

Section 4, Subsection 5.11.1 - Vendor must sign and agree to Attachment F - WV Division of Motor Vehicles Contract Privacy Policy.
Vendor Response: WILL COMPLY

Gemalto confirms that we have signed and agreed to "Attachment F - WV Division of Motor Vehicles Contract Privacy Policy" as required by the State.

Section4, Subsection 5.11.2 - Vendor must sign and agree to Attachment H- PII Acknowledgement.
Vendor Response: WILL COMPLY

Gemalto confirms that we have signed and agreed to "Attachment H- PII Acknowledgement" as required by the State.

Section 4, Subsection 5.12. - Access to Data

Section 4, Subsection 5.12.1 - Access to the central image/demographic system will be restricted to individuals whose duties require such access and are authorized by the Agency.
Vendor Response: WILL COMPLY

Gemalto confirms that access to our Central Server (CS) solution (the central image/demographic system) will be restricted to individuals whose duties require such access and are authorized by the Agency. Access control and restrictions are managed through integration with the State's Active Directory though the use of user groups.

Section 4, Subsection 5.12.2 - Secure, remote access for Vendor staff for purposes of support will be allowed via the West Virginia Office of Technology Network Access Form (NAF) request process at no cost to the Vendor.
Vendor Response: WILL COMPLY

Gemalto understands and agrees that secure, remote access for Vendor staff for purposes of support will be allowed via the West Virginia Office of Technology Network Access Form (NAF) request process at no cost to Gemalto.

Section 4, Subsection 5.13 - System Performance

Section 4, Subsection 5.13.1 - The total time required from the time the image file transmit request is received by the central image/demographic system until the image file is being transmitted from the central image/demographic system shall not exceed one (1) second during the life of the contract. Total time for retrieval excludes the transmission time across any communications network.
Vendor Response: WILL COMPLY

Gemalto confirms that the total time required from the time the image file transmit request is received by the central image/demographic system until the image file is being transmitted from the central image/demographic system shall not exceed one (1) second during the life of the contract excluding transmission time across State networks. As the State is providing all datacenter hardware at WVOT, Gemalto will work with the State to clearly specify hardware or virtual server specifications and requirements in order to maintain this performance level.

Section 4, Subsection 5.14 - Software Optimization

Section 4, Subsection 5.14.1 - The Vendor is responsible for any optimization to the software that is required to maintain these response times no matter how many retrieval requests are received.
Vendor Response: WILL COMPLY

Gemalto confirms that we will be responsible for any optimization to the software that is required to maintain the required one (1) second response times no matter how many retrieval requests are received.

Section 4, Subsection 5.15 - Image Migration and Volume

Section 4, Subsection 5.15.1 - Vendor's solution must provide for the migration of credential images and index information from the current Gemalto ID system to the new central image/demographic system (CIDS). Migration must result in a -minimum of 98 percent usage of the current credential images. There are approximately 3 million JPG images that average 10kbs in size each.
Vendor Response: WILL COMPLY

Gemalto confirms that we will migrate all of the State's legacy data into their new location. For Federal Real ID compliance a state must adopt several practices that relate to auditing, two of which are the storage of digitized identity source documents for a minimum of 10 years, and mandatory facial image capture.

Hence we will ensure that we migrate 100% (One Hundred Percent) of all the data from the legacy system into our new solution. This data will include everything we have been storing for the state from credential images (photos), index information, scanned documents, fingerprints, to signatures and audit data. This will **provide the state with full accountability and a digital chain of evidence for all credentials issued** since the implementation of the current Gemalto MIDS system if it is requested for the purposes of Audit.

-------------------------------------BEGIN Gemalto Trade Secret Information-------------------------------

We have a proven Data Migration Methodology that has helped all the customers we have migrated data for to be assured that the legacy data is accounted for and provides them accountability in the audit of their business processes and data compliance directives.

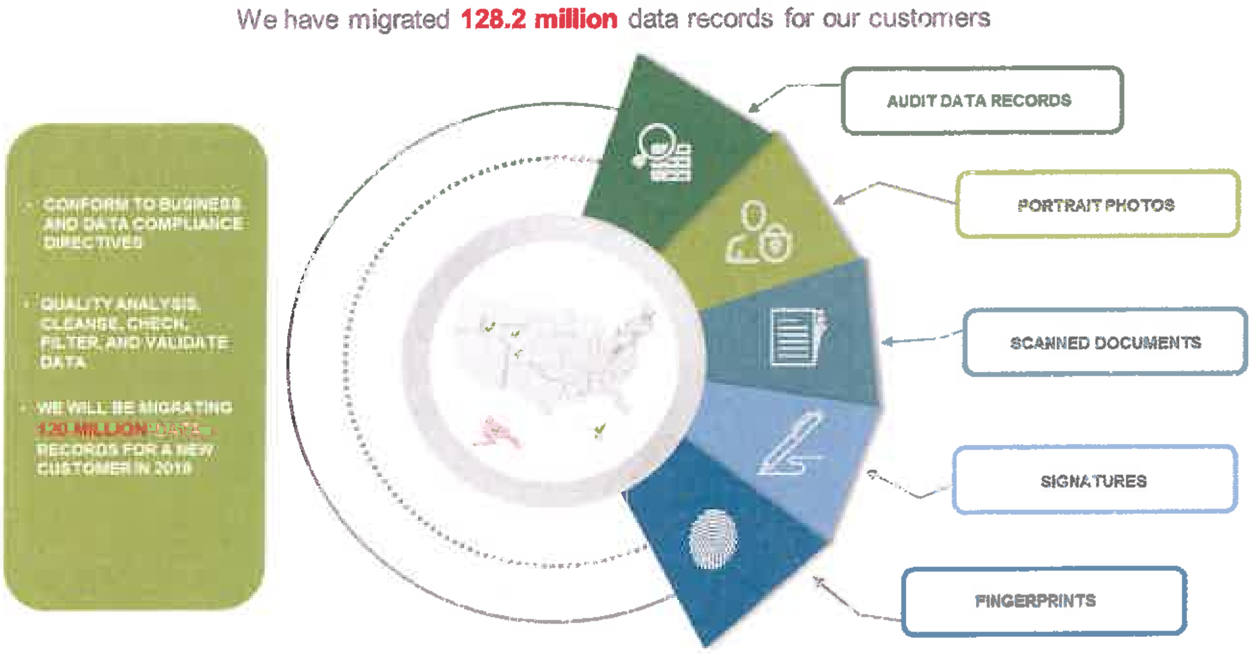

We have migrated 128.2 million data records for our customers
CONFORM TO BUSINESS AND DATA COMPLIANCE DIRECTIVES
QUALITY ANALYSIS, CLEANSE, CHECK, FILTER, AND VALIDATE DATA
WE WILL BE MIGRATING 120 MILLION DATA RECORDS FOR A NEW CUSTOMER IN 2018
AUDIT DATA RECORDS
PORTRAIT PHOTOS
SCANNED DOCUMENTS
SIGNATURES
FINGERPRINTS

FIGURE 2 - DATA MIGRATION STATISTICS

-------------------------------------END Gemalto Trade Secret Information-------------------------------

SECURE CENTRAL ISSUANCE FACILITY REQUIREMENTS.

Section 4, Subsection 5.16 - Credential Issuance

Section 4, Subsection 5.16.1 - Vendor must meet the requirements of the REAL ID Act of 2005 (http://www.dh5.gov/xlibrary/assets/real-id-act-text.pdf). Including any relevant security mandates, including those pertaining to personnel, with supporting documentation provided, as required.

Vendor Response: WILL COMPLY

Gemalto confirms that out Central Issuance Facility meets the requirements of the REAL ID Act of 2005 including all relevant security mandates, including those pertaining to personnel, with supporting documentation provided. Our Naspo Class II certified Central Issuance Facility is currently used to provide Real ID compliant centrally issued drivers licenses for the State of West Virginia.

Section 4, Subsection 5.17 - Communication with the Agency's Data Center - Transfer of Data

Section 4, Subsection 5.17.1 - The secure central issuance facility must communicate with the Office of Technology data center via a VPN tunnel, which hosts the Agency's mainframe, central image/demographic system, and dmvFIRST solutions.

Vendor Response: WILL COMPLY

We will collaborate with the state to configure a secure VPN tunnel between components that are hosted at WVOT and Gemalto Central Issuance facilities. This is something we are very familiar and proficient with as we have implemented this for other customers that host our solution on premise within their data centers.

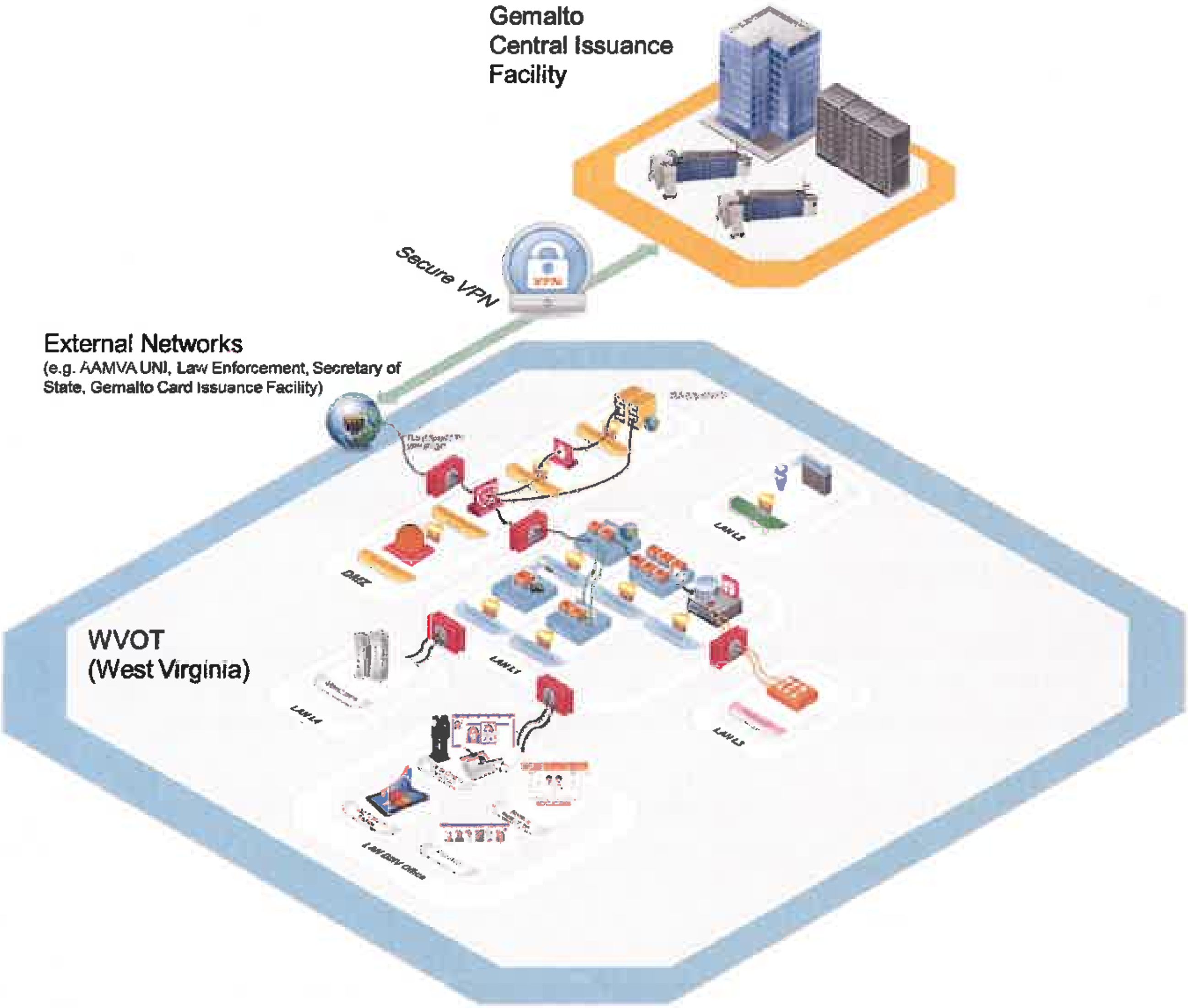


FIGURE 3: GEMALTO CENTRAL ISSUANCE FACILITY CONNECTIVITY ACROSS SECURE VPN

Gemalto central issuance facility is designed with hardware and networking infrastructure that is based on several cutting edge technologies from SafeNet (A Gemalto Company), HP, CISCO, Fortinet and Palo Alto. Supporting secure connectivity to customer sites as well as proactive network intrusion detection and prevention systems.

