



**STATE OF WEST VIRGINIA**

**SUBMITTED TO:**  
Department of Administration  
Purchasing Division  
Building 15  
2019 Washington Street, East  
Charleston, WV 25305-0130

**SEALED BID**  
Buyer: TL/32  
RFQ No. HSE01154  
Bid Opening Date: 9/7/2011  
Bid Opening Time: 1:30 p.m.

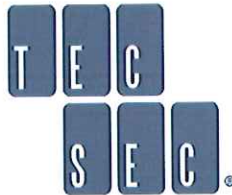
**TECHNICAL PROPOSAL**

**RESPONSE TO RFQ No. HSE01154**

**IDENTITY MANAGEMENT SERVICE OFFERING**

September 07, 2011

**SUBMITTED BY VENDOR:**



12950 Worldgate Drive, Suite 100  
Herndon, VA 20170  
Tel: 571-299-4100  
DUNS #: 965527679

RECEIVED

2011 SEP -6 PM 12:06

WV PURCHASING  
DIVISION

Signed: 

Michael Friedman  
VP Finance/Admin.

*7 Sept 2011*  
Date

Contact Person Concerning Quote:  
Michael Friedman, VP Finance and Admin..  
Phone: 571-299-4105 Fax: 571-299-4101  
mfriedman@tecsec.com



## Table of Contents

SECTION	PAGE
2.3 Attachment A: Vendor Response Sheet.....	3
2.3.1 Company Overview.....	3
2.3.2 Staff Qualification and Relevant Past Experience .....	4
2.3.3 References .....	8
2.3.4 Proposed Staffing Plan .....	8
2.3.5 Past Performance / Projects.....	9
2.4 Project Goals and Objectives .....	17
2.4.1 Identity Management.....	19
2.4.1.1 Governance: Policy and Overall Intent .....	19
2.4.1.2 Workflow Software .....	39
2.4.1.3 Equipment Recommendations.....	41
2.4.2 Attribute Management.....	43
2.4.2.1 On Card Authentication.....	43
2.5 Attachment B; Mandatory Requirements.....	45
2.5.1 Products and Services: General Services Administration (GSA) FIPS 201- Approved Products and Services List (APL).....	45
2.5.1.1 Enrollment Station.....	45
2.5.1.2 Issuance Station .....	48
2.5.2 Operational Execution: Practice.....	49
2.5.3 Products and Services: General Services Administration (GSA) FIPS 201 Approved Products & Services List (APL) and ANSI Standard criteria for attribute management.....	50
2.5.4 Validation Management .....	50
2.5.4.1 Validation is the Electronic Verification of the Identity and Attributes .....	50
2.5.4.2 Products and Services.....	50
2.5.5 Support .....	51
2.5.5.1 Installation and Training.....	51
2.5.5.2 Documentation and Multi-platform Topology .....	52
2.5.5.3 Reporting .....	52
2.5.5.4 Hardware and Software Maintenance .....	52
2.5.5.5 Reporting of Security Breaches.....	53
2.5.5.6 Cards.....	53
2.5.5.7 Data Storage Facility Agency-transmitted .....	53
3 Attachment C: Cost Sheet/Revised Under Separate Cover .....	64
4 Attachment D: West Virginia State –Wide Citizens Benefit Card (CBC) .....	65
5 Signed Addendums .....	76





## List of Figures

<b>FIGURE</b>	<b>PAGE</b>
Figure 1 SBIR – STTR Success Story .....	15
Figure 2 Armored Card Content .....	21
Figure 3 Population Density and DMV Locations .....	24
Figure 4 WV Identity Managed Service Offering at DMV Locations .....	25
Figure 5 Functions Performed At the Managed Service Central Site.....	30
Figure 6 Functional Diagram of TecSec’s Multi-Capability Card .....	33
Figure 7 WV CBC Hosting Multiple Applications .....	35
Figure 8 Identity Management Workflow Software .....	40
Figure 9 Armored Card Architecture Overview .....	68
Figure 10 Data Owners Linked to the Trusted Identity Platform .....	70
Figure 11 Using Data through the Trusted Identity Platform .....	71
Figure 12 Potential Annual Revenue from Attribute Container™ .....	72
Figure 13 Typical Card Program Allocation .....	73
Figure 14 Making Identity as a Service Affordable.....	74

## List of Tables

<b>TABLE</b>	<b>PAGE</b>
Table 1 Program Master Schedule .....	18
Table 2 DMV Kiosk Enrollment Throughput.....	26
Table 3-1 TecSec FIPS 140-2 Testing Certificates - Algorithms .....	55
Table 3-2 TecSec FIPS 140-2 Testing Certificates – Cryptographic Module .....	56
Table 3-3 TecSec FIPS 140-2 Testing Certificates - Hardware .....	56



## **2.3 Attachment A: Vendor Response Sheet**

### **2.3.1 Company Overview**

TecSec, founded in 1990, is a privately held small business located in Northern Virginia's technology corridor. TecSec's focus is on Information Security and Information Access Management, enforced through cryptography. TecSec provides software and hardware products based upon the company's 7<sup>th</sup> generation, standards-based Constructive Key Management (CKM<sup>®</sup>) technology, leveraging our large library of patents and still growing intellectual property.

TecSec provides:

- Federal Information Processing Standards (FIPS) certified smart card family
- Information Assurance products for networks, mobile devices, physical access, and desktop
- Information Management and Dynamic, Assured Information Sharing through cryptographically enforced Role Based Access Control (RBAC) and Attribute Based Access Control (ABAC)
- Integrated identity and enrollment hardware and software systems
- Support and services related to our information assurance products

Through a 21<sup>st</sup> Century key management system, designed especially for the world of large networks, TecSec's CKM<sup>®</sup> products bring privacy, confidentiality, and scalable management of content, independent of the means of transport or the type of information. Accordingly, CKM<sup>®</sup> technology has the potential to enhance the full range of likely digitized applications, including wireless, Critical Infrastructure Protection (CIP), and healthcare privacy enforcement. CKM<sup>®</sup> Enabled<sup>®</sup> solutions can be employed as software, firmware, hardware, or in a combination, including the TecSec Armored Card<sup>™</sup>. TecSec provides the Armored Card<sup>™</sup> which is the most recently enhanced version of the TecSec family of cards.

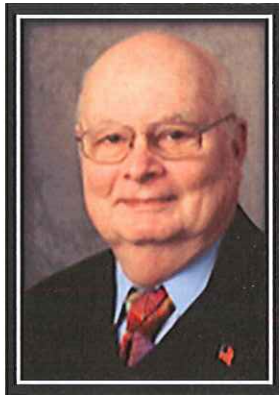
The TecSec card is an all American FIPS 201 certified and approved smart card with a starting memory size of 360K and separate processors for the contact and contactless operations, offering increased security. The enhanced version includes fast Secure Biometric Match on Card (SBMOC) and a secure multiple user, multiple application system that provides secure remote update capabilities, fine-grained secure memory allocation using the company's Secure Independently Licensed Object System, SILOS<sup>®</sup> Manager, and on-card CKM<sup>®</sup> capabilities.

TecSec has an unparalleled depth of experience in data security and the concept of information security (INFOSEC). Because of the nature of our cryptography business, TecSec's products have been certified by National Laboratories and evaluated by the nation's top security Agencies. National Standards (NIST, ANSI) have been written embracing our technology. What allows the TecSec Armored Card<sup>™</sup> to stand apart from other smart cards is the unique and powerful dynamic key technology provided by our CKM<sup>®</sup> product. All of this experience directly relates to TecSec's ability to provide an unequalled product and service to the State of West Virginia.





### 2.3.2 Staff Qualification and Relevant Past Experience

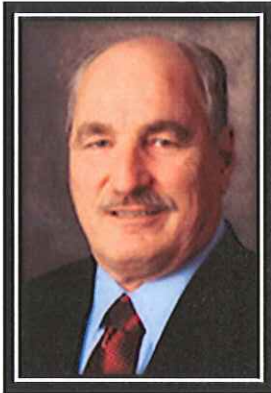


**Ed Scheidt – Founder and Chief Scientist**

Before founding TecSec in 1990, Ed held a variety of positions during his 26-year career at the US Central Intelligence Agency. Stemming from an operational background, Ed recognized the changing nature of communication patterns in America as PCs proliferated and were then formed into networks. In the early 1990's, Ed noted that encryption, which originated for primarily one-to-one communications, now faced new and substantially different key management requirements in large network or virtual network environments. ANSI X9.69, X9.93 and X9.73-2010 standards reflect this reality.

In forming TecSec and building the company's large IP library, he anticipated the flexibility and mobility required of 21<sup>st</sup> Century communication systems with a key management system that is primarily client-based and much less dependent upon a central server. The relative scalability achieved by this approach, together with encryption at the object level, provides enforced role based access (RBAC) and granularity not otherwise available, as well as attribute based access control (ABAC).

Ed remains deeply involved in the company's product development and expanding application solutions, just as he is in general management.



**Jay Wack - President and CEO**

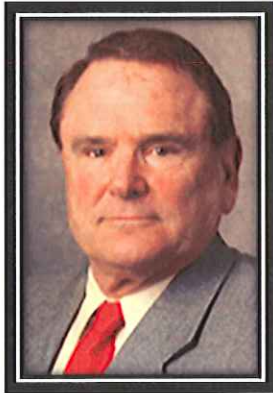
Jay began his career in electronics via the US Army in 1967, spent 18 months in Southeast Asia, and discharged in 1970. Upon his return he worked for Ampex as a field engineer while attending Montgomery College, studying Computer Science. Jay spent the next 20 years as an application engineer, specializing in microcontrollers and embedded microprocessors, representing Intel, National Semiconductor and serving the Mid-Atlantic Government market. Jay has been involved in the successful custom design of Application Specific Integrated Circuits (ASICs) as well.

In 1989, while addressing the data integrity issues on the Space Shuttle sensor network, Jay and Ed Scheidt were introduced and the two have been together as TecSec since then.

In 1995, Jay took an 18 month sabbatical from TecSec to work for the US Government as a technical advisor for Smart Card programs. During this time Jay worked on the Multi Access Reader Card (MARC) program. Contributing to the security specifications and acting in a technical support role based on his 20 prior years in the electronics industry.

Jay has been awarded over a dozen US patents in the areas of cryptography and security product design.





**Bruce Brotman – V.P. Strategy**

Bruce joined TecSec in September 2007 after having worked alongside of TecSec's President Jay Wack since 2005. At that time Bruce was Vice President for Strategic Planning at the National Biometric Security Project (NBSP) located in Morgantown, WV, a biometric testing facility.