Section 4, Subsection 5.17.2 - The transfer of information must be over secure channels and all data in motion must be encrypted, for instance using SMB 3 security enhancements.
Vendor Response: WILL COMPLY

Gemalto confirms that all data transfer will be over secure channels as required by the State. Gemalto understands the sensitivity of credential information stored by our systems and we take a proactive approach to ensure the security of systems and the data that we process. To ensure that data is properly protected, we use multiple levels of encryption for stored data and data in motion.

Section 4, Subsection 5.18 - Card Production Data Files

Section 4, Subsection 5.18.1 - The Agency will send the standard card production data file once daily.
Vendor Response: WILL COMPLY

Gemalto understands that the Agency will send the standard card production data file once daily. As the current vendor, we are familiar with the State's card production requests. Gemalto confirms our new solution will comply and support daily card production requests.

Section 4, Subsection 5.18.2 - The Vendors solution must be capable of receiving a card production data file seven (7) days a week.
Vendor Response: WILL COMPLY

Gemalto confirms that our solution is capable of receiving a card production data file seven (7) days a week. Our platforms are designed to run 24/7 apart from planned maintenance windows of which we will confirm to the state as part of our Support & Maintenance ITIL based best practices.

Section 4, Subsection 5.19 - Management of Central Issuance Facilities

Section 4, Subsection 5.19.1 - The Vendor shall be responsible for the complete management of the central issuance facility.
Vendor Response: WILL COMPLY

Gemalto confirms that we will be responsible for the complete management of the Central Issuance Facility. **Our facility is currently managed by Gemalto and is used to produce centrally issued drivers licenses for the State of West Virginia.**

Section 4, Subsection 5.19.2 - All hardware and software necessary for the operation of the secure central issuance facilities will be the responsibility of the Vendor.
Vendor Response: WILL COMPLY

Gemalto confirms that we will be responsible for all hardware and software necessary for the operation of the secure central issuance facilities. The hardware and software platforms are currently operational and are used to centrally issue drivers licenses for the State of West Virginia in addition to our other customers.

Section 4, Subsection 5.19.3 - All staffing and operational needs will be the responsibility of the Vendor.
Vendor Response: WILL COMPLY

Gemalto forms that we will be responsible for all staffing and operational needs of the Central Issuance Facility. Our facilities are currently staffed and operational.

Section 4, Subsection 5.19.4 - Security of the central issuance facilities will be the responsibility of the Vendor and must meet the security requirements of the REAL ID Act and any Department of Homeland Security published implementation rules.
Vendor Response: WILL COMPLY

Gemalto confirms that we will be responsible for the security of the central issuance facilities. Our Naspo Class II facilities are currently used to produce Real ID compliant driver's licenses for the State of West Virginia and other customers and meets the security requirements of the REAL ID Act and Department of Homeland Security published implementation rules.

Section 4, Subsection 5.20 - Standard Processing Time.

Section 4, Subsection 5.20.1 - Cards must be mailed via US Postal Service, from the production facility no later than two (2) regular business days following the printing of the credential.
Vendor Response: WILL COMPLY

Gemalto confirms that cards will be mailed via US Postal Service, from the production facility no later than two (2) regular business days following the printing of the credential. We currently provide this level of service to many of our customers.

Section 4, Subsection 5.20.2 - Vendor must have monitoring in place to ensure card production is completed within two business days after the appropriate fraud hold period.
Vendor Response: WILL COMPLY

Gemalto confirms that we have monitoring in place to ensure card production is completed within two business days after the appropriate fraud hold period. This is a standard feature of our central issuance platform, Production Manager.

Section 4, Subsection 5.20.3 - For cards not mailed within two (2) business days after the appropriate fraud hold period, Vendor must use Express Mail or other next day service for shipping the card to the applicant at no additional cost to the Agency.
Vendor Response: WILL COMPLY

Gemalto confirms that cards not mailed within two (2) business days after the appropriate fraud hold period will be shipped via a next day service to the applicant at no additional cost to the Agency. Gemalto currently meets this requirement for other current customers.

Section 4, Subsection 5.21 - Quality Assurance (QA)

Section 4, Subsection 5.21.1 - Vendor staff will be responsible for the QA checks of all items produced at the central issuance facility, including the Agency credentials, card carriers, and the process of preparing them for mailing.
Vendor Response: WILL COMPLY

Gemalto confirms that we will be responsible for the QA checks of all items produced at out central issuance facility, including the Agency credentials, card carriers, and the process of preparing them for mailing. We use automated quality assurance modules in our MX6100 machines to provide automated QA on 100% of the cards we centrally issue. In addition, we provide 100% manual inspections to ensure print and insertion quality.

Section 4, Subsection 5.22 - Card Mailing

Section 4, Subsection 5.22.1 - The Vendor shall be responsible for all USPS fees associated with postage and shipping.
Vendor Response: WILL COMPLY

Gemalto confirms that we will be responsible for all USPS fees associated with postage and shipping. As clarified in the response to Vendor question 30 in Addendum 3, Gemalto will invoice WVDMV monthly for actual postage costs.

Section 4, Subsection 5.22.2 - The Vendor shall mail all 'FOR FEDERAL' credentials using USPS paid online 'Signature Confirmation'.
Vendor Response: WILL COMPLY

Gemalto confirms that we will mail 'FOR FEDERAL' credentials using USPS paid online 'Signature Confirmation' as required by the State.

Section 4, Subsection 5.22.3 - All 'NOT FOR FEDERAL' credentials shall be mailed via USPS, using a return address specified by the Agency, unless the two-day production time is exceeded as defined in para.5.20.3.
Vendor Response: WILL COMPLY

Gemalto confirms that all 'NOT FOR FEDERAL' credentials shall be mailed via USPS, using a return address specified by the Agency, unless the two-day production time is exceeded as defined in para.5.20.3. We use USPS presorting in order to provide the most cost effective rates to the State.

Section 4, Subsection 5.22.4 - All envelopes shall be marked with "Return Receipt Requested" to prevent forwarding.
Vendor Response: WILL COMPLY

Gemalto confirms that all envelopes shall be marked with "Return Receipt Requested" to prevent forwarding as required by the State.

Section 4, Subsection 5.22.S - If a third-party Vendor is to be used for mail sorting, their processing time must be included in the maximum two (2) business days and the Vendor must be disclosed as a subcontractor.
Vendor Response: WILL COMPLY

Gemalto confirms that if a third-party Vendor is to be used for mail sorting, their processing time must be included in the maximum two (2) business days and the Vendor must be disclosed as a subcontractor however we currently pre-sort in house and do not use a subcontractor.

Section 4, Subsection 5.23 - Card Volume

Section 4, Subsection 5.23.1 - The central issuance system must be capable of meeting yearly production needs of approximately 500,000 cards.
Vendor Response: WILL COMPLY

Gemalto confirms that our Central Issuance Facility and Systems is capable of meeting the yearly production requirements of the State (approximately 500,000) cards. We build excess capacity into our systems and local redundancy to that we can still meet the State's daily volumes in the event that a machine goes down or requires maintenance.

Section 4, Subsection 5.23.2 - Sufficient capacity must be provided to accommodate system outages including repairs and preventative maintenance.
Vendor Response: WILL COMPLY

Gemalto confirms that our Central Issuance Facility has sufficient excess capacity to accommodate system outages including repairs and preventative maintenance while still meeting the State's daily production requirements. We build excess capacity into our systems and local redundancy to ensure we meet the requirements of our customers.

Section 4, Subsection 5.24 - Billing

Section 4, Subsection 5.24.1 - All cards printed and mailed from the central issuance facilities will be billed only after successful processing and transfer to the USPS.
Vendor Response: WILL COMPLY

Gemalto confirms that all cards printed and mailed from the central issuance facilities will be billed only after successful processing and transfer to the USPS as required by the State.

Section 4, Subsection 5.24.2 - Sufficient detail must be provided to allow the Agency to reconcile card counts between the invoice, the credential issuance system, and internal Agency systems.
Vendor Response: WILL COMPLY

Gemalto confirms that our solution will provide sufficient detail to allow the Agency to reconcile card counts between the invoice, the credential issuance system, and internal Agency systems. This detail may be easily accessed within our Web Reporting System (WRS) where users can run ad-hoc reports or filter standard card production reports based on date and card type.

Section 4, Subsection 5.24.3 - The Agency will only be responsible for paying the cost per card for cards issued to an applicant. The Agency will not pay for cards rejected due to material or printing process defects, or for cards used for system testing.
Vendor Response: WILL COMPLY

Gemalto confirms that the Agency will only be responsible for paying the cost per card for cards issued to an applicant. We do not bill our customers for cards rejected due to quality or used for testing. This is how we invoice all of our current customers.

Section 4, Subsection 5.24.4 - Vendor shall invoice WVDMV monthly for actual postage costs as a pass-through cost". Postage costs should not be included in the fixed price per card.
Vendor Response: WILL COMPLY

Gemalto confirms that we will invoice WVDMV monthly for actual postage costs as a pass-through cost". Gemalto confirms that postage costs are not be included in the fixed price per card.

Section 4, Subsection 5.24.5 - Vendor is to use the most cost-effective USPS product to meet the requirements of this RFP.
Vendor Response: WILL COMPLY

Gemalto confirms that we will use the most cost-effective USPS product to meet the requirements of this RFP. Our Central Issuance Facilities use presorting to achieve reduced postage costs.

Section 4, Subsection 5.24.6 Vendor must submit monthly invoices to WVDMV for actual postage costs.
Vendor Response: WILL COMPLY

Gemalto confirms that we will submit monthly invoices to WVDMV for actual postage costs as required. We currently invoice many of our customers this way as are set up to track actual postage costs.

CARD DESIGN AND SECURITY FEATURES REQUIREMENTS

Section 4, Subsection 5.25 - Data on Secure Temporary Driver's License and ID's

Section 4, Subsection 5.25.1 - The secure temporary DL or ID will include the same data that will be printed on the permanent, standard term card, including facial image and signature.
Vendor Response: WILL COMPLY

Gemalto confirms that the secure temporary DL or ID will include the same data that will be printed on the permanent, standard term card, including facial image and signature. Temporary DL/ID can include all of the data elements produced in the final credential including portraits, signatures, demographic data, and the PDF417 barcode. Overall, the look and feel is designed to match the final credential however it is constructed from paper and not plastic.

Section 4, Subsection 5.25 .2- Must include correct expiration date of temporary credential.
Vendor Response: WILL COMPLY

Gemalto confirms that the secure temporary DL or ID will include the correct expiration date of temporary credential and NOT the expiration date of the final credential as required by the State.

Section 4, Subsection 5.25.3 - Must state on face that it is a temporary credential.
Vendor Response: WILL COMPLY

Gemalto confirms that the secure temporary DL or ID will clearly state on the face that it is a temporary credential as required by the State. Gemalto will work with the State to clearly define all secure temporary DL or ID layouts, data elements, design, and verbiage.

Section 4, Subsection 5.25.4- Must include statement, "Valid for operation of motor vehicle only".
Vendor Response: WILL COMPLY

Gemalto confirms that the secure temporary DL will include statement, "Valid for operation of motor vehicle only" for all applicable secure temporary DLs as required by the State. Gemalto will work with the State to clearly define all secure temporary DL or ID layouts, data elements, design, and verbiage.

Section 4, Subsection 5.25.5 - Must have a fraud-warning marker on the temporary credential, for any application that is marked for potential fraud, i.e. not meeting the facial 1:1 match.
Vendor Response: WILL COMPLY

Gemalto confirms that the secure temporary DL or ID will have a fraud-warning marker on the temporary credential, for any application that is marked for potential fraud, i.e. not meeting the facial 1:1 match as required by the State. Gemalto will work with the State to clearly define all secure temporary DL or ID layouts, data elements, design, and verbiage.

Section 4, Subsection 5.26 - Card Types

Section 4, Subsection 5.26.1 - Vendor's solution must produce the card types defined in Attachment G-Current Card Types, as issued by the Agency.
Vendor Response: WILL COMPLY

Gemalto agrees to collaborate with the jurisdiction to develop Driver License and Identification documents for both 'FOR FEDERAL' and 'NOT FOR FEDERAL' to meet all current card types consisting of:

- Driver License
- Bi-optic Driver License
- Bi-optic Instruction Permit
- Commercial Driver License
- Commercial Driver License Permit
- Instruction Permit
- Motorcycle Only Driver License
- Motorcycle Instruction Permit
- Bi-optic Driver License, Under 21
- Bi-optic Instruction Permit, Under 21
- Commercial Driver License, Under 21
- Commercial Driver License Permit, Under 21
- Full Class E License, Under 21
- Instruction Permit, Under 21
- Level One, Instruction Permit, Under 21
- Level Two, Instruction Permit, Under 18
- Motorcycle Only Driver License, Under 21
- Motorcycle Instruction Permit, Under 21
- Driver License, Under 21
- Non-Operators Identification
- Employee ID Card
- Sample Card

Gemalto will design the cards using only two major card designs with two orientations each. The 'Under 21' documents will be presented in a portrait format whereas the '21 and Over' documents will be presented in a landscape format. Driver Licenses will be printed on the 'Driver License' design document whereas non-Driver License documents will use the 'Identification' design. The banner of each card will feature the type document it represents.

During the CDF, all card formats and designs will be reviewed, discussed and approved to ensure that the banners symbolize exactly how the cards should be represented. At all times, Gemalto will adhere to the AAMVA requirements to ensure the documents remain compliant.

Section 4, Subsection 5.27 - Card Design.

Section 4, Subsection 5.27.1 - Card design shall be based on 2016 AAMVA DLJID Card Design Standard (http://www.aamva.org/201 6CardDesignStandard/).
Vendor Response: WILL COMPLY

Gemalto follows the current AAMVA standard (2016 DL/ID CDS) for the production of driver licenses and identification documents for our North American customers. We work with the jurisdiction to ensure their cards are compliant to the latest standard.

Each of our cards are serialized (REAL ID requirement) with preprinted inventory control numbers, and are always considered as sensitive components. Gemalto tracks each of these serialized card bodies internally so that we have accurate up-to-date accounts of what is received, on hand, used, wasted, and destroyed.

The 2016 DL/ID CDS has stringent requirements on what constitutes a compliant card design. These requirements incorporate the minimum acceptable set of features and characteristics of the document to guarantee global interoperability. AAMVA does however afford flexibility for each jurisdiction to make some changes to its design to make each document unique to their municipality.

The Gemalto card designs issued today in other jurisdictions, are created by expert designers who understand fully the importance of adhering to the AAMVA and ISO standards. Each approved card design is manufactured in the most secure manner, using the most secure equipment and materials and have been approved by AAMVA's courtesy verification process (CVP).

Gemalto participates with many working groups, including those within AAMVA, in efforts that lead toward new legislation. Gemalto monitors and responds to updates to the latest AAMVA DL/ID Card Design Standard, and Subpart D, §37.41 of the REAL ID regulation. We continually examine our customer's driver licenses, identification cards, and issuance processes to assure each maintains compliance. We have adapted our products and solutions for existing customers to help meet changing laws, rules, and regulations. We meet with our customers if there are any potential legislation changes that could impact their current solution to ascertain they are fully aware of changing requirements.

The AAMVA DL/ID CDS has stringent requirements for document dimensions, layout of the human readable data elements, text, images, as well as machine-readable technologies. There are two orientations for the documents. If the cardholder is under 21 years of age, the card layout will be represented in a portrait format whereas a 21-and-over cardholder will have their information displayed in a landscape format. The card body itself is divided into five zones. Each zone has specific guidelines to follow in terms of background color, text truncation rules, photograph format and quality, signature representation, use of security features as specified in ISO/IEC CD18013-1 for ISO Compliant Driver Licenses.

During the CDF, Gemalto will propose a representation of their documents incorporating all mandatory features and characteristics and then will present optional elements that can be incorporated. Once the CDF team develops a representation including all desired features (both mandatory and optional), Gemalto will include all features in the RQS and will present them to the jurisdiction for their approval. Throughout this process, Gemalto will always be cognizant of the required AAMVA DL/ID CDS to ensure no change prohibits the documents from being compliant.

Mandatory Data Elements that must visually appear:

Card Reference	Zone Placement	Data Element	Card type
1	II	Family Name	Both
2	II	Given Names	Both
3	II	Date of Birth	Both
4a	II	Date of Issue	Both
4b	II	Date of Expiry	Both
4d	II	Customer Identifier	Both
5	II	Document Unique Identifier	Both
	III	Cardholder Photo	Both
	II/III	Cardholder Signature	Both
8	II	Cardholder Address	Both
9	II/IV	Vehicle Classification/Categories	DL
9a	II/IV	Endorsements (Additional privileges)	DL
12	II/IV	Restrictions	DL
15	II	Cardholder Sex	Both
16	II	Height	Both
18	II	Eye Color	Both

In addition there are many optional data elements that can be presented during the CDF. The jurisdiction may choose to add additional data elements or leave the design as proposed. During the actual personalization approval process, minor changes can be made as long as they follow the AAMVA content and placement requirement guidelines.

Section 4, Subsection 5.27.2 - Card design must comply with West Virginia Code §Chapter 17B Motor Vehicle Driver's License (http://www.legi5.state.wv.us/wvcode/Code.cfm?chap=17b&art=1).
Vendor Response: WILL COMPLY

Gemalto confirms that card design must comply with West Virginia Code §Chapter 17B Motor Vehicle Driver's License as required by the State. Gemalto has a clearly defined Card Design Forum process to ensure compliance will all of our customers' requirements including State Legislation.

Section 4, Subsection 5.28 - Card Materials and Security Features

Section 4, Subsection 5.28.1 - Card materials must be serialized during manufacturing.
Vendor Response: WILL COMPLY

Gemalto confirms that our secure cardstock will be serialized during manufacturing. This serial number will be used to track the card throughout the entire manufacturing and personalization process. In addition, our MX6100 card personalization machines use the serial number to track the card within the machines and to ensure that right cards are attached to the right carrier.

Section 4, Subsection 5.28.2 - Specific card layout and design will be selected during the planning phase after contract award.
Vendor Response: WILL COMPLY

When designing a highly secure driver license, the primary task is to identify potential threats. Because it is so prevalent, the driver's license is the official identification card for North America. It must be carried at all times when operating a vehicle and, in most locations, it must be presented to law enforcement upon request. It also serves as a source document to obtain additional identification documents, such as a passport, and is accepted as proof of identity to board domestic aircraft. With its clear importance, the potential threats to the driver's license are high, requiring detailed planning to counteract these threats.

Necessary security measures must be selected to counter any potential threats. These measures are security features that typically include special inks, security printing processes, optical variable devices, and/or special features incorporated into the card body structure.

Printed features serve as the foundation to all security documents. Gemalto's manufacturing facilities offer state of the art security printing and card construction. As requested in the RFP, all security features will be proposed after award. West Virginia can be assured that Gemalto will be able to meet or exceed any expectation for a secure document offering. As described in Section 4.4, Gemalto has a very robust process to ensure the jurisdiction plays an integral part in the design of their documents. There are a standard suite of features that Gemalto always recommends but will present all applicable features during the CDF.

The goal is to choose a substrate that is highly resistant to change. Your documents will come into contact with environmental conditions and accidental or deliberate misuse. This can leave your credential susceptible to chips, tearing or delamination. Gemalto recommends PET/PVC as the standard offering for customers requiring a durable substrate (5-10 year life) with a color photo. The Polyethylene Terephthalate (PET) core is an excellent substrate for security printing while the Polyvinyl Chloride (PVC) layer has been proven to be an excellent substrate to apply secure laminates to during post-personalization.

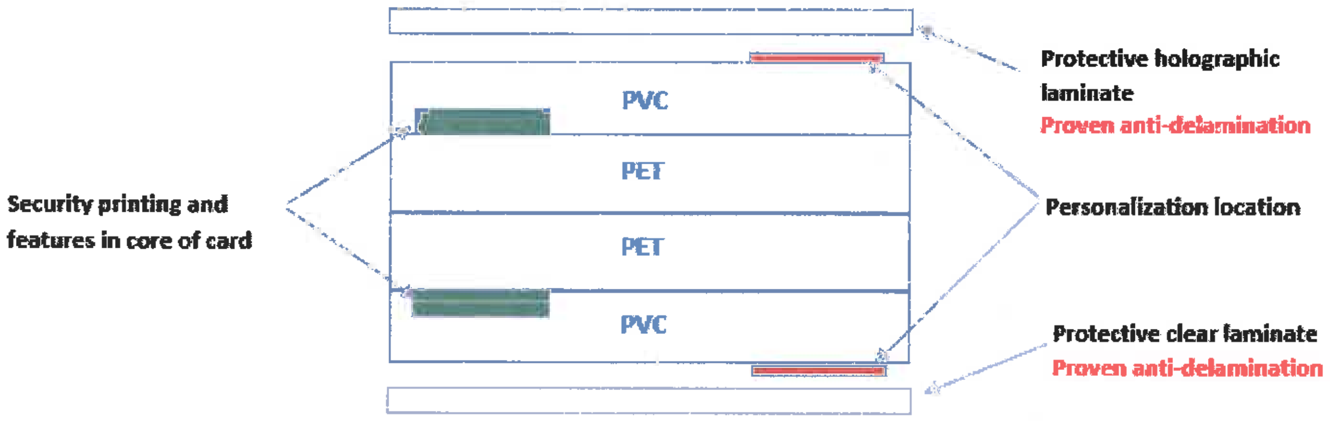

PVC
PET
PET
PVC
Security printing and features in core of card
Protective holographic laminate
Proven anti-delamination
Personalization location
Protective clear laminate
Proven anti-delamination

FIGURE 4: PET PVC CARD STRUCTURE

Our PET/PVC offering is personalized via a thermal retransfer printing process. This composition substrate provides a more durable offering that can withstand higher heat settings required for retransfer printing and lamination. This PET/PVC composite substrate is bonded together with special adhesives and pressure providing a more resilient card body with added security capability.

Gemalto offers the largest portfolio of security features in the industry. While designing your credential, our design and security experts will propose the best combination of features to provide the most security for your jurisdiction while also providing an attractive document that all West Virginians will be proud to carry. All our offerings exceed all card format and design requirements in the 2016 release of the "*AAMVA DL/ID Card Design Standard*".

Section 4, Subsection 5.28.3 - The credential must comply with 2016 AAMVA DLJID Card Design Standard - Annex B Physical Security requirements listed (http://www.aamva.org/2016CardDesignStandard/).
Vendor Response: WILL COMPLY

Gemalto is very familiar with the 2016 AAMVA DL/ID Design Standards specified in Annex B and ensures all North American DL/ID documents adhere to these standards. The key requirements are categorized in four categories of security features:

- Card Design
- Security Design
- Security Ink/Pigments
- Protecting Personalized Data Protection

AAMVA recognizes three security feature levels:

- Level 1 – A Level 1 security device supports first line inspection. These features can be easily seen or felt.
- Level 2 – A Level 2 security device supports second line inspection. These features typically require investigative equipment such as UV lights or magnifying glasses in order to view them.
- Level 3 – A Level 3 security device supports third line inspection. These are typically known to few people and require forensic equipment in order to view them

The PET/PVC substrate offers a large portfolio of AAMVA Card Design Level 1 and Level 2 security features that work together to protect against efforts by the criminal to do the following:

- Counterfeit, alter, simulate or reproduce a genuine document
- Alter, delete, modify, mask, or tamper with data concerning the original or lawful card holder
- Substitute or alter the original or lawful card holder's photograph and/or signature by any means
- Create a fraudulent document using components from legitimate driver licenses or identification cards

Compliance to the 2016 AAMVA DL/ID CDS for printed cards requires that each document meet the minimum mandatory security features defined for each family: **Card Body; Security Design**; and **Background Printing**, plus include the defined number of optional security feature within each family. Each document must also include at least one covert level 3 feature, which requires forensic inspection.

Gemalto produces secure documents by utilizing a combination of security features that provide different levels of security under different levels of analysis, and that also provide reasonable tradeoffs between accessibility and complexity. Gemalto selects a combination of different features that span overt, covert and forensic functions and act to complement each other in the document. We understand the importance of Level 1 features as the majority of the inspections are performed without the use of any tools. The front line needs to have features they can rely upon to differentiate the genuine from the counterfeit. When available for closer inspection, our Level 2 features provide a strong confidence level during authentication. Gemalto will propose a Level 3 forensic feature that is impossible to duplicate.