Prior to joining NBSP he was a Senior Executive (SES) Federal Security Director at the Transportation Security Administration (TSA). There he oversaw the first complete federalization of a Category One airport (Louisville International Airport). In 2003 he was promoted to TSA HQ where he was the founding Director of the Credentialing Program Office.

Prior to his term at TSA, Bruce was the Chief Information Officer at the National White Collar Crime Center, located in Fairmont, WV. Here he provided a national support network for enforcement agencies, state regulatory bodies, state and local prosecution offices, and other organizations involved in the prevention, investigation, and prosecution of high-tech, economic crimes and terrorism.

Bruce retired from the FBI in Oct. 1998, at which time he was the (SES) Special Agent in charge of the FBI's external automation support to the worldwide law enforcement community. While in that position with the Criminal Justice Information Services Division (CJIS), he developed and executed the concept for the FBI's new Automated Fingerprint System, known as IAFIS. Bruce, whose early FBI background was related to the investigation of violent crimes, is the author of several publications relating to crisis management and aircraft piracy. He is the recipient of numerous awards from the Director of the FBI; various police agencies; and the FAA. He is the recipient of the "Vice President's Hammer Award" for significant contributions to the President's National performance Review Principles; the "Government Technology Leadership Award;" and the FBI's most coveted award, "The FBI Medal of Valor."

Bruce is also an attorney, commercial pilot and flight instructor. In addition, he is a member of the Board of Directors of the "Center for Security Policy", a member of the Advisory Board to Hewlett Packard – Federal, a member of the Fraternal Order of Police, The International Chiefs of Police, the Florida Bar Association and the Phi Delta Phi International Legal Fraternity. Bruce holds TS/ISSA security clearances.





### **Michael Friedman – VP Finance & Administration**

Michael S. Friedman joined TecSec in 2007 as its General Counsel and Chief Financial Officer. Mike has over 30 years' experience in senior management including both public and private companies. Beginning with his service in the United States Air Force General Counsel's Office, where he was counsel to the Air Force Office of Special Investigations, Mike has provided advice and counsel to some of the country's most significant companies concerning risk mitigation and compliance. Mike was the Chief Operating Officer of a company advising the UN and the US Security Coordinator on issues related to border crossings from the West Bank and Gaza to Israel. Mike served as the Vice President and General Counsel of Abraxas Corporation which supports the US intelligence community. He also served as the Special Assistant to the Director of the Office of Safety Act Implementation within the Science and Technology Directorate of the Department of Homeland Security, where he was responsible for the development of the risk mitigation program for companies with emerging anti-terrorism technologies. Mike holds TS/ISSA security clearances.

### **Ron Lang – VP Programs**

Ron joined TecSec in 2007. He is a retired naval line officer with 29 years of active service in both operational and systems acquisition management positions. Ron has been the Director of Engineering of the Sparrow missile (AIM/RIM7), the logistics manager (APML) of the F14 fighter aircraft, member of the Operational Test and Development Force (OPTEVFOR), including numerous at sea and command positions in fighter squadrons and aircraft carriers. He was a professor of Engineering Management at the Defense Systems Management College (now the Defense Acquisition University) where he chaired the Systems Engineering Management Department including the Systems Engineering Management Course, certifying Department of Defense level 3 engineers. In his last assignment in the Navy he was on loan to the FBI as program manager of the FBI's national computer network known as NCIC. In that position he managed the technical update of NCIC 2000, incorporating the latest computer technology and biometrics into that important national law enforcement program. Ron has also held a business development position with Northrop Grumman Corporation where he developed business strategy for aircraft support and services as well as homeland security programs.

### **Ron Parsons – VP Integrated Solutions & Services**

Ron Parsons joined TecSec in 2005. He oversees the development, deployment, and support of software solutions; including the integration of Constructive Key Management (CKM<sup>®</sup>) technology into existing customer applications as well as focusing attention on new markets. Ron founded and ran two quick reaction electronic and software design companies over a twenty year period; servicing commercial, civilian, and Department of Defense (DoD) customers across the country. He also served as an Associate Director at NIST (National Institute of Standards & Technology) before assisting in the launch of several organizations focused on electronic commerce, identity management, and information security. Ron served as the Director of the Federal Sector for CommerceNet, was founding co-chairman of FiXS (Federation for Identity and Cross Credentialing Services), and founding co-chairman of FEGC (Federated Electronic Government Coalition).





### **2.3.3 References**

References are provided in the Past Performance Section of this proposal, with regard to specific projects.

### **2.3.4 Proposed Staffing Plan**

TecSec principal staff for this Managed Service program will be a Program Manager, an Assistant Program Manager, and a Technical Staff Assistant. Additional TecSec staff will be utilized as necessary. TecSec's office will be located at 874 Fairmont Road, Suite F, Morgantown, WV 26501. TecSec will provide a fully conforming Data Center at its WV address and a Backup Data Center in Northern Virginia. The Help Desk will also be managed from the WV facility. Technical and Logistics support will be provided from TecSec's corporate facility located at 12950 Worldgate Drive, Herndon, VA. 20170. In addition, TecSec has a support network of hardware and software vendors who provide support for the products and services that are incorporated into the TecSec product lines. TecSec is very confident that its professional team can resolve any program or technical issue in a rapid and satisfactory fashion. The TecSec Program Manager (PM) and senior executives will be present at the Orals/Demonstration to discuss further any staffing questions.



### 2.3.5 Past Performance / Projects

#### **Project: United States Postal Service**

**Location:** 475 L'Enfant Plaza SW, Room 6921, Washington, DC 20260-6921

**Project Manager and Contact Info:** Steven N. Benson, Manager, Delivery and Retail  
Business Systems (202-268-4614)

**Type of Project:** State One Card Identification Program Initiative (Phase I). Project provided Technical Assistance and Advisory Services to the USPS for Phase I, Applied Research and Development.

#### **Goals and Objectives and How They Were Met:**

The Key Objectives of the Project were to demonstrate a fully functional proof of concept system that could be used to analyze the scalability, business models, and engineering parameters of a secure, standalone enrollment and identity management system, complete with PIV certified cards and infrastructure for use in Citizen's Benefit Card (CBC) programs of the type proposed in Attachment D to this proposal.

*Scope and Complexity of the Efforts:* Demonstration of an end to end system design, software development, and enrollment hardware manufacture. The TecSec delivered demonstration was a functionally complete system.

*How the Customer Benefited Operationally or Strategically:* The customer was able to determine the technical viability, validate the potential revenue flow and future implementation costs in order to determine the value of a potential USPS revenue generating program that had both State and National implementation.

*Description of Other Aspects of the Project to Demonstrate its Relevance:* The project included end to end data integrity and security, communication with external data repositories, and the issuance and use of biometric enabled PIV cards for multiple diverse functions including, governmental functions, private commercial transactions, and electronic filing of health care documents while providing protection of private information through the use of standards based cryptographic key management.

*Description of the Team Member's Role in the Project and the Challenges and Lessons Learned from the Experience as the Prime or Subcontractor:* TecSec's role in this project included design, development, and production of the demonstration system and support of the customer in evaluation of system performance.

*The challenges and lessons learned included:* Demonstration of an end to end technical solution that solves the national technical challenge of universal security of all types of digital data while providing an economic business case for state and national use. Additional challenges included providing an affordable and easily generated biometric based Identity of Merit.

*Description of the Integration of Resources (e.g. Personnel, Tools, Applications, etc.) into the Customer's Environment:* The project involved close coordination with senior management, program management, and technical leads of the customer. It involved PIV technologies, secure





WEB interfaces, .NET implementations, and demonstration of the potential for linkage into the customers Lightweight Directory Access Protocol LDAP systems.

*The use of Creative and Innovative Solutions in Achieving or Exceeding Customer Objectives:* Through the use of Role Based Dynamic Key technologies, we were able to demonstrate a scalable end to end solution in a very short time with minimal impact on existing systems.

*System Design, Development, Implementation, and Integration:* TecSec designed and produced a complete end to end hardware system including a stand-alone enrollment system, multiple demonstration kiosks and stations integrated with the TecSec PIV, including secure on-card Biometric Matching (SBMOC) to validate individual identity.

*Software Design and Development:* TecSec designed and produced a technology demonstration system of TecSec products focused on its certified biometric based identification card platform (Eagle Card) combined with cryptography (CKM<sup>®</sup>) and attribute containers packaged as a USPS administered program.

**Project: US Investigations Services**

**Location:** 1137 Branchton Rd, Annandale, PA 16018

**Project Manager and Contact Info:** Stephen Heard, Project Manager

**Type of Project / Goals and Objectives / How They Were Met:**

TecSec developed, integrated, and delivered a demonstration system for the purposes of protecting, compartmentalizing, and sharing sensitive background information. The work included the development and delivery of multiple training modules to a cross section of the corporate staff. On this program, TecSec supplied security system design support, software development support, documentation development, and training.



**Project: Intermec**

**Location:** Ft. Belvoir, Virginia

**Project Manager and Contact Info:** Ron Teeters, Program Manager  
28707 Gilchrist Dr., Willowick, OH 44095  
Ron.Teeters@intermec.com

**Type of Project / Goals and Objectives / How They Were Met:**

TecSec developed, integrated, and delivered a complete suite of middleware that enabled secure communication with smart cards from multiple manufacturers across a diverse product line of hand held devices. The work included the modification and delivery of a comprehensive Software Development Kit (SDK) to allow for future expansion and updates. The interfaces that TecSec designed and delivered have been deployed on thousands of handheld devices in military and civilian applications

**Project: BAE Systems**

**Location:** Reston, VA

**Project Manager and Contact Info:** Albert Dunn;  
11487 Sunset Hills Rd, Reston, VA 20190;  
Phone: 703-668-4268

**Type of Project / Goals and Objectives / How They Were Met:**

TecSec delivered two integrated solutions to BAE Systems. The first system was utilized for the protection and sharing of sensitive information by the Department of Homeland Security among a diverse and geographically distributed team. The second system allowed for protection of information on servers and during communication between secure locations. On these efforts, TecSec supplied security architecture, security system design support, software development, system integration, documentation development, online customer support, and training.