Gemalto has manufactured secure identification documents for decades. Our identification cards and driver licenses are produced in the most secure manner. Beginning with sheets of layered plastics, we build our substrates to incorporate security features within the document. Any attempt to alter these substrates fractures the document, making identification of this attack extremely obvious to even the casual inspector. Then we apply security printing with industrial printing presses able to produce designs, colors, patterns, and security features that desktop printers cannot replicate. Our personalization information is protected by state of the art security laminates that make photo substitution impossible to undertake without obvious signs of tampering.

Each of Gemalto's card body offerings are compliant with the 2016 AAMVA DL/ID CDS. Each offering is a UV-A dull substrate material and adheres to the mandatory security feature set guidelines. Our offerings have fixed printed dynamic data on different layers, are tamper evident and are bonded securely. Many of the other optional items found in the Gemalto offerings such as the pre-printed serial numbering are included in all offerings.

Card Body Design: 1 Mandatory feature (M) and at least 2 optional features (O)

#	Security Feature	AAMVA M/O	Gemalto Feature
1.1	UV-A dull substrate material	M	✓
1.2	Fixed printed and/or dynamic data on different layers	O	✓
1.3	Tamper evident card body	O	✓
1.4	Taggant substances for genuine authentication	O	Gemalto optional feature
1.5	Look through element (transparent) such as window	O	✓
1.6	Look through element comprising grey levels	O	Gemalto optional feature
1.7	Card core inclusions	O	✓
1.8	Pre-printed serial number on card blanks	O	✓
1.9	Embossed surface pattern	O	Gemalto optional feature for PC cards
1.10	Embedded thread, fiber or planchette	O	n/a
1.11	Security bonding	O	✓

Security Design

When designing a secure DL/ID, the primary task is to identify any potential threats. Once identified, the necessary security measures are selected to counter these potential threats. Finally, a visually aesthetic design incorporating these security features is chosen. Virtually all of the security features below are offered in Gemalto's portfolio. As you see in the table below, Gemalto far exceeds the requirements for security design.

Security Design, Resistant to Reproduction: 2 Mandatory features (M) and at least 2 optional features (O)

#	Security Feature	AAMVA M/O	Gemalto Feature
2.1	No CMYK colors and at least 2 special colors	M	✓
2.2	Guilloche design	M	✓
2.3	Anti-scan pattern	O	✓
2.4	Micro printed text	O	✓
2.5	Duplex security pattern	O	✓
2.6	Rainbow printing	O	✓
2.7	Deliberate error into the design or microprint	O	✓
2.8	Use of non-standard type-fonts	O	optional
2.9	Front to back (see through) register	O	optional
2.10	Micro Optical Imaging	O	optional

Background Printing
After a secure design is created, the Gemalto manufacturing facility takes the artwork and converts it to press-ready media so our expert printers can begin the process of applying secure ink to plastic. As you see in the table below, Gemalto meets the mandatory and optional requirements of this family of requirements, and addresses each of the other features as options.

Security Inks/Pigments: 1 Mandatory feature (M) and at least 2 optional features (O)

#	Security Feature	AAMVA M/O	Gemalto Feature
3.1	Security background printing	M	✓
3.1.1	UV fluorescent ink in security background	O	✓
3.1.2	Optical effect pigments (other than UV or IR pigments)	O	optional
3.1.3	IR-fluorescent ink	O	optional
3.1.4	IR-drop out inks	O	optional
3.1.5	Non-optical effect pigments	O	optional
3.1.6	Metameric Ink	O	optional
3.1.7	Phosphorescent Ink	O	optional
3.1.8	Tagged Ink	O	✓

Finally, in the Protecting Personalized Data Features (Table B.4) of the 2016 AAMVA DL/ID CDS, there are four mandatory and at least one optional feature required. Gemalto will propose features to meet these requirements upon award.

Level 3 Feature

Gemalto includes one (1) Level 3 feature which will be disclosed post award under controlled conditions. This feature is not described any further in this response and the necessary information will only be delivered to a designated jurisdiction appointee following contract award. Gemalto will demonstrate the existence of this Level 3 security feature in a private session with the jurisdiction appointed designee, as required.

The security features Gemalto will propose from Tables B.1, B.2, and B.3 are applied in our card manufacturing process using thermal retransfer printing. These features are embedded with the card. The features we will propose from Table B.4 are applied using laser engraving. The pre-printed serial number on card blanks (REAL ID) will be applied using laser engraving.

Gemalto's entire cardstock manufacturing process is not generally commercially available and is extremely cost prohibitive and requires great skill and years of experience to perfect. It is important to understand that the cardstock is comprised of multiple layers so that we can apply security printing and features on multiple layers making if far more difficult to alter or modify. These layers are printed in large sheets, collated, and laminated in such a way as to be fused with only heat and pressure so that it is a solid structure.

During the Collaborative Design Forum Gemalto will define the locations for our standard offerings and welcome the opportunity to discuss additional optional features.

Section 4, Subsection 5.29 - Card Design Changes

Section 4, Subsection 5.29.1 - Any changes to the card design will be handled by Change Request, approved by the agency based on an hourly rate as defined in Attachment C Cost Sheet.
Vendor Response: WILL COMPLY

Gemalto confirms that any changes to the card design will be handled by Change Request, approved by the agency based on an hourly rate as defined in Attachment C Cost Sheet as required by the State.

Section 4, Subsection 5.29.2 - Vendor must implement card format changes within 30 days of Change Request approval.
Vendor Response: WILL COMPLY

Gemalto confirms that implement card format changes within 30 days of Change Request and updated layout approval.

Section 4, Subsection 5.30 - Consumables for Secure Temporary DL

Section 4, Subsection 5.30.1 - Secure paper stock to produce secure temporary DL will be provided to the Agency by the Vendor.
Vendor Response: WILL COMPLY

Gemalto confirms that secure paper stock to produce secure temporary DL will be provided to the Agency by the Gemalto. Our proposed secure paper stock includes the following security features:

- **UV Fibers** - fibers are visible when put under a UV light source **(Illustrated Below).**
- **Toner Retention/Fusion** – this allows the toner to penetrate the paper deeply making it difficult to change.
- **Chemically Reactive Stains**– this causes the stock to stain if bleach or other chemicals are used.
- **Microtext** – This text is printed on the substrate and requires magnification to read with the naked eye.

COVERT SYSTEM REQUIREMENTS

Section 4, Subsection 5.31 - The Agency requires system functionality to support the issuance of covert credentials. For security reasons, details of the desired functionality will not be provided as part of the Request for Proposal. The Agency believes that Vendors understand the needs for this type of program and will be able to address those needs appropriately during the planning and design phase of the project. Vendor must not include details of their covert systems in their response but must acknowledge that this is a required functionality that must be provided.

Vendor Response: WILL COMPLY

Gemalto confirms that our solution supports the issuance of covert credentials. We have implemented this feature for some of our current customers and have designed it in a way to prevent covert issuances from being distinguishable from normal issuances within our solution so that if there was a mole in the Agency, they would not be able to uncover the true identity of undercover officers.

MAINTENANCE AND SUPPORT.

Section 4, Subsection 5.32 - This is a critical system and shall be operational and fully supported 7:00 a.m. to 8:00 p.m. EST Monday through Friday, and 7:00 a.m. to 2:00 p.m. EST on Saturday.

Vendor Response: WILL COMPLY

Gemalto confirms that our solution will be fully operational and fully supported 7:00 a.m. to 8:00 p.m. EST Monday through Friday, and 7:00 a.m. to 2:00 p.m. EST on Saturday. Our solution is designed to be fully operational 24/7 to facilitate after hours investigations, reporting, and other scenarios.

Section 4, Subsection 5.33 - The Vendor's solution must be compatible with the networking and operating environment established by the Office of Technology at the time of award, currently consisting of:

5.33.1 Internet Explorer version: 11
5.33.2 Java version: 7
5.33.3 .NET Framework version: 4.1

Vendor Response: WILL COMPLY

Gemalto confirms that our current solution is compatible with the networking and operating environment established by the Office of Technology as currently listed including Internet Explorer version: 11, Java version: 7, and .NET Framework version: 4.1. We will maintain compliance with the Office of Technology throughout the life of the contract as required by the State. Changes to the environment will be managed through the Change Request process as specified below in "Section 4, Subsection 5.34".

Section 4, Subsection 5.34 - Changes to this environment will be addressed by Change Order as this environment could change as new security vulnerabilities are identified and addressed in future updates.

Vendor Response: WILL COMPLY

Gemalto confirms that changes to the IT environment will be addressed by Change Order as this environment could change as new security vulnerabilities are identified and addressed in future updates. This is standard procedure for our IT and support processes.

Section 4, Subsection 5.35 - The Vendor's solution must maintain full functionality and operations with any Office of Technology published security update within 30 days of scheduled release.

Vendor Response: WILL COMPLY

Gemalto confirms that our solution will maintain full functionality and operations with any Office of Technology published security update within 30 days of scheduled release as required by the State. Gemalto confirms that changes to the IT environment such as WVOT security updates will be addressed by Change Order raised by the state.

PROJECT MANAGEMENT Responsibilities

Section 4, Subsection 5.36 - Project Work Plan

Section 4, Subsection 5.36.1 - The project work plan will be as detailed, as possible with the understanding that it will be revised during the planning and initiation phase of the project.
Vendor Response: WILL COMPLY

Gemalto confirms that the project work plan will be as detailed, as possible with the understanding that it will be revised during the planning and initiation phase of the project. This will be managed, monitored, and modified by the PMP certified Gemalto project manager.

Section 4, Subsection 5.36.2 - The project work plan will be a living document that must be kept up to date with tasks completed, modified, or added through the life of the project.
Vendor Response: WILL COMPLY

Gemalto understands that the project work plan will be a living document and confirms that it will be kept up to date with cards completed, modified, or added throughout the life of the project. This process will be managed and monitored by the PMP certified Gemalto project manager.

Section 4, Subsection 5.36.3 - The project work plan will be used as a measurement of progress.
Vendor Response: WILL COMPLY

Gemalto confirms that the project work plan will be used as a measurement of progress. Project status measurement in addition to risk and issue monitoring will be performed by the PMP certified Gemalto project manager.

Section 4, Subsection 5.37 - Performance Testing

Section 4, Subsection 5.37.1 - Performance testing shall end when the system has met the standard of performance for a period of seven (7) consecutive calendar days. The standard of performance shall mean the system operates in conformance with the Vendor's technical and functional specifications, in conformance with this contract, and in conformance to the mutually agreed test criteria.
Vendor Response: WILL COMPLY

Gemalto confirms that performance testing shall end when the system has met the standard of performance for a period of seven (7) consecutive calendar days. We have taken this into consideration and factored in additional time in our Project Plan and proposed schedule.

Section 4, Subsection 5.37.2 - If the System fails during a seven (7) day period, the Vendor will re-start performance testing. The testing shall continue daily until the standard of performance is met, without downtime, for a total of seven (7) calendar days.
Vendor Response: WILL COMPLY

Gemalto understands that if the System fails during a seven (7) day period, the Vendor will re-start performance testing. Gemalto confirms that testing shall continue daily until the standard of performance is met, without downtime, for a total of seven (7) calendar days. This requirement will be included in our Acceptance Test Plan to ensure compliance with the State's requirements.

Section 4, Subsection 5.37.3 - The Vendor is to provide the mechanism to create load and stress conditions. Metrics and results of the load and stress testing must be provided to the Agency for review and approval.
Vendor Response: WILL COMPLY

Gemalto confirms that we will provide a mechanism to create load and stress conditions and metrics/results of the load and stress testing will be submitted to the Agency for review and approval. Agency. We use Soap UI which is testing software which enables to test both functionality and performance in real world conditions. This allows us to perform actions such as simulating transaction volumes and increasing them until the system breaks so we know the real works limits or simulate connections speeds between the primary and disaster recovery data center and various field offices (if the State was considering changing or upgrading infrastructure).