**Project: Motorola Corporation**

**Location:** Schaumburg, IL

**Project Manager and Contact Info:** Neerja Bylsma;  
1303 E. Arlington Road,  
Schaumburg, IL 60196  
neerja.bylsma@motorla.com

**Type of Project / Goals and Objectives / How They Were Met:**

TecSec developed, integrated, and delivered a suite of security products for Information Assurance that included server, desktop, and mobile applications. The work also included the





modification and delivery of a complete Software Development Kit (SDK). On this program TecSec provided the System software development, security architecture analysis, security software development, and documentation support to assist the customer in their strategic planning and tactical implementation of role based information assurance.

**Project: Boeing 777 Aircraft Project**

**Location:** El Segundo, CA

**Project Manager and Contact Info:** George Mullner

**Type of Project / Goals and Objectives / How They Were Met:**

Boeing Corporation integrated CKM<sup>®</sup> into its document management software for the building of the Boeing 777 Aircraft. This was done to address 2 points:

- Use of CKM<sup>®</sup> satisfied the International Trade and Arms Regulations (ITAR)
- Use of CKM<sup>®</sup> supported secure sharing of a single document/drawing with each of many recipients (suppliers, vendors, partners) seeing only the part of the document appropriate to their needs.

**Project: Boeing Digital Cinema Project**

**Location:** Hollywood, CA

**Project Manager and Contact Info:** Ishmael (Izzy) Rodriguez  
719-638-5046

**Type of Project / Goals and Objectives / How They Were Met:**

TecSec provided role based access control (RBAC) to distribute digital content through the supply chain. TecSec encrypted 16 movies, including Star Wars Attack of the Clones, so that the digital content navigated from the movie producer to the movie projector and the content was encrypted from end to end. This capability allowed for the digital distribution and avoidance of the cost of physically moving celluloid. The project ended when Boeing abandoned this line of business.



**Project: HSARPA SBIR 1 & 2**

**Location:** Fort Huachuca, AZ

**Project Manager and Contact Info:** Peter Miller/John D. Hoyt; DHS, HSARPA,  
245 Murray Lane, Bldg 410, Washington, DC 20528;  
Phone: 202-254-6144

**Type of Project / Goals and Objectives / How They Were Met:**

The Supervisory Control and Data Acquisition (SCADA) is a critical infrastructure system that is subject to attack. The utility industry increasingly is relying upon SCADA Energy Management System (EMS) and Distributed Control System (DCS) in the performance of utility operations. In general, these SCADA and EMS/DCS resources were originally designed with security that does not keep pace with the malice present in the operational environment. This has opened up system vulnerability to cyber intrusion, and other attacks. These attacks either physical or virtual can directly challenge equipment design and safety limits, causing system malfunctions and/or catastrophic shutdowns.

TecSec's CKM<sup>®</sup> was approved to provide the ability for a role-based access control (RBAC) to any digital object in the Critical Infrastructure Protection (CIP). The design called for CKM<sup>®</sup> to be instantiated as a comprehensive key management solution i.e., Secure Cryptographic Management System (SCMS) in a modular componentized architecture to meet the security needs of the utility industry.

Under Phase 1 of the Small Business Innovative Research (SBIR) contract, TecSec developed a prototype design of a SCMS for the SCADA DCS. Within Phase 2, the SCMS effort focused on the following:

- Prototype of the SCMS by integrating CKM<sup>®</sup> into General Electric's XA21 Control Master Software.
- Extend and expand the SCMS functionality beyond the basic RBAC by incorporating the Defense in Depth (DID) security concepts.
- Analyze and validate the security robustness of CKM<sup>®</sup> technology.
- Design an EMS architecture to accommodate Internet Protocol (IP)-based network where its perimeter is ill defined.
- Address the commercialization aspect of CKM<sup>®</sup> security solution adaptation.





**Project: Joint Warrior Interoperability Demonstration**

**Location:** Australia, Canada, NSWC Dahlgren, ESC Hanscom AFB, New Zealand, SPAWAR San Diego

**Project Manager and Contact Info:** Richard Fastring  
SPAWAR, San Diego, CA

**Type of Project / Goals and Objectives / How They Were Met:**

TecSec participated in the Joint Warrior Interoperability Demonstration (JWID) as a security component of the Defense Collaborative Tool Set (DCTS) program, providing data separation and role based access control authorization. TecSec's role was to provide technology that satisfied the following requirements:

- Support the CIT01.06 Role Based Security for Coalition Interoperability Trials (CIT)
- Provide differential access to Microsoft® Word files
- Provide differential access to other files
- Demonstrate different levels of access

The technology was deployed and exercised during JWID in Australia, Canada, NSWC Dahlgren, ESC Hanscom AFB, New Zealand, and SPAWAR San Diego.

For more detailed information regarding the JWID operation see the following except from the DoD SBIR Success Stories Book.



State of West Virginia  
RFQ No. HSE01154  
Identity Management Service Offering



## Department Of The Navy Success Stories SBIR/STTR





**DRM Binding With CKM**

**TecSec DRM**

**About the Technology**

In an effort to develop a highly trusted, secure workstation with encryption TecSec, Inc. developed a cryptography key management system called Constructive Key Management® (CKM®). Server based encrypted systems limited the networks' ability to achieve the growing need for scalability and operating efficiency. TecSec's cryptographic technology also provides end-to-end security that can now include a hard token where CKM is embedded in integrated circuits in smart cards.

The CKM Enabled® Smart Card carries RFID and logical access to PCs, functioning as a federating device, permitting ID Management for controlled access among various applications. The cardholder gains a mobile ID device, where permissions vary depending upon one's role and/or location. Keys are created on the fly and not stored. Different access permissions are assigned to objects as determined by the message originator, consistent with need to know and information sharing policy. Otherwise, only the enterprise owner can recreate keys. Information is highly granular and managed at the object level. Laptop content protection is one selected military application of CKM. Homeland Security (DHS) Advanced Research supports TecSec's Cyber Security solution in the nation's power grid, a HSPD 7 Critical Infrastructure solution. Treasury Department and the Center for Medicare/Medicaid Services employ CKM for laptop and workstation protection. This early Navy work has since been subsumed in the Net Centricity orientation of current Joint Global Information Grid (JGIG) programs.

**Military and Commercial Significance**

TecSec's object management greatly expands the functionality of encryption through enforcement of information rights management. CKM provides a range of solutions, safeguards information, and selectively shares data within or outside of an organization. TECSEC's reduced role for the server and heightened functionality at the workstation has brought a paradigm shift that provides role based access, at the object level, to anything digital that can be named, be it physical, logical, or functional.

**SPAWAR**

**TECSEC INCORPORATED**

ANTENNA INVESTIGATE TECHNIQUES TO  
DEVELOP HIGHLY TRUSTED SECURITY  
FEATURES FOR WORKSTATIONS

46

Topic Number: N91-057  
(SPAWAR)

SBIR Investment: \$79.5K  
Project Revenue: \$23.05M

**TecSec Incorporated**

1953 Oakleaf Road  
Vienna, VA 22182  
(703) 744-5444  
www.tecsec.com  
John Petty  
johnpetty@tecsec.com

**APPLICATIONS**

- DoD: Iraq - Biometrics recording and verification
- Joint Battle Center Lab - Coalition Information Sharing
- Joint Warrior Interoperability Demonstrations of Interface Applications
- Joint Emergency Management Framework
- SOCM/USAFAC: Operational & Coalition Forces Communication
- National Counter Terrorism Center - Multiple forms security on a common platform

**About the Company**

TecSec is a standards-based product and solutions company, which focuses on data management and information privacy and confidentiality. TecSec develops and sells information assurance through a cryptographic approach that enforces management's rules and standards of conduct. TecSec has greatly expanded the applications of cryptographic through its basic characteristics, assisted by a highly sophisticated key management system. The product life cycle of a new generation of cryptography and key management system requires protracted periods of development and testing. The SBIR program has been most helpful in this dedicated and lengthy process.

Figure 1 SBIR – STTR Success Story

### Project: STTR Contract on Information Centric Security with the Office of Naval Research (ONR)

Location: Arlington, VA

Project Manager and Contact Info: John Williams (ONR) [Williajr@onr.navy.mil](mailto:Williajr@onr.navy.mil)  
703-696-0342

#### Type of Project / Goals and Objectives / How They Were Met:

This Small Business Technology Transfer (STTR) Phase I addressed attacks from an insider threat. The need exists where the data-at-rest would have to be compartmentalized so that only those roles allowed access, based on adequate security level and need to know, would have the appropriate permissions required to access the information. The working model demonstrated a combination client and server version based on ANSI X9.69 for a representative operational environment. The information centric security system was intended to meet the following





categorized objectives: access control, key management, data protection, interoperability, audit trail and logging, system misuse and damage assessment, as well as various modes of operation.

**Project: CKM® Workstation Contract with SPAWAR**

**Location:** San Diego, CA

**Project Manager and Contact Info:** Paul Adams 619-553-3422  
or Cheryl Bowman 619-553-3429

**Type of Project / Goals and Objectives / How They Were Met:**

CKM® Workstation was developed to monitor CKM® activities on a Space and Warfare Command (SPAWAR) Local Area Network (LAN). Monitored activities included:

- Encryption
- Decryption
- Cut and paste operations
- Printing
- User logon information

This monitored information was audited and stored encrypted on the workstation. Periodically, the security workstation polled the workstations for the information.

The workstations on the LAN were CKM Enabled®. The audit file was encrypted and inaccessible by the workstation user. The security workstation was CKM® Enabled.

**Project: Contract on Secure Telephone Unit with White House Communications Agency (WHCA), AT&T, Rockwell-Collins**

**Location:** Washington, DC

**Project Manager and Contact Info:** Not Available

**Type of Project / Goals and Objectives / How They Were Met:**

TecSec, as the 'Small Business of the Year' for Rockwell, developed a tempest compliant "Mobile STU III", a highly secure cellular telecommunications device, known as the Travel STU Briefcase, which was designed to secure all manners of communications over cellular and landline transmission systems. TecSec further developed a new satellite communication unit for secure communications anywhere in the world via the INMARSAT-M satellite network, known as SECSAT Secure Satellite Communication Terminal. The SECSAT has been designed, tested, and certified for compliance with the National Security Telecommunications and Information Systems Security Advisory Memorandum (NSTISSM) Tempest/I-92, which supersedes NACSIM 5100A.



## 2.4 Project Goals and Objectives

TecSec intends to provide the State of West Virginia's Division of Homeland Security and Emergency Management an Identity Management Service that fully conforms to the goals and specifications defined in HSE01154. As a manufacturer of certified personal identification products and state of the art cryptographic data protection devices, TecSec has designed and tested products that meet or exceed West Virginia's requirements. As part of this proposal TecSec will demonstrate to the Department of Homeland Security the required performance and the extensive overall system capability. This demonstration will provide the State of West Virginia complete confidence in TecSec's ability to meet their short and long term goals. In addition, TecSec wants the State to recognize our desire to assist the State of West Virginia to become the unquestioned National Leader in personal identification.