Section 4, Subsection 5.38 - Change Control Plan

Section 4, Subsection 5.38.1 - The Vendor shall develop, implement, and maintain a Change Control Plan, subject to the Agency approval, in accordance with industry standards that sets forth the procedures for controlling changes to project scope, cost, schedule, and quality requirements. The Change Control Plan shall include the procedures and entities involved with requesting, evaluating and approving changes to the project deliverables.
Vendor Response: WILL COMPLY

Gemalto confirms that we will develop, implement, and maintain a Change Control Plan, subject to the Agency approval, in accordance with industry standards that sets forth the procedures for controlling changes to project scope, cost, schedule, and quality requirements. Gemalto's change request process follows the standards of the Project Management Institute and will be managed by our PMP certified project manager.

Section 4, Subsection 5.38.2 - All changes must be documented. Approval must be obtained prior to any work on changes. Documented changes must have official sign-off by both the Agency and Vendor project managers and must include the reason for the change.
Vendor Response: WILL COMPLY

Gemalto confirms that all changes will be documented. We will not proceed with implementation without approval in the form of official sign-off by both the Agency and Gemalto project managers and will include the reason for the change. This requirement follows our standard change request process. We currently follow this process for the State of West Virginia.

Section 4, Subsection 5.39 - Change Orders

Section 4, Subsection 5.39.1 - Care must be taken when evaluating the requirements and preparing the cost proposal. Change orders are rarely approved. If a scope change does occur impacting the cost or timeline of the project, the Agency Project Manager and the Agency Purchasing Office must be notified in writing immediately upon discovery and BEFORE any work takes place.
Vendor Response: WILL COMPLY

Gemalto forms that we have taken care in our evaluation of the Agency's requirements and in preparation of our cost proposal. As the current vendor, we understand the requirements of the Agency and have factored this into our cost proposal. Gemalto confirms that our PMP certified project manager will notify the Agency the Agency Project Manager and the Agency Purchasing Office immediately, in writing, upon the discovery of any issues and before any work is started.

Section 4, Subsection 5.39.2 - Change orders submitted for work that has already been completed will NOT be considered. Written approval must be obtained prior to any work that is considered outside the original scope.
Vendor Response: WILL COMPLY

Gemalto understand that change orders submitted for work that has already been completed will NOT be considered. We will seek written approval prior to starting any work that is considered outside the original scope. This will be monitored and managed by the Gemalto project manager.

Section 4, Subsection 5.40 - Upgrades, Patches, Fixes, or Other System Updates

Section 4, Subsection 5.40.1 - Ongoing changes to the Vendor's systems or hardware must be documented, tested, and approved by the Agency. Any changes during the life of the contract fall under the testing criteria listed above in paragraph 4.30 thru 4.33.
Vendor Response: WILL COMPLY

Gemalto confirms that ongoing changes our systems and hardware will be documented, tested, and approved by the Agency and will fall under the testing criteria as defined by the State. Documentation, approval, testing, and updates to our specifications, user guides, and training materials are all part of our standard change request process.

Section 4, Subsection 5.40.2 - Implementation or release of Vendor changes to any of the Vendor's software or hardware must be scheduled and approved by the Agency.
Vendor Response: WILL COMPLY

Gemalto confirms that implementation or release of changes to any of our software or hardware will be scheduled and approved by the Agency. This will be managed by the Gemalto project manager during initial project delivery and the service delivery manager during the remainder of the contract.

Section 4, Subsection 5.40.3 - In the event of a problem with the upgrade, patch, fix, or other system updates, the Vendor shall have a plan to immediately restore the previous version or release to keep facilities in production.
Vendor Response: WILL COMPLY

Gemalto confirms that we will have a plan to immediately restore the previous version or release to keep facilities in production in the event of a problem with the upgrade, patch, fix, or other system updates. We follow IT industry best practices, version control, and use software deployment suites that enable us to quickly roll back to earlier versions of software.

Section 4, Subsection 5.41 - Right to Reproduce and Distribute

Section 4, Subsection 5.40.1 - All training material and documentation of this system will become the property of the Agency, which includes the right to reproduce documentation for distribution to system users and managers. All training material and documentation is subject to the Agency approval prior to use.
Vendor Response: WILL COMPLY

Gemalto confirms that the Agency will have the right to reproduce documentation for distribution to system users and managers, all training material and documentation of this system will become the property of the Agency, and all training material and documentation is subject to the Agency approval prior to use.

Section 4, Subsection 5.42 - Training Plan

Section 4, Subsection 5.42.1 - Training dates for Train-the-Trainer will be determined as part of the implementation plan. The Vendor will be responsible for delivering the training to all employees designated as Train-the-Trainers.
Vendor Response: WILL COMPLY

Gemalto confirms that all training dates, including dates for "Train-the-Trainer" sessions will be included into our overall implementation plan. Gemalto will deliver \ training to all employees designated as Train-the-Trainer as required by the Agency.

Section 4, Subsection 5.42.2 - The training plan will be subject to the Agency's approval.
Vendor Response: WILL COMPLY

Gemalto confirms that the training plan will be subject to the Agency's approval. We will submit a Training Plan to the State as required as part of our overall Project Plan.

Section 4, Subsection 5.43 - Training Costs

Section 4, Subsection 5.43.1 - The cost of all training and training materials must be included in cost of the card. The Agency will not be responsible for vendor related travel expenses associated with installation or training at facilities.
Vendor Response: WILL COMPLY

Gemalto confirms that the cost of all training and training materials is included in our cost per card. This Agency will not be responsible for any additional training costs unless the scope of training is modified and mutually approved through the change request process.

Section 4, Subsection 5.44 - Implementation Plan

Section 4, Subsection 5.44.1 - The Vendor must fully implement the system and all components at all facilities in the State of West Virginia by October 1, 2019.
Vendor Response: WILL COMPLY

Gemalto confirms that we will fully implement the system and all components at all facilities in the State of West Virginia by October 1, 2019. As the current vendor, we can mitigate any risk to the State as we are already experienced and knowledgeable with regards to Agency systems, operations and business requirements. We have taken the required implementation date into consideration in our preliminary project plan detailed in "A-03-Attachment A-Vendor Response Sheet".

Section 4, Subsection 5.45 - Data Migration

Section 4, Subsection 5.45.1 - The Vendor must provide a detailed plan for migrating the data from the current MIDS image database into the new central image/demographic system database.
Vendor Response: WILL COMPLY

Gemalto confirms that we will provide a detailed plan for migrating the data from the current MIDS image database into the new central image/demographic system database. **As the current vendor, we understand the architecture of the current database and can guarantee that 100% of the State's records will be migrated into the new solution.**

Gemalto will ensure that the data identified as requiring migration during the Project Data Migration Workshop with the State will be migrated following the Gemalto Data Migration Methodology depicted below. The migration will be documented (Data Migration Plan) as part of the project implementation plan.

------------------------------------BEGIN Gemalto Trade Secret Information------------------------------

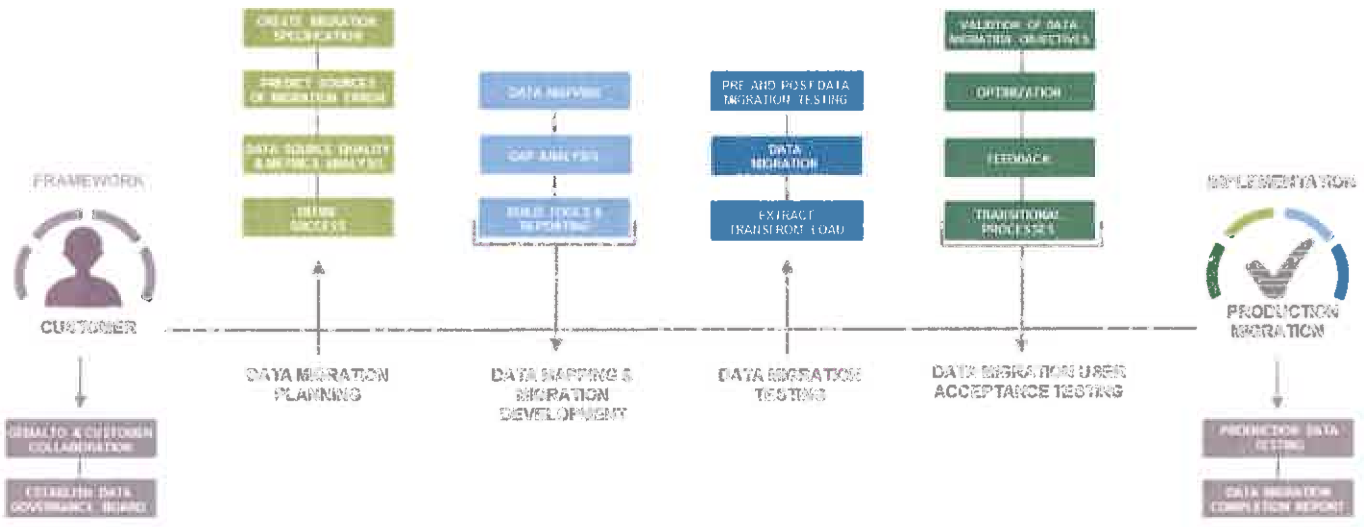

FRAMEWORK
CUSTOMER
GEMALTO & CUSTOMER COLLABORATION
ESTABLISH DATA GOVERNANCE BOARD
CREATE MIGRATION SPECIFICATION
PREDICT SOURCES OF MIGRATION ERROR
DATA SOURCE QUALITY & METRICS ANALYSIS
DEFINE SUCCESS
DATA MIGRATION PLANNING
DATA MAPPING
GAP ANALYSIS
BUILD TOOLS & REPORTING
DATA MAPPING & MIGRATION DEVELOPMENT
PRE AND POST DATA MIGRATION TESTING
DATA MIGRATION
EXTRACT TRANSFROM LOAD
DATA MIGRATION TESTING
VALIDATION OF DATA MIGRATION OBJECTIVES
OPTIMIZATION
FEEDBACK
TRANSITIONAL PROCESSES
DATA MIGRATION USER ACCEPTANCE TESTING
IMPLEMENTATION
PRODUCTION MIGRATION
PRODUCTION DATA TESTING
DATA MIGRATION COMPLETION REPORT

FIGURE 5 - DATA MIGRATION METHODOLOGY

The criteria that constitutes the 100% successful migration will also be defined and mutually agreed upon in the Project Data Migration Workshop and documented in the Data Migration Plan which will be provided to the State, in addition to the final Data Migration Report post deployment of the solution across the State.

------------------------------------END Gemalto Trade Secret Information---------------------------------

SERVICE LEVEL AGREEMENT

Section 4, Subsection 5.46 - Preventive and Remedial Maintenance

Section 4, Subsection 5.46.1 - The Vendor shall provide all remedial and preventative maintenance for all system components (hardware and software) including provision of all parts and labor during the term of the contract.

Vendor Response: WILL COMPLY

Gemalto confirms that we will provide all remedial and preventative maintenance for all system components (hardware and software) including provision of all parts and labor during the term of the contract. Field support will be provided by the field technicians currently supporting the Agency who are already familiar with the State's facilities, locations, and staff.

Section 4, Subsection 5.46.2 - On-site remedial and preventative maintenance for facility equipment shall be available during facility working hours, generally between 7:00am and 8:00pm, Eastern Time, Monday through Friday, and 7:00am and 2:00pm, Eastern Time on Saturday.

Vendor Response: WILL COMPLY

Gemalto confirms that on-site remedial and preventative maintenance for facility equipment shall be available during facility working hours, between 7:00am and 8:00pm, Eastern Time, Monday through Friday, and 7:00am and 2:00pm, Eastern Time on Saturday as required by the Agency.

Section 4, Subsection 5.46.3 - Preventative maintenance for the central image/demographic system and/or facial recognition system components must be completed during pre-arranged maintenance windows, generally on weekends, outside of normal business hours.

Vendor Response: WILL COMPLY

Gemalto confirms that preventative maintenance for our Central Server (CS) solution (central image/demographic system and/or facial recognition system components) will be completed during pre-arranged maintenance windows, generally on weekends, outside of normal business hours. The Gemalto Service Delivery Manager will work with the Agency and Office of Technology to schedule all planned maintenance.

Gemalto will issue a MOP (Methods of procedure) for any pre-arranged maintenance to be coordinated with the relevant members of the state to notify them and request approval to proceed. The MOP is a document detailing a step-by-step sequence of actions to be executed by maintenance/operations technicians performing an operation or action that implies a change of state in the solution. Such actions include switching servers on or off, opening or closing firewall ports, and other actions that could pose a risk to the normal operation of the data center. The purpose of an MOP is to control actions to ensure the desired outcome. In addition the MOP includes a roll-back plan to ensure the system can be returned to its original state before any changes were applied.