Table 1 is an overall Program Schedule commencing upon contract award.





State of West Virginia  
RFQ No. HSE01154  
Identity Management Service Offering



ID	Task Name	Duration	Start	Finish
1	Program Kick-off	16 days	Mon 10/3/11	Mon 10/24/11
2	ARO	0 days	Mon 10/3/11	Mon 10/3/11
3	Kick-off Meeting	0 days	Mon 10/10/11	Mon 10/10/11
4	Tech Policy & Card Design	0 days	Mon 10/17/11	Mon 10/17/11
5	Final Site Selection	0 days	Mon 10/24/11	Mon 10/24/11
6	Monthly Status Reports	241 days	Thu 10/13/11	Thu 9/13/12
20	Enrollee Attribute Data	95 days	Mon 10/17/11	Mon 2/27/12
21	Attribute Data Determination	0 days	Mon 10/17/11	Mon 10/17/11
22	Attribute Data Collection Template	15 days	Tue 11/1/11	Mon 11/21/11
23	State Collection Initiative	60 days	Tue 11/22/11	Mon 2/13/12
24	Provide Data to TecSec	0 days	Mon 2/13/12	Mon 2/13/12
25	Load Adjudication DataBase & Integrate	10 days	Tue 2/14/12	Mon 2/27/12
26	DMV Enrollment Stations	149 days	Tue 11/15/11	Fri 6/8/12
27	Installation	49 days	Tue 11/15/11	Fri 1/20/12
28	Site Survey	5 days	Tue 11/15/11	Mon 11/21/11
29	Site Preparation	20 days	Tue 11/22/11	Mon 12/19/11
30	Kiosk Delivery & Prep	5 days	Mon 12/26/11	Fri 12/30/11
31	Kiosk Installation	5 days	Mon 1/2/12	Fri 1/6/12
32	Central Site Installation	10 days	Mon 1/2/12	Fri 1/13/12
33	System Test	5 days	Mon 1/16/12	Fri 1/20/12
34	System Sign-off	0 days	Fri 1/20/12	Fri 1/20/12
35	Training	5 days	Mon 1/23/12	Fri 1/27/12
36	DMV On-Site Training	2 days	Mon 1/23/12	Tue 1/24/12
37	DMV On-the-Job Oversight	3 days	Wed 1/25/12	Fri 1/27/12
38	Enrollment	90 days	Wed 1/25/12	Tue 5/29/12
39	Enrollee Adjudication by WV State	90 days	Mon 1/30/12	Fri 6/1/12
40	Card Issuance	90 days	Mon 2/6/12	Fri 6/8/12
41	5,000 Armored Card Users	0 days	Fri 6/8/12	Fri 6/8/12

Table 1 Program Master Schedule



## **2.4.1 Identity Management**

### **2.4.1.1 Governance: Policy and Overall Intent**

#### **A. Produce Identity Management System**

*Produce an Identity Management System that establishes a unique identity in accordance with Federal and other standards defining a high level of assurance and that will implement 2 and 3 factor authentication, encryption and digital signature functionality.*

The above requirement will be fully demonstrated as an end to end system in West Virginia at the Orals/Demonstration Event. TecSec, a standards-based solutions provider, will enable the State of West Virginia to not only address its current requirements, but also provides a solution that will 'grow' with the State's ever-changing needs and position the State to handle those future technical demands with regards to identity, security, and fraud reduction and reap the benefits of the related cost savings.

TecSec subscribes to the principle of developing products that fully comply with national and international technical standards. By so doing, TecSec maximizes product interoperability, enables seamless integration, and enhances system scalability. In the standards-based requirements sub-section, there are standards called out that refer to TecSec concepts which are further defined by the ANSI dynamic key management community defining a high level of assurance for the unique identity being developed. The called out standards are becoming more critical as the perimeters of networks are becoming more blurred, demanding that the data itself be persistently protected. This need for data level protection is also true for mobile and wireless communications. Subsequent sections summarize the certifications of the hardware, software, firmware, and algorithms, as well as NIST-sponsored Secure Biometrics Match-on-Card (SBMOC) testing associated with the TecSec Armored Card™, also known as the "Citizen's Benefit Card," (a name coined by West Virginia during one of TecSec's earlier meetings with cabinet level personnel).

TecSec developed a federated smart token, the Armored Card™, which includes capabilities for personal identity and associated with attributes/roles. It also contains all of the required elements for PIV-I including identity, certificates, digital signature and etc. On the Armored Card™, CKM® encryption is used for; differential access to content, logical and physical access control, and confidentiality.

Other capabilities of the federated Armored Card™ include a secure biometric match-on-card within a contact physical format (International Standards Organization [ISO] 7816), as well as contactless (ISO 14443) mode, Public Key Infrastructure (PKI) support, Constructive Key Management (CKM®) support, and a contact modality for external application interface and support.

Additionally, the TecSec solution implements 2 and 3 factor authentication through the following:





- Armored Card™ (something you have)
- Personal Identification Number (PIN) (something you know)
- Fingerprint Biometric (something you are)
  - Facial and Iris are also available

In summary, the technologies associated with a smart card can now be viewed as an Armored Card™ with capabilities providing a high assurance that:

- A personal unique identity can be established, and once that identity is confirmed using 2 and 3 factor identification;
- Access to data and services associated with an individual's attribute(s)/permission(s)/role(s) can be confirmed, and finally;
- Separate secure encrypted Attribute Containers™ can be created on the Armored Card™ to ensure business equality is maintained among different applications that are promoting business objectives.

In 2005, TecSec understood that its patented cryptographic products combined with a robust identity of merit (Armored Card™) fully met the needs and objectives of HSPD-12 and the Real ID Act. In addition, the TecSec approach far exceeds the Real ID Act requirements by allowing the use of the Armored Card™ to securely address local, state, and federal program needs plus access to an unlimited commercial marketplace. The TecSec secure biometric match on card feature, utilizing secure data compartmented on the card to prevent unauthorized access, becomes the essential foundation of electronic storage and transfer of information for government and business use as further elaborated in the business plan section of this proposal (Attachment D). **Uniquely, the expanded capability of the TecSec Armored Card™ permits a positive cash flow to the State.** No other card on the market today or envisioned for the near future has the technology or the robustness to match the Armored Card™.

TecSec has designed and independently certified under FIPS 140-2 and FIPS 201 a smart card (Figure 2) which has the following unique characteristics:

- Dual Chip; Contact and Contactless (no antennae is attached to the main memory, therefore, cannot be skimmed vs. other cards with a single chip)
- Large capacity chips have a base memory of 368 Kilobytes (288 contact / 80 contactless), expandable up to 8 Megs vs. other cards with small limited space chips
- Memory segmented into independent secure attribute containers (vs. other cards without the capability)
- 50 MHz processor (verses other cards with slow less capable processors)
- Secure Biometric (fingerprint) MATCH ON CARD (ANSI 378) can use other biometrics e.g. Iris/Face (vs. other cards that do biometric match on reader/server that create security issues)
- CKM® cryptography ensures the security of data so the loss of the card will not mean the loss of data (vs. other cards that are not encrypted)



- True Multi-Owner/Multi-Function capability (verses single use or complex single owner cards that do not have the ability to house secure independent attribute containers)
- Single Threaded technology with RAM flush between attribute container usage to prevent any object reuse or subsequent application access to spillage or left over data.
- Standards based:
  - Fully tested and certified FIPS 140-2 level 3
  - NIST 800-73-3
  - FIPS 201
  - ANSI X9.73-2010 cryptographic message syntax ASN-1 and XML
  - ANSI X9.69 Framework for Key Management Extensions – CKM<sup>®</sup>
  - ANSI X9.96 Secure XML
  - ANSI X9.112 Secure Wireless
  - ANSI 385
  - ANSI 378
- All American Sourced
- It is a PIV and PIV-I card enhanced with CKM<sup>®</sup>
- On the GSA Approved Product List (APL) #424 for HSPD-12

## Armored Card Contents

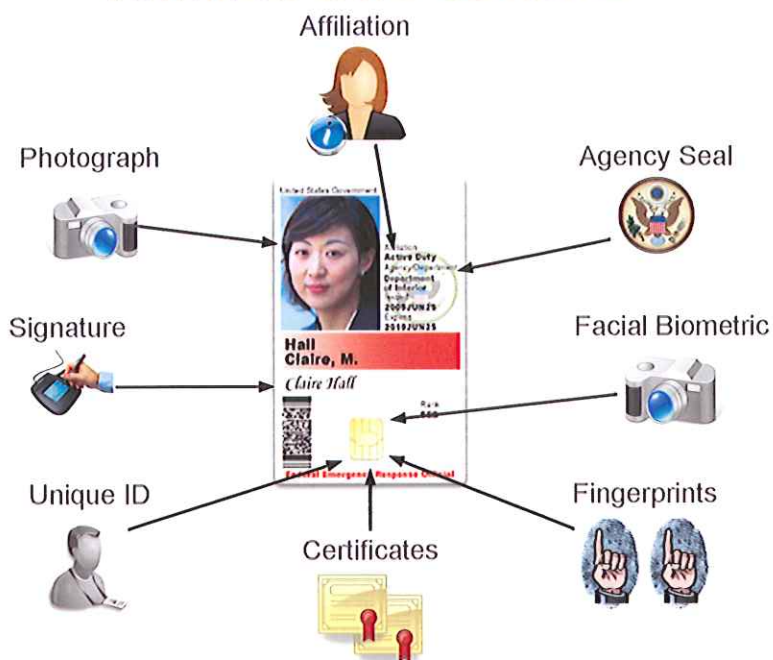


Figure 2 Armored Card Content





State of West Virginia  
RFQ No. HSE01154  
Identity Management Service Offering



In summary, the TecSec Armored Card™ approach is unique and is:

- The only all American sourced product on the GSA Approved Products List
- The only dual chip configuration through testing -- 7816 contact and separate 14443 contact less chips
- The only card solution supporting 368k (288/80) bytes of EPROM; with expansion to 8 megs-- others are offering 72 and 128 k of EPROM
- The only solution that supports multiple, cryptographically unique, hardware fire walled Attribute Containers™. The SILOS® Manager allows the creation of Attribute Containers™ each Container to be a separate application or data store, with hardware and cryptography to assure no overlap or access from one to another. Issuer cannot read any Container other than their own.
- The only American secure biometric match on card tested and passed by NIST for both contact and contactless operation in under 1 second with 1/10,000 accuracy
- The Armored Card™ has been tested for FIPS 140-2 and FIPS 201 by InfoGuard and the physical certification for the card body construction by Exponent Laboratory, both meeting the specifications for the Government Common Access Card (CAC).

CKM® has been reviewed for cryptographic accuracy and conformance through a FIPS 140-2 evaluation. A copy of the certificates can be found at end of this section. In addition, the following algorithms have been tested and certified under FIPS 140-2.

FIPS-approved algorithms: AES (Certs. #345 and #379); Triple-DES (Certs. #407 and #422); SHS (Certs. #420 and #450); HMAC (Certs. #149 and #167); RNG (Certs. #165 and #181); RSA (Certs. #116 and #131); DSA (Certs. #155, #163, and #165).



## **A.1. Baseline Implementation**

### **Enrollment System Metrics**

Program requirement: 5,000 person enrollment and issuance for WV Homeland Security needs.

Managed Service: Central site to compile and store encrypted personal information and biometric data.



In designing its implementation program, TecSec balanced overall cost against inconvenience to the enrollees. The result of that assessment is a decision to establish three enrollment centers within West Virginia, each located at a DMV within the most populated areas of the State. The locations selected recognize the population centers and minimize travel distances and times for enrollees living in less populated areas of the State. Given that each enrollment center has the capability to enroll in excess of 2000 people per month (See Table 2 on page 26) and the initial target enrollment is only 5000, it is simply not cost effective or efficient to establish additional enrollment centers; however, the TecSec system has been designed to easily and seamlessly expand the number of enrollment centers as the program grows. TecSec believes the selected locations will provide the State's leadership with a conveniently located yet sufficiently distributed system to both showcase and demonstrate to future business case organizations the value of the system and provide initial service to the entirety of the State.

TecSec proposes the initial enrollment centers be established at:

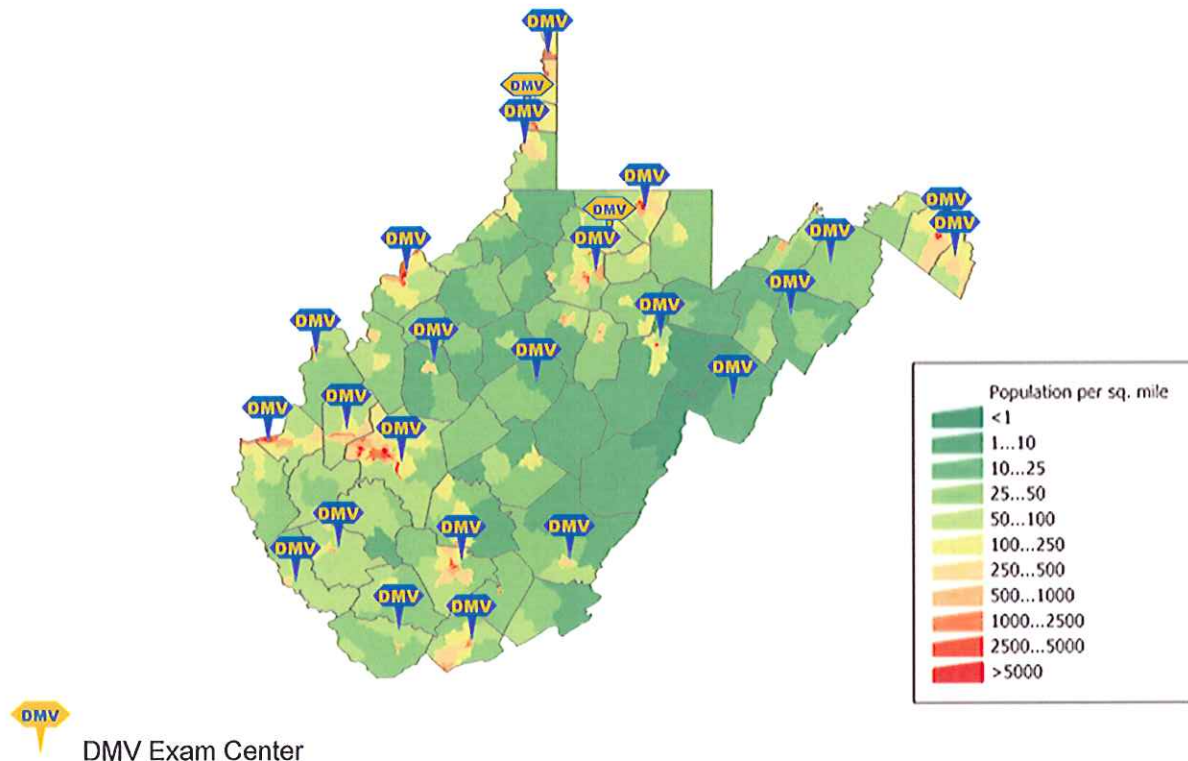
- Kanawha DMV, 5707 MacCorkle Ave SE, Suite 400, Charleston, WV 25317
- Morgantown DMV, 1525 Deckers Creek Blvd, Morgantown, WV 26505
- Martinsburg DMV, 1438 Edwin Miller Boulevard, Martinsburg, WV 25404







State of West Virginia  
RFQ No. HSE01154  
Identity Management Service Offering



**Figure 3 Population Density and DMV Locations**

Figure 4 (below) highlights the functions that will be performed at the three selected DMV sites. They include applicant enrollment, smart card printing, card activation and issuance.



# West Virginia: Identity Management Services Offering Department Of Motor Vehicles Location

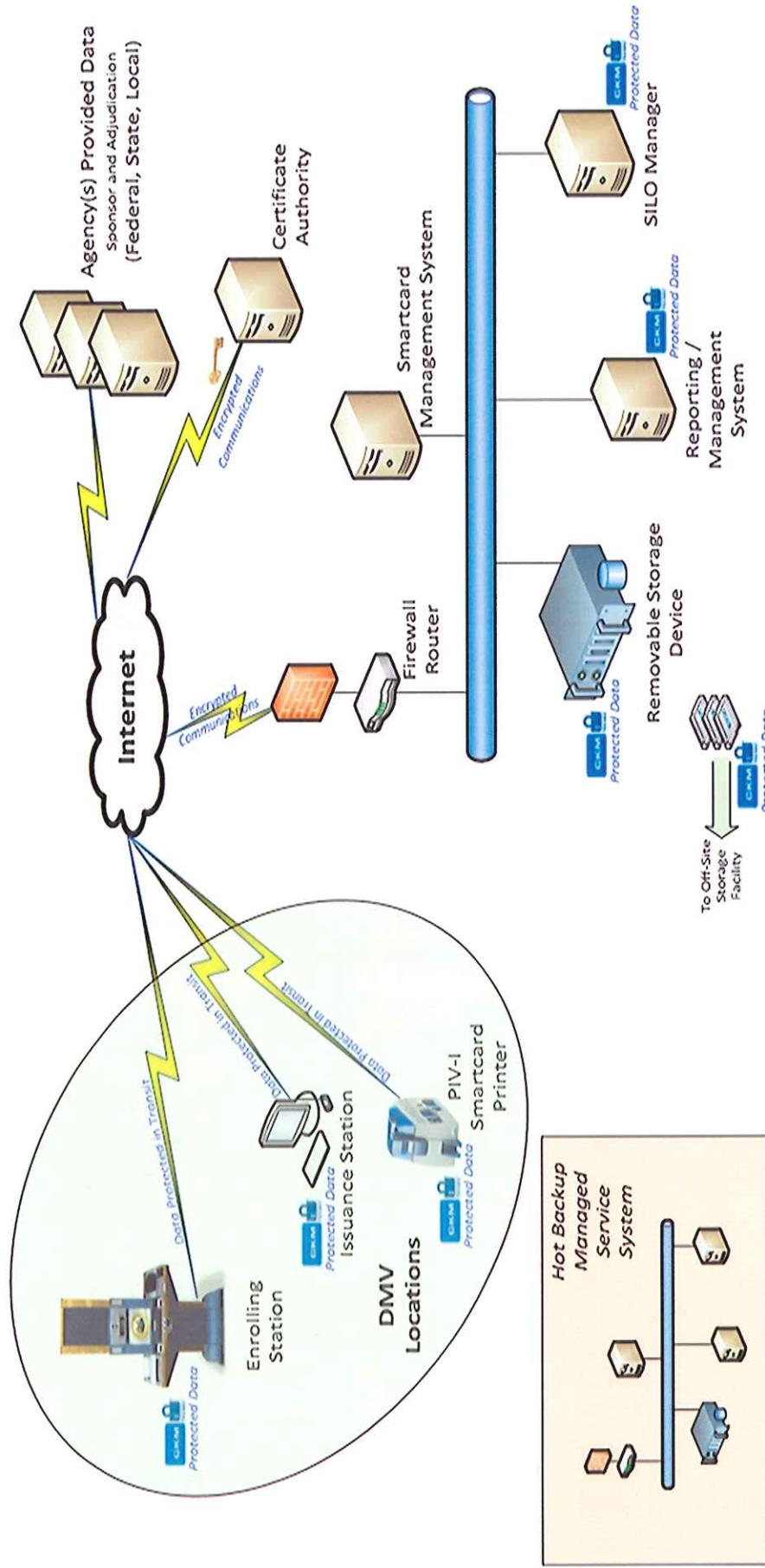


Figure 4 WV Identity Managed Service Offering at DMV Locations



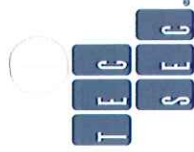


Table 2 DMV Kiosk Enrollment Throughput

## DMV KIOSK ENROLLMENT THROUGHPUT

PARAMETERS AND CALCULATIONS	
Number of DMV Site Kiosks	3
Weekday Days	5
Weekend Days	0.1
Weekday Hours	8
Weekend Hours	1
Weekly Hours - total	40
Weeks/year	52
Annual Hours	6,252
Total Fed Holidays	10
State Holiday Hours	80
Weather Closure (Hrs/Yr)	40
Annual Work Hours - Total	6,132
Users Enrolled per Hour	4
Users Enrolled per Year	24,528
Users Enrolled per Month	2,044
Months to Enroll 5000	2.5