Section 4, Subsection 5.46.4 - No costs related to maintenance of hardware and software, including travel time and expenses, shall be billable to the Agency. These costs must be included in the cost per card.
Vendor Response: WILL COMPLY

Gemalto confirms that all ICW maintenance costs have been included in our cost per card and that the Agency will not be charged for any costs related to the maintenance of hardware or software including travel time and expenses.

As per the answer to question 94 in addendum 3, the state will be responsible for WVOT hosting fees for OS, database, hardware and system software at WVOT.

Section 4, Subsection 5.47 - Service Response Times

Section 4, Subsection 5.47.1 - Chronic or repeat issues - the Vendor will immediately dispatch a system expert to the site of the local image server or facial recognition system if a problem remains undiagnosed and/or unresolved after twenty-four (24) hours, and if the problem affects facility operations or other issuance or retrieval operations or prevents or impedes proper database storage and back up processes, even if it does not result in down time.
Vendor Response: WILL COMPLY

Gemalto confirms that we will immediately dispatch a system expert to the site of the local image server or facial recognition system if a problem remains undiagnosed and/or unresolved after twenty-four (24) hours, and if the problem affects facility operations or other issuance or retrieval operations or prevents or impedes proper database storage and back up processes, even if it does not result in down time. We have multiple levels of technical support and will escalate any issue with our Central Server (CS) solution.

Section 4, Subsection 5.47.2 - If reported problems are not resolved within the required response times, the Vendor shall be deemed in default of these standards of performance. In such an instance, the Vendor and the Agency will determine if it is necessary to provide an alternative solution that allows operations to continue.
Vendor Response: WILL COMPLY

Gemalto understands that if reported problems are not resolved within the required response times, Gemalto shall be deemed in default of these standards of performance. In this instance, Gemalto will work with the Agency to determine if it is necessary to provide an alternative solution that allows operations to continue.

Section 4, Subsection 5.47.3 - Support issues, tickets, or calls must not be closed without confirmation from the Agency that the issue has been resolved.
Vendor Response: WILL COMPLY

Gemalto confirms that all support issues, tickets, or calls must not be closed without confirmation from the Agency that the issue has been resolved.

Section 4, Subsection 5.48 - System Availability

Section 4, Subsection 5.48.1 - All image capture workstations must be available during regular Agency business hours, and during extended hours for special events as needed.
Vendor Response: WILL COMPLY

Gemalto confirms that all image capture workstations (ICW) will be available during regular Agency business hours, and during extended hours for special events as needed. Our solution is designed to be operational 24/7 so we will not have any issues for special events as needed.

Section 4, Subsection 5.48.2 - All servers used as part of the Vendor solution must be configured for automatic failover to minimize system downtime.
Vendor Response: WILL COMPLY

Gemalto confirms that all servers used as part of the Vendor solution will be configured for automatic failover to minimize system downtime. Our solution has been designed to automatically recover in these scenarios and we will work with the Office of Technology to ensure that servers are configured to automatically fail over and will test this with the Agency as required.

Section 4, Subsection 5.48.3 - Monthly maintenance windows for servers will be established, and the Vendor must provide notification of their intent to utilize the maintenance window no less than 1 week in advance.
Vendor Response: WILL COMPLY

Gemalto confirms that monthly maintenance windows for servers will be established, and Gemalto will provide notification of their intent to utilize the maintenance window no less than 1 week in advance. This will be managed and coordinated by the Gemalto Service Delivery Manager sending a MOP (Method of Procedure) detailing the maintenance activities to the state for approval.

Section 4, Subsection 5.48.4 • Downtime is defined as any time that any portion of the ICW or FRS systems are unavailable for normal business operations; and when the Agency approved work around is not available.
Vendor Response: WILL COMPLY

Gemalto understands that downtime is defined as any time that any portion of the ICW or FRS systems are unavailable for normal business operations; and when the Agency approved work around is not available.

Section 4, Subsection 5.48.5 - Downtime will start from the time the Agency first notifies the Vendor's designated representative or Help Desk of the inoperative condition until it is returned to working order.
Vendor Response: WILL COMPLY

Gemalto understands that downtime will start from the time the Agency first notifies the Gemalto designated representative or Help Desk of the inoperative condition by completing/submitting an Incident Form that details the inoperative condition and the time measured will be until it is returned to working order and will use this to measure our issue resolution performance.

The Incident Form is used to assist Gemalto to record and diagnose the issue, the final specifications of the content of the form shall be defined during the specifications phase of the project with the State.

Section 4, Subsection 5.49 - Help Desk Support

Section 4, Subsection 5.49.1 During the entire term of the contract, the Vendor will provide the Agency with a toll- free Help Desk number and email address to contact the Vendor for technical support. At a minimum, the Help Desk Hours must be:
5.49.1.1 7:00am to 8:00pm, Eastern Time Monday through Friday
5.49.1.2 7:00am to 2:00pm, Eastern Time Saturdays
5.49.1.3 Extended hours as needed for special events such as the West Virginia State Fair.
Vendor Response: WILL COMPLY

Gemalto confirms that we will provide the Agency with a toll- free Help Desk number and email address to contact the Vendor for technical support in addition to access to our online ticketing tool. Help desk hours will be, at a minimum, 7:00am to 8:00pm, Eastern Time Monday through Friday and 7:00am to 2:00pm, Eastern Time Saturdays. We will support the Agency with extended hours as needed for special events such as the West Virginia State Fair as we currently do.

Section 4, Subsection 5.50 - Field Service Support

Section 4, Subsection 5.50.1 - The Agency must be provided with a list of all field service technicians, and the technicians must have a means of identifying themselves to the Agency staff when they arrive at the Agency location.
Vendor Response: WILL COMPLY

Gemalto confirms that we will provide the Agency with a list of all field service technicians, and the technicians will have a means of identifying themselves to the Agency staff when they arrive at the Agency location. Gemalto will capitalize on our existing field technicians who are already familiar with the Agency staff.

Section 4, Subsection 5.50.1 - As part of the support agreement, Field service technicians will be required to set up and remove equipment for any special events, such as the West Virginia State Fair and other public demonstrations as determined by the State Governor or the Agency Commissioner.
Vendor Response: WILL COMPLY

Gemalto understands and confirms that field service technicians will be required to set up and remove equipment for any special events, such as the West Virginia State Fair and other public demonstrations as determined by the State Governor or the Agency Commissioner.

INFORMATION TECHNOLOGY REQUIREMENTS

Section 4, Subsection 5.51 - Communications

Section 4, Subsection 5.50.1 - The Agency will be responsible for data communication between the facilities and the Agency data center. Communication between the Agency data center and the central production facilities will be the responsibility of the Vendor.
Vendor Response: WILL COMPLY

Gemalto confirms that we will be responsible for the communication between the Agency data center and the Central Issuance Facilities as required by the Agency. Gemalto understands that The Agency will be responsible for data communication between the facilities and the Agency data center.

Section 4, Subsection 5.52 - Data Storage

Section 4, Subsection 5.52.1 - All documents scanned or collected in the application or production of a credential will be stored at the State's data center to comply with the State of West Virginia statutory requirements, administrative rules, and records retention requirements.
Vendor Response: WILL COMPLY

Gemalto confirms that all documents scanned or collected in the application or production of a credential will be stored at the State's data center and will comply with the State of West Virginia statutory requirements, administrative rules, and records retention requirements. Gemalto will work with the Agency during the planning phase of the project to clearly define and then implement all requirements related to data storage, protection, and retention.

Section 4, Subsection 5.52.2 - The data associated with this system is the property of the Agency and is not available for resale or distribution.
Vendor Response: WILL COMPLY

Gemalto confirms that data associated with this system is the property of the Agency and is not available for resale or distribution. All of the State's data will remain the sole property of the State.

Section 4, Subsection 5.52.3 - Data sent to the central production facility servers for card printing must be deleted no more than thirty (30) days after receipt of the print request.
Vendor Response: WILL COMPLY

Gemalto confirms that all data sent to the central production facility servers for card printing will be deleted no more than thirty (30) days after receipt of the print request. Gemalto will work with the Agency during the planning phase of the project to clearly define all data retention policies and procedures.

Section 4, Subsection 5.53 - Software Updates

Section 4, Subsection 5.53.1 - Major software enhancements shall be charged on an hourly basis as defined by Attachment C - Cost Sheet. These enhancements could include, but shall not be limited to, State Legislative and Federal Rule or Compliance changes.
Vendor Response: WILL COMPLY

Gemalto confirms that major software enhancements will be charged on an hourly basis as defined by "Attachment C - Cost Sheet" as required by the Agency. We accept that these enhancements could include, but will not be limited to State Legislative and Federal Rule or Compliance changes.

Section 4, Subsection 5.53.2 - The Vendor must develop and provide a formal back-out plan for all updates in the event of failure.
Vendor Response: WILL COMPLY

Gemalto confirms that we will develop and provide the Agency with a formal back-out plan for all updates in the event of failure. We will follow industry best practices for rolling back updates and changes to the system in order to minimize risk for the Agency. All updates will be deployed with a MOP (Method of Procedure) that will state a clear deployment and formal back-out plan.

Section 4, Subsection 5.54 - Change to Production System

Section 4, Subsection 5.54.1 - At no time, shall anyone on the Vendor's staff make changes to the Agency production systems without coordination with the Agency, full system testing by both the Vendor and the Agency, and strict adherence to the change management process.

Vendor Response: WILL COMPLY

Gemalto confirms that at no time, will any Gemalto staff make changes to the Agency production systems without coordination with (and approval from) the Agency, full system testing by both the Vendor and the Agency, and strict adherence to the change management process. Our change management process has strict processes and procedures in place to ensure that this requirement is adhered to. Once a Change Request is approved, the Agency will be furnished with a MOP (Method of Procedure) detailing the deployment schedule and changes that will be made.

Section 4, Subsection 5.55 - 14 Day Pre-Post Support Plan

Section 4, Subsection 5.55.1 - The successful completion of the 14-day pre-post support period as determined by the Agency shall result in System Acceptance, leading to the issuance of the first Change Order.

Vendor Response: WILL COMPLY

Gemalto confirms that the successful completion of the 14-day pre-post support period, as determined by the Agency, will result in System Acceptance, leading to the issuance of the first Change Order. This follows our standard procedure and process for system acceptance and we have taken this into account for our project plan.

Section 4, Subsection 5.56 - End of Contract

Section 4, Subsection 5.56.1 - At the end of the contract, or sooner, if the contract is terminated, the Vendor must transfer all image files and data to the Agency or third-party database and delete all relevant data from their hosted servers with written approval from the Agency

Vendor Response: WILL COMPLY

Gemalto confirms that, at the end of the contract, or sooner, if the contract is terminated, we will transfer all image files and data to the Agency or third-party database and delete all relevant data from their hosted servers with written approval from the Agency in a timely manner as required by the Agency.

By signing below, I certify that I have reviewed this Request for Proposal in its entirety; understand the requirements, terms and conditions, and other information contained herein; that I am submitting this proposal for review and consideration; that I am authorized by the bidder to execute this bid or any documents related thereto on bidder's behalf; that I am authorized to bind the bidder in a contractual relationship; and that, to the best of my knowledge, the bidder has properly registered with any State agency that may require registration.

Gemalto Inc.
(Company)

Neville Pattinson, Senior Vice President Government Sales
(Representative Name, Title)

(Signature)

6/27/2018
(Date)

1-512-257-3982
(Contact Phone/Fax Number)

Attachment C:

Cost Sheet is submitted in a separate sealed envelope as requested in the RFP instructions.