ANNUAL HOLIDAY SCHEDULE	
Monday, January 2*	New Year's Day
Monday, January 16	Martin Luther King, Jr.
Monday, February 20**	Washington's Birthday
Monday, May 28	Memorial Day
Wednesday, July 4	Independence Day
Monday, September 3	Labor Day
Monday, October 8	Columbus Day
Monday, November 12***	Veterans Day
Thursday, November 22	Thanksgiving Day
Tuesday, December 25	Christmas Day

**CHARLESTON DMV OFFICE HOURS:**  
Monday to Friday: 8:00 am - 6:00 pm  
Saturday: 8:00 am - 12:00 pm

**CHARLES TOWN DMV OFFICE HOURS:**  
Monday to Friday: 8:30 am - 5:00 pm

**MORGANTOWN DMV OFFICE HOURS:**  
Monday to Friday: 8:30 am - 5:00 pm



## **A.2 TecSec Enrollment System**

### **A.2.1 Enrollment Kiosk**

The TecSec Enrollment System incorporates a self-contained biometric enrollment kiosk, a portal for data consolidation and an effective chain of trust from the capture point through distribution to the subscribing agency. The TecSec enrollment system:

- Captures linked biographical identity information stored on a card or a remote database and provides the ability to confirm or update identity information;
- Captures facial image, fingerprints, iris and signature biometrics and confirms that the captured images comply with applicable quality criteria and standards;
- Immediately encrypts all personally identifiable information (PII) captured during enrollment with CKM<sup>®</sup>
- Capture and automatic validity checking of all required breeder documents regardless of any physical format (cards, passport, letter and legal size documents), contact and contactless smart cards data and other documents suitable for scanning. Process also includes automatic validity checking of breeder documents to ensure authenticity;
- Transfers encrypted transaction information from the kiosk to a secure portal through a very robust chain of trust mechanism and once receipt is confirmed enrollment transaction data on the kiosk is deleted. No PII is ever stored locally on the kiosk;
- Provides a complete chain of trust from the point of capture of personal information through delivery to the subscribing agency using CKM<sup>®</sup> technology.



The TecSec Multi-Biometric Enrollment Kiosk is purpose built to:

- Operate in either a self-service, operator supervised, or remote operator supervised mode with simple graphics, visual and audible prompts to guide the user to an easy and quick transaction;
- Minimize the transaction time with clear graphics and instructions, simple steps, fast and accurate biometric capture processes, all based on proven ergonomic principles;
- Provide Americans With Disabilities Act (ADA) access and operation for applicants of varying heights, disabled applicants in wheel chairs, and applicants with visual or hearing impairments;
- Withstand heavy use in public spaces with a rugged shell, high reliability components, and minimal routine maintenance requirements;





- Provide internal monitoring that will confirm kiosk and network operational readiness and detect tampering, environmental issues, or degradation of performance that would indicate the need for service;
- Provide for trusted remote health monitoring, diagnostics, and controlled software updates;
- Operate as a trusted device within the overall TecSec chain of trust for the credentialing process;
- Provide a transaction audit trail including capture of keystrokes, process interaction timing, proof of enrollment capture events, and a video of the enrollment transaction;
- Comply with applicable standards including ADA, FBI, HSPD 12, PIV, PIV-I and CAC.

The TecSec Enrollment kiosk provides fast, high quality, accessible, and secure capture of personal data as part of the credentialing system. It is a fully designed and tested system requiring no expensive facility modifications to install -- just plug it into an electrical wall socket, hook it up to an internet connection, and it is ready to start enrolling. It is a high quality, robust, relatively inexpensive tool designed to produce high quality enrollments at high speed. With this device, enrolling the 5000 cards will have minimal impact upon other ongoing DMV operations.

Applicant enrollment is one of three primary functions to be conducted at the likely designated DMV's. The TecSec designed process will begin when an applicant arrives at the DMV location with the personal identification documentation required by West Virginia (commonly referred to as "Breeder Documents"). The PIV-I standards of FIPS 201 leaves the decision of what breeder documents are necessary to the discretion of the state. If desired by West Virginia, TecSec will assist in the determination of the appropriate documents necessary to establish the desired level of confidence for West Virginia's "Identity of Merit."

Assuming the credentialing of First Responders will be a West Virginia priority, for these initial 5000 enrollees, the first step in the enrollment process is for the trained DMV employee to check the WV Division of Homeland Security database to ensure the applicant is on the emergency personnel sponsor list. Next, the DMV employee operating the enrollment kiosk will perform a visual inspection of the documents presented and then process those documents into the TecSec Enrollment kiosk for an electronic validity check, thereby starting the process of enrollment. Assuming all of the documents pass<sup>1</sup>, the DMV operator will guide the applicant through the use of the enrollment station and capture the applicant's identity biometric information. Once complete the applicant's personal data is digitized and encrypted, it will be sent securely to the TecSec Central data repository in Morgantown and, upon confirmation of receipt, immediately deleted from the Enrollment kiosk.

---

<sup>1</sup> TecSec will work with West Virginia to establish procedures for dealing with documents that do not pass the validity checks.



### **A.2.2 Smart Card Printing**

The second function performed at the DMV will be card printing. The applicant's personal data is sent to the TecSec secure central data storage facility where applicant identification and adjudication information is stored. Once adjudication is complete, the necessary printing data including personal identification, biometric identification, PIV-I Certifications and any pre-authorized Attribute Containers are transmitted to the DMV where the card will be personalized and printed. TecSec envisions the card will be printed in a secure location within the DMV to ensure positive control of the serialized Armored Cards™.

TecSec recommends the DataCard SP75plus color card printer and encoder because of its compatibility with TecSec software products, capability of programming both the contact and contactless chips resident in the Armored Card™ in a single pass, and ability of performing lamination with high-resolution holographic images for additional security. It is a very high quality printer that operates quietly and smoothly, that has proven to be affordable to own and operate. TecSec has priced the DataCard SP75plus printer in the Attachment C.

### **A.2.3 Card Activation and Issuance**

The third function to be performed at the DMV is Card Activation and Issuance. A biometric card reader in conjunction with a Windows based Personal Computer (PC) operating with TecSec supplied software is all that is necessary to activate a card. Once the card is printed, the applicant will verify his/her identity to the DMV operator; place their finger on a biometric card reader which then transmits the captured fingerprint to the card where a biometric match is conducted. The card is then activated and any Attribute Container permission's are downloaded to the card. The applicant is now fully enrolled and his/her card is ready for daily use including, when the program expands as outlined in Attachment D, the adding of additional Attribute Containers.

There are several readers on the market, TecSec recommends the Precise Biometrics Model 250 MC which is priced in Attachment C. Any quality Microsoft Windows based PC will satisfy card activation needs.

### **A.3.0 Managed Service Central Site**

The TecSec Managed Service central site is located at 874 Fairmont Road, Suite F, Morgantown, WV 26501. The operational characteristics of the Managed Service Central site are included in detail in Attachment B, Section 2.5.5.7 in this proposal.

Figure 5 depicts the central site, its connectivity and security elements.





# West Virginia: Identity Management Services Offering Managed Service Central Site

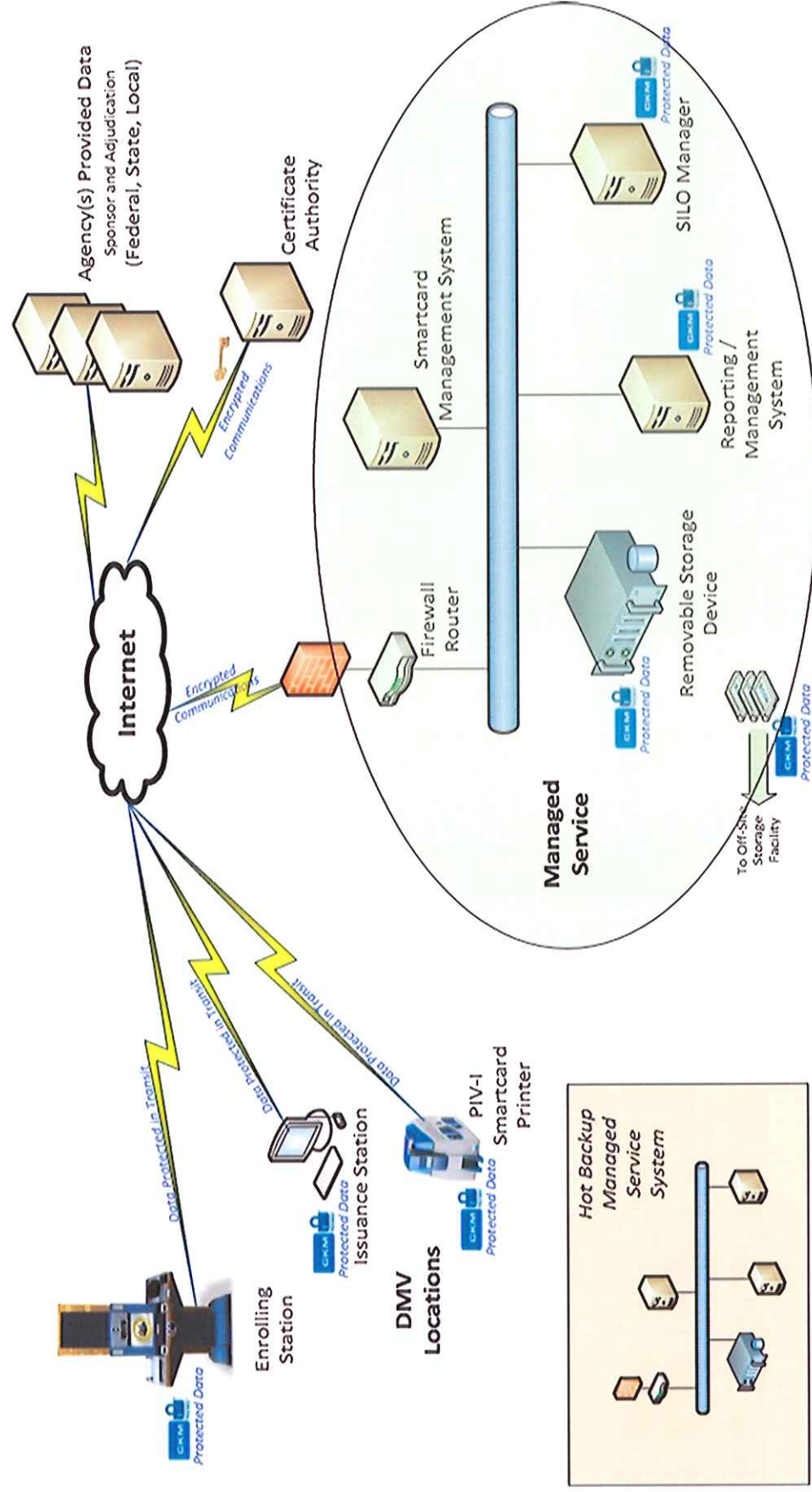


Figure 5 Functions Performed At the Managed Service Central Site



The Managed Services Central Site has the Smartcard Management System, Reporting Management Server, SILOS<sup>®</sup> Manager Server, and a Removable Storage Backup device. The Smartcard Management system controls the movement and direction of all card essential functions. Once all necessary enrollment steps have been completed, the system requests and obtains the necessary personal certificates from the Certificate Authority, and queries the SILOS<sup>®</sup> Manager Server to determine if there are any authorized Attribute Containers<sup>™</sup> to be created during issuance, prior to authorizing the issuance of the specific card. The Smartcard Management system has the capability to accommodate an independent adjudication request of questionable document either in a manual mode or through automated connections with various government databases necessary to confirm status of an applicant.<sup>2</sup> The user information that will reside on the card is returned to the DMV Issuance Station in encrypted form for card printing and subsequent card activation. Once the Card Management Server receives a response indicating that the Card was successfully activated, all the account information is archived.

A mirror image hot backup site is located in Northern Virginia. It contains the same functionality as the primary site and provides redundancy and Continuity of Operations Plans (COOP) capability. No user personal data resides outside the protected system.

---

<sup>2</sup> While not requested in this RFP, the Smart Card Management system can also be configured to perform centralized adjudication of identity prior to card issuance, providing the consistency and verification not possible using a distributed adjudication methodology.





#### ***2.4.1.1 Governance: Policy and Overall Intent-continued***

### **B. Issued and Sustained Trustworthy Identity Management Offering**

*Enable functionality where the credential is not part of a single application but rather is issued and sustained as trustworthy by the identity management offering. Has the ability to be used by many applications to reduce the cost of implementation across the WV state enterprise.*

The Multi-Function capability of the TecSec Armored Card™ through the use of CKM® encryption and Attribute Containers will be thoroughly demonstrated in a real time environment at the Orals/Demonstration Event.

TecSec's multi-owner/multi-function smart card is purpose built as a federation device and allows for a single card to provide multiple, discrete Attribute Containers of memory in which information is stored. The Attribute Containers™ are created through the use of the SILOS® Manager software tool, utilizing the patented CKM® cryptography at the digital object level, allowing differential access to the content contained in the memory as well as differential access to the information in each Attribute Container.

The TecSec SILOS® Manager supports multiple applications across any enterprise, recognizing that while identity is global, permissions are always local. Each SILOS® Manager created Attribute Container™ can be owned and managed independently by different agencies, allowing existing organizational and contractual relationships to be maintained. The technology enables state or federal agencies to insert permissions and/or privileges into an assigned container on the Armored Card™, which acts as a federation broker securely providing benefits and services to agencies, corporations, and citizens. In short, enrollment and adjudication of an individual establishes a trusted identity in the system. Multiple bits of information or application data can then be securely loaded on the single federation device, the card, thereby leveraging the established identity of merit.

The Armored Card™ is capable of storing information on the card as well as performing cryptographic functions; such as, authentication and secure biometric match, on the card itself. TecSec's patented SILOS® Manager enables each application provider to manage its own data without interference from the others. It is also completely flexible and extensible, allowing new application Attribute Containers™ to be added or removed as required by the changing circumstances of the cardholder, all under the supervision of the card management system, without the need to reissue a card with each change.

The Armored Card™ supports the federation of multiple enterprise permission sets on a common platform, with separation maintained by cryptography. The enterprise owner establishes an access control model defining the authorization requirements for their resources. This model is represented as a set of credentials. These credentials are distributed to the federation device. Multiple enterprise owners may place their credentials on the same federation device, independent of any other data owner. The card's capability to securely and cryptographically





store multiple credentials associated with multiple applications reduces the overall implementation costs associated with credential management across the WV State enterprise.

The TecSec identity solution described in Attachment D will have a big impact on the cost related to the operation and maintenance of programs within West Virginia that benefit from the establishment of an identity . Currently, each program has its own application, identity adjudication, and card issuance and management system, resulting in costly duplication across many program offices. The TecSec solution will allow for consolidation of identity verification, as well as card issuance and management into a single function, leaving each program office with the single responsibility of determining entitlement and feeding that entitlement data into an Attribute Container on the TecSec Armored Card™. The elimination of the duplicative administrative costs of performing identity verification and managing card issuance will result in an immediate savings for the multitude of card issuing programs currently in West Virginia.

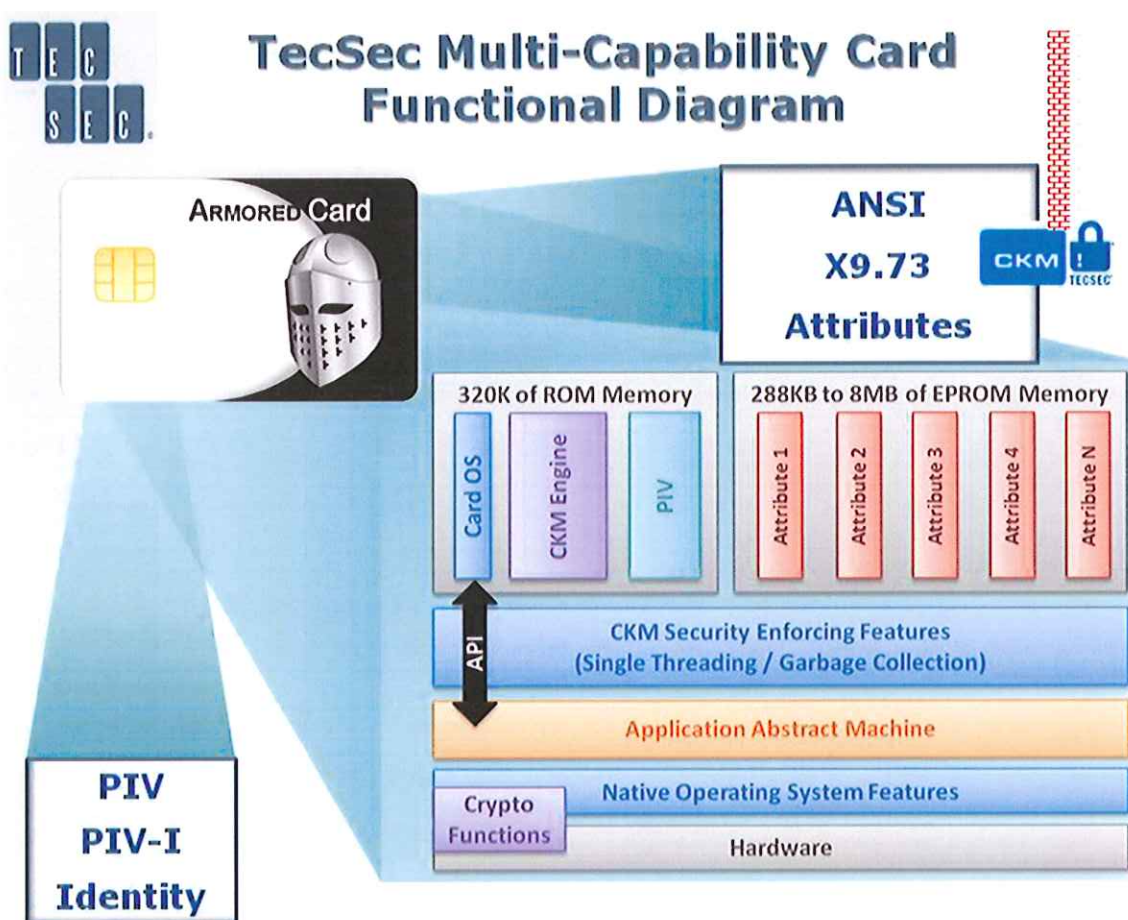


Figure 6 Functional Diagram of TecSec's Multi-Capability Card





#### ***2.4.1.1 Governance: Policy and Overall Intent-continued***

### **C. One Unique ID Credential used by Many Applications**

*Enable functionality where a credential is issued once to a unique identity and used by an unlimited number of applications dedicated by WV.*

When “Assuring” an identity by using a hardware token, like the Armored Card™, it is necessary to provide a mechanism that will assure the card only works for the person to whom it was issued. This process is necessary to prevent the card from being used by any other person, and to assure that a lost card cannot be operated without the need to wait for revocation of that card. The mechanism as published in the FIPS 201-2 DRAFT by the National Institute of Standards and Technology (NIST) is called Biometric Match on Card (BMOC). The placement of a biometric template/mathematical value on the card which can then be used to limit the cards usage to that one person to whom it was issued. The template must be stored on the card, and the computation of comparison must be made on the card itself for several reasons. First, privacy and confidentiality are a foundation of the solution. The idea of sending the stored fingerprint template from the card to a reader/server or a central database for comparison opens the door to significant security concerns. The card must work as a self-contained unit in all circumstances. The TecSec manufactured Armored Card™ is the only certified card that has the ability to provide an ANSI 378, Standards based, secure match on the card from both the contact and contactless interfaces.

TecSec’s federated Armored Card™ includes capabilities supporting personal identity and identity associated with roles/attributes. Encryption is used for enforcement; for electronic signature, for access control, and for confidentiality. The large memory capacity of the Armored Card™ is such that it can store data in discrete memory Attribute Containers™, supporting multiple applications, with assurances of liability separation. Each application exists within its prescribed memory space, assigned by the card issuer (WV) and enforced by CKM® encryption. An application and its data are confined to a specific memory area or Attribute Container. The issuer of the Armored Card™ can delete but not access the content once the Attribute Container™ has been assigned by the State to an organization other than the issuer. The operating system is single threaded so only one application at a time can be accessed, and the RAM is flushed between each application to prevent object reuse. The result of this application assignment approach is that the card issuer only has to track memory allocation while not being concerned with the functionality of a specific application. The card appears to act as a single function device to each of its resident applications and to the associated service or function with which the application interacts.