Moundsville	400 Teletech Drive, Suite 100 Moundsville, WV 26041	8:30 AM to 5:00 PM Monday through Friday	1
Parkersburg	601 Lubeck Avenue Parkersburg, WV 26101	8:30 AM to 5:00 PM Monday through Friday	2
Point Pleasant	1408 Kanawha Street Point Pleasant, WV 25550	8:30 AM to 5:00 PM Monday through Friday	1
Princeton	198 Davis Street Princeton, WV 24740	8:30 AM to 5:00 PM Monday through Friday	1
Romney	HC 63, Box 2570 Romney, WV 26757	8:30 AM to 5:00 PM Monday through Friday	1
Spencer	115 Church Street Spencer, WV 25276	8:30 AM to 5:00 PM Monday through Friday	1
Summersville	2 Armory Way Summersville, WV 26651	8:30 AM to 5:00 PM Monday through Friday	2
Weirton	100 Municipal Plaza, Suite 100 Weirton, WV 26062	8:30 AM to 5:00 PM Monday through Friday	1
Welch	92 McDowell Street Welch, WV 24801	8:30 AM to 5:00 PM Monday through Friday	1
Williamson	225 East 3rd Avenue Williamson, WV 25661	8:30 AM to 5:00 PM Monday through Friday	1
Winfield	116 Liberty Square Hurricane, WV 25526	8:30 AM to 5:00 PM Monday through Friday	1

Attachment E: Production Volumes

Not FOR FEDERAL Use Driver's License and ID

Card Type /Description	Count
Driver's License	208,258
Bioptic Driver's License	32
Bi-optic Instruction Permit	4
Commercial Driver's License	11,016
Commercial Driver's License Permit	4,329
Instruction Permit	16,389
Motorcycle Only Driver's License	5
Motorcycle Instruction Permit	5,841
Bi-optic Driver's License, Under 21	4
Bi-optic Instruction Permit, Under 21	1
Commercial Driver's License, Under 21	93
Commercial Driver's License Permit, Under 21	93
Full Class E License, Under 21	2,258
Instruction Permit, Under 21	11,791
Level One, Instruction Permit, Under 21	16,976
Level Two, Instruction Permit, Under 18	11,172
Motorcycle Only Driver's License, Under 21	0
Motorcycle Instruction Permit, Under 21	3
Driver's License, Under 21	17,036
Non-Operators Identification	53,154
Employee ID Card	3,102
Sample Card	196
Total for all types	361,757

REQUEST FOR PROPOSAL

WVDMV Driver's License and Credential Issuance System (*dmvLICENSE*) CRFP DMV1800000001

FOR FEDERAL Use Driver's License and ID

Card Type /Description	Count
Driver's License	105,150
Bi-optic Driver's License	27
Bi-optic Instruction Permit	1
Commercial Driver's License	7,956
Commercial Driver's License Permit	0
Instruction Permit	27
Motorcycle Only Driver's License	1
Motorcycle Instruction Permit	0
Bi-optic Driver's License, Under 21	5
Bi-optic Instruction Permit, Under 21	0
Commercial Driver's License, Under 21	40
Commercial Driver's License Permit, Under 21	40
Full Class E License, Under 21	850
Instruction Permit, Under 21	15
Level One, Instruction Permit, Under 21	17
Level Two, Instruction Permit, Under 18	1,277
Motorcycle Only Driver's License, Under 21	0
Motorcycle Instruction Permit, Under 21	0
Driver's License, Under 21	5,257
Non-Operators Identification	3,601
Employee ID Card	0
Sample Card	0
Total for all types	124,264

Volume by Location

Location	Count
Beckley	27,145
Charles Town	23,830
Clarksburg	29,890
Elkins	18,090
Fairmont	13,980
Flatwoods	9,283
Franklin	2,156
Huntington	30,385
IS&S – Investigations, Security & Support Services	29
Kanawha City	58,701
Kanawha City HQ – Test	68
Kanawha City HQ – Driver Services	1,081
Lewisburg	13,134
Logan	12,641
Martinsburg	27,631
Moorefield	8,394
Morgantown	35,146
Moundsville	25,475
Parkersburg	29,620
Point Pleasants	7,728
Princeton	19,260
Romney	14,292
Spencer	7,553
Summersville	11,349
Weirton	14,045
Welch	7,886
Williamson	6,147
Winfield	30,944
Total	485.883

REQUEST FOR PROPOSAL

WVDMV Driver's License and Credential Issuance System
(*dmvLICENSE*) CRFP DMV1800000001

Attachment F:

WV Division of Motor Vehicles Contract Privacy Policy

1. That the Agency is the record owner of and maintains electronic Driver Licensing and Motor Vehicle Information, including Personal Information and Sensitive Personal Information as defined in the federal Driver Privacy Protection Act ("DPPA") and the Uniform Motor Vehicles Records Disclosure Act (§17A-2A-1 et seq.) ("UMVRDA");

2. That pursuant to §17A-2A- 7(a)(1), the Driver Licensing and Vehicle Information is available for release from the Agency to a governmental agency including any entity acting on behalf of a governmental agency in carrying out its function;

3. That the Agency will permit to the Vendor computer inquiry access to the Mainframe System, if necessary, using unique employees accounts, except those records which the AGENCY has been directed not to disclose pursuant to West Virginia Code or federal law as amended, by the person about whom the record is kept;

4. That the Vendor will use the information obtained hereunder only for the purpose set forth in their Statement of Work and made a part hereof, in compliance with federal and state privacy laws and the **Privacy Program** attached to and made part of this Agreement;

5. The Vendor agrees to reimburse the AGENCY, its agents, officers and employees for all claims, loss, damage, injury and liability asserted against the AGENCY, and any of their agents, officers and employees resulting from the negligent, criminal or willful wrongful use or misuse of the information provided to the Vendor on the part of the Vendor, its agents, officers, employees, contractors or a third party;

6. The Vendor assumes full responsibility for the care, custody, control, disclosure and use of the information provided to it by the AGENCY pursuant to this Agreement. The Vendor agrees to ensure that the disclosure of information received from the AGENCY complies with this Agreement. The Vendor assumes full responsibility for its disclosure of information pursuant to all Federal and State laws governing the disclosure and protection of such information, including but not limited to, the Federal Fair Credit Reporting Act (Law 91058), Driver's Privacy Protection Act, (Public Law 103-322 at 18 U.S.C. 123), the amendment to the Driver Privacy Protection Act, (Section 350 of Public Law 106-69), the West Virginia Uniform Motor Vehicle Records Disclosure Act, hereinafter the **WVURDA** (W. Va. Code 17A-2A-1 et seq.), the Privacy Act of 1974, Computer Security Act 1987, the Federal Information Security Management Act of 2002 (FISMA P.L. 107-347, December 17, 2002), the FIPS Publication 199, Standards for Security

Categorization of Federal Information and Information Systems, FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems, OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000, NIST SP 800-44 Version 2, Guidelines on Securing Public Web Servers, and NISP SP 800-14 Generally Accepted Principles and Practices for Security Information Technology Systems and W. Va. Code §17C-5A-3, all as amended;

7. That the Vendor shall immediately notify the AGENCY upon its discovery that the Vehicle or Driver owner address information provided to it has been released, used or disclosed in violation of this Agreement, in violation of any federal law, in violation of West Virginia law or upon the filing of any claim or complaint for misuse or release of the AGENCY's Vehicle Licensing Information made against the Vendor or against the AGENCY. Immediate notification for any privacy breach means that the Vendor will notify the AGENCY by calling 304.926.0708, by calling the West Virginia Office of Technology at 304.558.9966 or 877.558.9966 and by notifying the AGENCY in writing within **24 hours** if it discovers that personal information provided under this Agreement has been used, disclosed or are being used in violation of the Agreement, or state or federal laws. Immediate notification for any privacy breach of Social Security Numbers, if applicable, means that the agency will notify the Social Security Administration within **one hour** of the breach by calling the SSA's National Network Service Center toll free at **877-697-4889**;

8. The Vendor will provide the name, title and telephone number of its designated Security Administrator, as well as a photo copy of the Administrator's state issued driver's license or non-driver identification, to AGENCY before any records are accessed. The Security Administrator will be the employee of the Vendor who is responsible for access and use of any AGENCY records. The Security Administrator will be the employee of the Vendor who is responsible for requesting log-on identification numbers from the AGENCY and to whom the AGENCY may provide log-on identification numbers. The Security Administrator is responsible for the security of all log-on identification numbers assigned to the Vendor and will ensure that the assigned log-on identification numbers and passwords are not exchanged or shared with any other person(s) or entities. **Additionally, the Security Administrator is responsible for ensuring that every Vendor employee with access to the records completes a Confidentiality Agreement and returns it to the AGENCY prior to use of the AGENCY records.** All Confidentiality Agreements are made a part of this Agreement. If the Security Administrator or any employee of the Vendor leaves the employ of the Vendor or changes job duties and no longer requires access to AGENCY records as part of their official job assignments, the Security Administrator **will immediately notify the AGENCY.** The access log-on code for the employee will be cancelled. Prior to issuing a log-on number for a new employee, the Security Administrator will submit a signed Confidentiality Agreement from that employee which will become an addendum to this

Agreement. Nothing in this Agreement authorizes the Vendor to have more than seven hundred and twenty-nine (729) log-on access numbers at a time. **Within 30 days of separation or transfer, the Security Administrator will notify the AGENCY of any authorized user who no longer needs access to our records and may make a request to authorize a new log-on access number on a one for one basis;**

9. The Vendor may not use any information provided hereunder for any purpose not listed in this Agreement without prior written approval of the AGENCY;

10. The Vendor agrees that it will not use any information contained in or derived from the records accessed from AGENCY for the purposes of marketing, surveys or solicitation;

11. The Vendor is specifically prohibited from releasing, selling, assigning or otherwise transferring information from AGENCY records to any unauthorized person, firm, association, corporation or government agency without permission in writing from the AGENCY;

12. The Vendor agrees to immediately notify the AGENCY of any claim asserted against the Vendor because of any use of the information provided pursuant to this Agreement. The Vendor agrees that AGENCY shall retain all ownership rights to the information provided pursuant to this Agreement or derived therefrom. The Vendor will enter personal information that it will verify with the AGENCY records. The Vendor agrees that it shall only use, store or combine data as authorizcd under state and federal law. The Vendor will only release information to the minimum necessary extent to execute its duties under state and federal law and in accordance with this Agreement. Provided, nothing in this Agreement prevents the Vendor from creating a database of personal information obtained from other sources;

13. The Vendor will take all reasonable precautions to protect against unauthorized access or release of AGENCY data records, confidential records or confidential information in its custody;

14. The Vendor agrees that any breach of this Agreement or unlawful use, sale or release of AGENCY records in any form by the Vendor or any of its clients will result in the immediate termination of this Agreement without prior notice to the Vendor. The Vendor agrees to reimburse to AGENCY all reasonable costs and attorney fees by the Vendor of its unlawful sale, release or use of any of AGENCY records;

15. This Agreement shall remain in full force and effect unless canceled by either party upon thirty (30) days written notice or anytime with the mutual consent of both parties. This Agreement shall terminate immediately upon discovery that any information provided to Vendor by the AGENCY has been used or disclosed in violation of this Agreement, State or Federal law. This Agreement shall terminate immediately if changes in West Virginia or Federal law prohibit the AGENCY

from releasing the information accessed by this Agreement;

16. The Vendor and its employees, agents, contractors, subcontractors, assigns and heirs who will have access to the provided AGENCY records agree to read the **Privacy Program**. All personnel who will have access to the AGENCY's records must sign a **Confidentiality Agreement** prior to access of AGENCY records. Vendor employees who will have access to the Agency's records must submit a copy of their government-issued photo ID or driver's license with photograph. Failure to comply with this provision will affect deadlines required by the Vendor to access AGENCY records. The Vendor agrees that failure to submit Confidentiality Agreements from all Vendor employees who will access AGENCY's records constitutes a breach of the Agreement and the Vendor agrees that the AGENCY may terminate the Agreement without consequence to AGENCY on that basis;

17. The Vendor hereby agrees that it will only access Personally Identifiable Information, hereinafter PII, **as required to perform its duties** under the Agreement. The Vendor understands that it is required to secure the PII that it accesses as part of this Agreement and to ensure that it is not accessed by unauthorized individuals, or released to any other persons, companies or entities. The Vendor agrees that it will not allow its employees to share account access information or passwords;

18. The Vendor agrees that it **will not release or allow access** to AGENCY records to any person or company **outside the United States of America;**

19. This document, together with the Vendor's Statement of Work, the completed Vendor Employees' Confidentiality Agreements with photo IDs and the List of Vendor employees who will have a unique access account assigned to that individual will constitute the entire Agreement between the parties;

20. This Agreement is not assignable by the Vendor;

21. Venue of any lawsuit filed by any party arising in whole or in part out of this Agreement shall be in the Circuit Court of Kanawha County; and

22. This Agreement may only be revised or amended in writing by mutual consent of both parties or with 30 days' prior written notice by either of the parties.

Vendor: Gemalto Inc

Authorized Signature: ______________________

Date: 6 / 27 / 2018

Attachment G: Current Card Types

Not FOR FEDERAL Use Driver's License and ID	FOR FEDERAL Use Driver's License and ID
Bi-optic Driver's License	Bi-optic Driver's License
Bi-optic Driver's License, Under 21	Bi-optic Driver's License, Under 21
Bi-optic Instruction Permit	
Bi-optic Instruction Permit, Under 21	
Commercial Driver's License	Commercial Driver's License
Commercial Driver's License, Under 21	Commercial Driver's License, Under 21
Commercial Driver's License Permit	
Commercial Driver's License Permit, Under 21	
Driver's License, Full Class E	Driver's License, Full Class E
Driver's License, Full Class E, Under 21	Driver's License, Full Class E, Under 21
Instruction Permit	
Level One, Instruction Permit, Under 18	
Level Two, Restricted Driver's License, Under 18	Level Two, Restricted Driver's License. Under 18
Level Three, Restricted Driver's License, Under 18	Level Three, Restricted Driver's License, Under 18
Motorcycle Only Driver's License	Motorcycle Only Driver's License
Motorcycle Only Driver's License, Under 21	Motorcycle Only Driver's License, Under 21
Motorcycle Only Driver's License, Under 18	Motorcycle Only Driver's License, Under 18
Motorcycle Instruction Permit	
Motorcycle Instruction Permit, Under 21	
Non-Operators Identification	Non-Operators Identification
Kid/ Youth Identification	
Salesperson License	
Secondary ID	
DHHR REDI	
Natural Resources Law Enforcement	
Sample Card	Sample Card

Employee ID Types

BC	Bureau of Commerce
BE	Environmental Protection
BP	Bureau of Employment Programs
CE	County Employee
DP	Division of Protective Services
DT	De artment of Transportation
ED	Department of Education
FA	Department of Administration
GI	Generic Identification
GV	Governor's Office

HD	House of Delegates
HH	DHHR
LE	Supreme Courts of Appeals
MA	De artment of Military Affairs
MV	Division of Motor Vehicles
PS	Public Service Commission
SB	WV State Bar
SE	Senate of West Virginia
SI	Commission on Special Investigations
TR	Department of Tax and Revenue

Attachment H

PII Acknowledgement

The Vendor understands that this Agreement requires access to Personally Identifiable Information or PII found within the WVDMV's records. Personally Identifiable Information includes any information that can identify a person, including, but not limited to the name, address, social security number, driver's license number, date of birth, photograph, computerized image, telephone number, medical information or disability information of any person or organization found in DMV records.

The Vendor understands that any PII obtained from the WVDMV's records is subject to the federal Driver Privacy Protection Act and the West Virginia Uniform Records Disclosure Act, hereinafter WVURDA found at West Virginia Code §17A-2A-1, et seq. A copy of the WVURDA is attached and made a part of this Agreement.

The Vendor and its' employees, agents, contractors, subcontractors, assigns and heirs agree to read the WVURDA, and all personnel who will have access to the WVDMV's records must sign a Confidentiality Agreement prior to access to PII found within the WVDMV's records. Failure to comply with this provision may affect deadlines required by the Vendor. The Vendor agrees that failure to submit Confidentiality Agreements from all Vendor users of the WVDMV's records constitutes a breach of the Agreement and the WVDMV may terminate the Agreement without consequence to WVDMV on that basis. To complete the Confidentiality Agreement, the Division's Privacy Program must be reviewed by each user. Copies of the Division's Privacy Policy and the Confidentiality Agreement are attached and are made part of this Agreement.

The Vendor hereby agrees that it will only access PII as required to perform its duties under the Agreement. The Vendor understands that it is required to secure the PII that it accesses as part of this Agreement and to ensure that it is not accessed by unauthorized individuals or released to any other persons, companies or entities.

The Vendor agrees to keep all personal and non personal information accessed from testing applicants and WVDMV confidential and protected from intentional and unintentional disclosure;

The Vendor acknowledges that authorized access or transactions provide no right to possession or ownership by the Vendor to the WVDMV's data records or to the records of the testing applicants at any time;

The Vendor shall not access or retain any data submitted by testing applicants or by the WVDMV for any reason other than the information that it is required to retain under this Agreement in its transaction logs;

The Vendor will ensure that it does not aggregate information or create any databases to information which it has access, including WVDMV's data and data submitted by testing applicants for the purposes of building comprehensive data records or for any other purpose;

The Vendor will take all reasonable precautions to protect against unauthorized access or release of WVDMV data records, confidential records or confidential information in its custody;

The Vendor will follow the notification requirement if it discovers that information or services provided under this Agreement have been disclosed or are being used in violation of the federal Driver Privacy Protection Act, the West Virginia Records Disclosure Act, the federal Privacy Act of 1974 or any other state or federal laws. **The Vendor shall also immediately notify the WVDMV within 24 hours by telephone at 304.558.2723 and by facsimile machine at 304.558.1987 as well as the West Virginia Office of Technology at 304.558.9966 or 877.558.9966 if it discovers that personal information provided under this Agreement have been disclosed or are being used in violation of the Agreement, or state or federal laws;**

AGREED:

NEVILLE PATTINSON
Printed Name

Signature

SVP GOVERNMENT SALES
Title

6/25/2018
Date

WV-10
Approved / Revised
09/15/17

State of West Virginia
VENDOR PREFERENCE CERTIFICATE

Certification and application is hereby made for Preference in accordance with *West Virginia Code*, §5A-3-37. (Does not apply to construction contracts). *West Virginia Code*, §5A-3-37, provides an opportunity for qualifying vendors to request (at the time of bid) preference for their residency status. Such preference is an evaluation method only and will be applied only to the cost bid in accordance with the *West Virginia Code*. This certificate for application is to be used to request such preference. The Purchasing Division will make the determination of the Vendor Preference, if applicable.

1. □ **Application is made for 2.5% vendor preference for the reason checked:**
Bidder is an individual resident vendor and has resided continuously in West Virginia, or bidder is a partnership, association or corporation resident vendor and has maintained its headquarters or principal place of business continuously in West Virginia, for four (4) years immediately preceding the date of this certification; **or,**

□ Bidder is a resident vendor partnership, association, or corporation with at least eighty percent of ownership interest of bidder held by another entity that meets the applicable four year residency requirement; **or,**

□ Bidder is a nonresident vendor which has an affiliate or subsidiary which employs a minimum of one hundred state residents and which has maintained its headquarters or principal place of business within West Virginia continuously for the four (4) years immediately preceding the date of this certification; **or,**

2. □ **Application is made for 2.5% vendor preference for the reason checked:**
Bidder is a resident vendor who certifies that, during the life of the contract, on average at least 75% of the employees working on the project being bid are residents of West Virginia who have resided in the state continuously for the two years immediately preceding submission of this bid; **or,**

3. □ **Application is made for 2.5% vendor preference for the reason checked:**
Bidder is a nonresident vendor that employs a minimum of one hundred state residents, or a nonresident vendor which has an affiliate or subsidiary which maintains its headquarters or principal place of business within West Virginia and employs a minimum of one hundred state residents, and for purposes of producing or distributing the commodities or completing the project which is the subject of the bidder's bid and continuously over the entire term of the project, on average at least seventy-five percent of the bidder's employees or the bidder's affiliate's or subsidiary's employees are residents of West Virginia who have resided in the state continuously for the two immediately preceding years and the vendor's bid; **or,**

4. □ **Application is made for 5% vendor preference for the reason checked:**
Bidder meets either the requirement of both subdivisions (1) and (2) or subdivision (1) and (3) as stated above; **or,**

5. □ **Application is made for 3.5% vendor preference who is a veteran for the reason checked:**
Bidder is an individual resident vendor who is a veteran of the United States armed forces, the reserves or the National Guard and has resided in West Virginia continuously for the four years immediately preceding the date on which the bid is submitted; **or,**

6. □ **Application is made for 3.5% vendor preference who is a veteran for the reason checked:**
Bidder is a resident vendor who is a veteran of the United States armed forces, the reserves or the National Guard, if, for purposes of producing or distributing the commodities or completing the project which is the subject of the vendor's bid and continuously over the entire term of the project, on average at least seventy-five percent of the vendor's employees are residents of West Virginia who have resided in the state continuously for the two immediately preceding years.

7. **Application is made for preference as a non-resident small, women- and minority-owned business, in accordance with *West Virginia Code* §5A-3-59 and *West Virginia Code of State Rules*.**
□ Bidder has been or expects to be approved prior to contract award by the Purchasing Division as a certified small, women- and minority-owned business.

Bidder understands if the Secretary of Revenue determines that a Bidder receiving preference has failed to continue to meet the requirements for such preference, the Secretary may order the Director of Purchasing to: (a) rescind the contract or purchase order; or (b) assess a penalty against such Bidder in an amount not to exceed 5% of the bid amount and that such penalty will be paid to the contracting agency or deducted from any unpaid balance on the contract or purchase order.

By submission of this certificate, Bidder agrees to disclose any reasonably requested information to the Purchasing Division and authorizes the Department of Revenue to disclose to the Director of Purchasing appropriate information verifying that Bidder has paid the required business taxes, provided that such information does not contain the amounts of taxes paid nor any other information deemed by the Tax Commissioner to be confidential.

Bidder hereby certifies that this certificate is true and accurate in all respects; and that if a contract is issued to Bidder and if anything contained within this certificate changes during the term of the contract, Bidder will notify the Purchasing Division in writing immediately.

Bidder: Gemalto, Inc. **Signed:**

Date: 6/27/2018 **Title:** Senior Vice President Government Sales

**Check any combination of preference consideration(s) indicated above, which you are entitled to receive.*

REQUEST FOR PROPOSAL

WVDMV Driver's License and Credential Issuance System (*dmvLICENSE*) CRFP DMV1800000001

By signing below, I certify that I have reviewed this Request for Proposal in its entirety; understand the requirements, terms and conditions, and other information contained herein; that I am submitting this proposal for review and consideration; that I am authorized by the bidder to execute this bid or any documents related thereto on bidder's behalf; that I am authorized to bind the bidder in a contractual relationship; and that, to the best of my knowledge, the bidder has properly registered with any State agency that may require registration.

Gemalto, Inc
(Company)

NEVILLE PATTINSON , SVP GOVERNMENT SALES
(Representative Name, Title)

512 825 3082
(Contact Phone/Fax Number)

6/27/2018
(Date)

DESIGNATED CONTACT: Vendor appoints the individual identified in this Section as the Contract Administrator and the initial point of contact for matters relating to this Contract.

Neville Pattinson, Senior Vice President Government Sales
(Name, Title)

(Printed Name and Title)
Arboretum Plaza II, 9442 Capital of TX HWY N, Suite 2-100, Austin, TX 78759
(Address)
1-512-257-3982
(Phone Number) / (Fax Number)
Neville.Pattinson@gemalto.com
(email address)

CERTIFICATION AND SIGNATURE: By signing below, or submitting documentation through wvOASIS, I certify that I have reviewed this Solicitation in its entirety; that I understand the requirements, terms and conditions, and other information contained herein; that this bid, offer or proposal constitutes an offer to the State that cannot be unilaterally withdrawn; that the product or service proposed meets the mandatory requirements contained in the Solicitation for that product or service, unless otherwise stated herein; that the Vendor accepts the terms and conditions contained in the Solicitation, unless otherwise stated herein; that I am submitting this bid, offer or proposal for review and consideration; that I am authorized by the vendor to execute and submit this bid, offer, or proposal, or any documents related thereto on vendor's behalf; that I am authorized to bind the vendor in a contractual relationship; and that to the best of my knowledge, the vendor has properly registered with any State agency that may require registration.

Gemalto, Inc.
(Company)

(Authorized Signature) (Representative Name, Title)

Neville Pattinson Senior Vice President Government Sales
(Printed Name and Title of Authorized Representative)

6/25/2018
(Date)

1-512-257-3982
(Phone Number) (Fax Number)

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: CRFQ DMV1800000001

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:
(Check the box next to each addendum received)

[x] Addendum No. 1

[X] Addendum No. 2

[x] Addendum No. 3

[X] Addendum No. 4

[ ] Addendum No. 5

[ ] Addendum No. 6

[ ] Addendum No. 7

[ ] Addendum No. 8

[ ] Addendum No. 9

[ ] Addendum No. 10

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

Gemalto, Inc.
Company

Authorized Signature

6/25/2018
Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.