One Armored Card™ is able to contain many Attribute Containers™ within its boundaries, thereby allowing the Member-owner to have many Roles, each isolated from the others by a combination of the CKM® encryption, the SILOS® Management software, the Operating System, and hardware features of the card itself. Applications could be as varied as allowing a Member with one card to have access to many compartments, as shown in the following figure (figure 7):



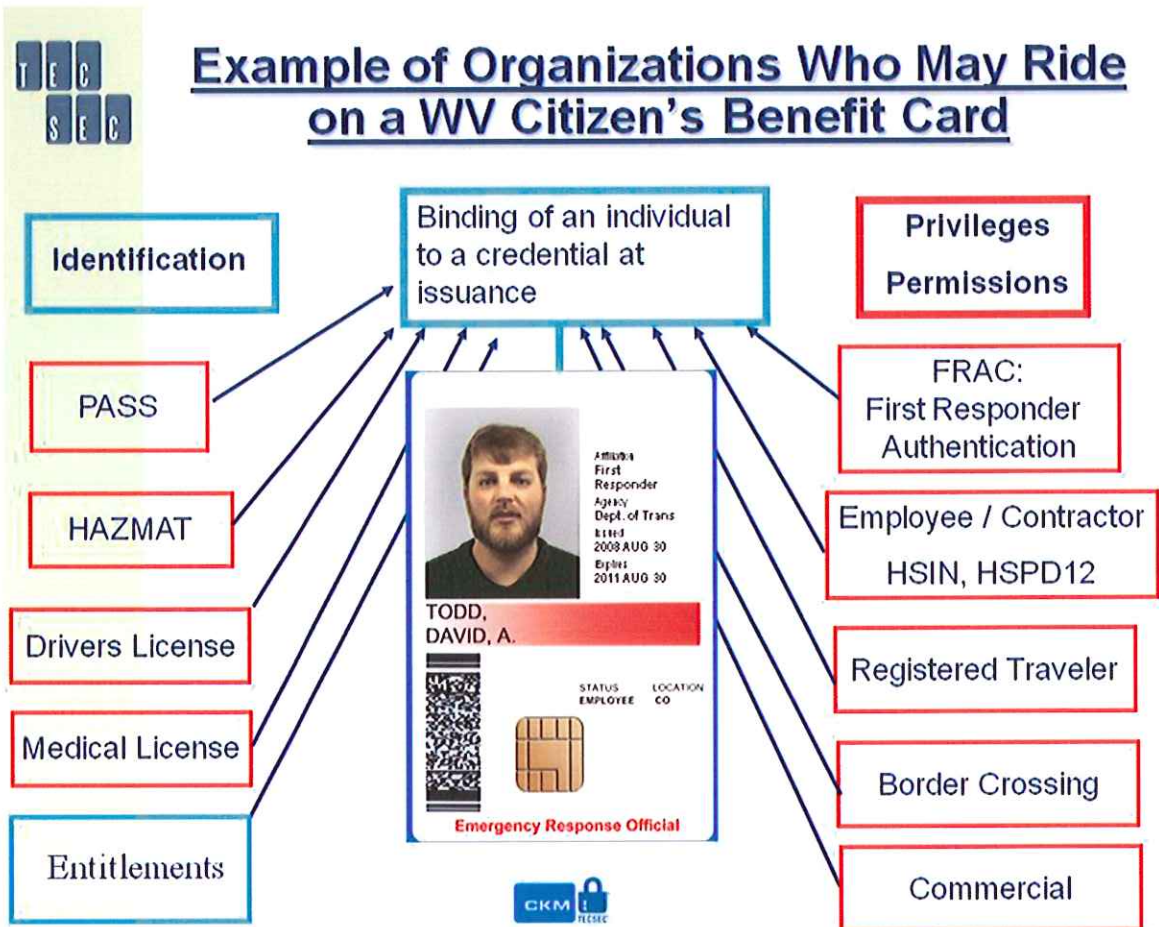


Figure 7 WV CBC Hosting Multiple Applications

While this CKM Enabled<sup>®</sup> Attribute Container<sup>™</sup> concept is unique to TecSec, all aspects of security are very important when it comes to the feasibility of a multi-application card. If multiple Attribute Container<sup>™</sup> owners each have their proprietary applications on a single card, for example, they are going to want assurance there will be no leakage of their data to anyone else. For security applications, it is essential that privileges allotted to one Attribute Container<sup>™</sup> on the Armored Card<sup>™</sup> do not also apply to other Attribute Containers<sup>™</sup> established on the card. CKM Enabled<sup>®</sup> Attribute Containers<sup>™</sup> offer users both access control and confidentiality for each of the separate applications and associated content on the smart card.

The number of applications/Attribute Containers<sup>™</sup> resident on the card is only limited by the amount of memory resident on the card. See Attachment D for the state wide approach for maintaining an almost unlimited number of applications resident on the card as dictated by West Virginia.





#### ***2.4.1.1 Governance: Policy and Overall Intent-continued***

### **D. Secure Data and Digital Signature**

*When used, enable an environment where data at rest and in transmission has the ability to be encrypted and documents digitally signed so as to maximize privacy requirements.*

The term "digital signature" applies to the technique of adding a string of characters to an electronic message that serves to mathematically verify the identity of the sender. A digital signature is a non-forgeable transformation of data that allows proof of the source with non-repudiation and the verification of the integrity of that data. Essentially, digital signature is a form of encryption using the appropriate certificate validated key.

The TecSec solution creates a PIV-I certified environment that provides the appropriate certificate for digital signing. Digital Signature by itself, however, provides no confidentiality and TecSec has augmented the environment for the enrollment and issuance process by using CKM<sup>®</sup> to protect the confidentiality of the data in transit and at rest.



#### 2.4.1.1 Governance: Policy and Overall Intent-continued

### **E. Personally Identifiable Data Authorized Access Only**

*When used, enable an environment where personally identifiable data will be made unreadable and unusable to unauthorized personnel in all applications where applied.*

The standards-based solution (including ANSI X9.69, X9.96 X9.112 and X9-73-2010) provided by TecSec establishes an environment where personally identifiable data is protected, and only accessible to those individuals possessing the correct credentials and with the designated authorization to view the information.

In the first instance, nothing on a TecSec Armored Card™ can be read without the card first being activated by a biometric match performed on the card. Thus a lost or stolen card cannot reveal any personally identifiable data beyond that printed on its face in accordance with the design to be established by West Virginia. Second, since each application is only capable of decrypting and reading its permission set from its own discreet, encrypted, Attribute Container™, there is no possibility of obtaining any information other than that authorized. Third, since the Armored Card™ performs a RAM flush between operations, there is no “leftover” personally identifiable information available in any common space on the card for a sophisticated hacker to access. Finally, any communications between the card and the centralized location where the encrypted enrollment record is stored will be encrypted with CKM®. In short, the TecSec Armored Card™ and the system proposed provides:

- Identity Protection – an individual’s identity is protected because no one can gain access to their private data without their permission.
- Security – no individual can gain access to any privilege to which they are not entitled. No agency or office can obtain information about another without express permission. Also, no application can interfere with another application on the system, or gain access to another application’s data.
- Consistency – individuals, agencies, and offices can be assured of a state mandated level of assurance for each individual, properly bound to a credential.

In an overall context, security for information can be summed up as authorizing someone to have access to information and, additionally, enforcing access to information through rules, attributes, or roles.





#### ***2.4.1.1 Governance: Policy and Overall Intent-continued***

### **F. Convenience and Cost Reduction by Migrating Paper to Digital Infrastructure**

*When used, will enable an environment to streamline and migrate state based transactions from paper based to the use of the digital infrastructure so as to reduce cost and provide convenience to the citizens of WV.*

There are two significant cost elements that are immediately addressed by implementing the plan discussed in Attachment D. The first, and the one with the largest financial impact, is fraud. A significant amount of all benefit programs is lost due to the inability to provide positive confirmation of the identity of the recipient of the services or benefit. Whether from improper sharing of a benefit card, the outright theft of a card, or the submission of false identity to create multiple enrollments, the end result is the same – diversion of program resources through payments to unqualified recipients. Similarly, on the provider side, a considerable amount of fraud comes in the form of billing irregularities.

The establishment of the TecSec identity solution described in Attachment D will virtually eliminate fraud based on identity. The TecSec Armored Card™, through the combination of its encrypted Attribute Containers™ and necessity of a biometric match on card prior to use, will prevent sharing of benefit cards, obtaining services with a stolen card, and, since it is based on a single identity of merit, will also prevent establishment of a false identity for the purpose of multiple enrollments. Similarly, the requirement to use the card to obtain benefits will eliminate many provider based frauds, especially billing for phantom beneficiaries.

The second area where the TecSec identity solution described in Attachment D will have a big impact is in the operation and maintenance of these same programs. Currently, each program uses a substantial amount of the program monies to operate and maintain a separate and distinct card program. Each program has its own application, identity adjudication, and card issuance and management system, resulting in costly duplication across many program offices. The TecSec solution will allow for consolidation of identity verification as well as card issuance and management into a single function, leaving each program office with the single responsibility of determining entitlement and feeding that entitlement data into an Attribute Container™ on the TecSec card. The elimination of the duplicative administrative costs of performing identity verification and managing card issuance will result in an immediate savings for the multitude of card issuing programs in West Virginia. In addition, by charging non-resident agencies and commercial entities for leasing Attribute Containers™ on the Armored Card™, the entire TecSec identity solution can become a source of revenue for West Virginia.

Third, using the TecSec identity solution described in Attachment D will facilitate secure electronic billing since the necessary billing information can be extracted from the Attribute Container™ on the Armored Card™ by a service provider with appropriate permission to read the necessary data from the card. The ability to extract this data in an automated and accurate fashion and combine it with electronic data from the service provider will enable secure real time billing and reporting, both facilitating the elimination of paper and establishing a positive



electronic audit trail. In addition, the efficiencies in transmission of data will allow for faster processing of transactions and faster fulfillment of state obligations to its citizens, enhancing convenience while providing a far greater level of privacy and security for the citizens' transactions.

#### **2.4.1.2 Workflow Software**

*Workflow software Manages Identity and Card Lifecycle Process Management activities. The Certificate Authority governs the issuance of Card Certificates.*

Workflow Software is included in all of the TecSec products. The TecSec Enrollment Kiosk contains work flow software that automatically sequences the data capture for enrollment, ensuring that each step is accomplished successfully before advancing to the next step. Failure to complete a step results in notification to the operator to redo the failed operation. This automated work flow sequencing ensures that a complete valid record is created before transmission to the centralized Card Management system. The Card Management system utilized by TecSec will be linked directly to the Certificate Authority and the linkage and processing of the Certificates will be certified by the Certificate Authority. Figure 8 is a high level process flow diagram of the automated card issuance process incorporated into the TecSec Workflow Software.





State of West Virginia  
RFQ No. HSE01154  
Identity Management Service Offering

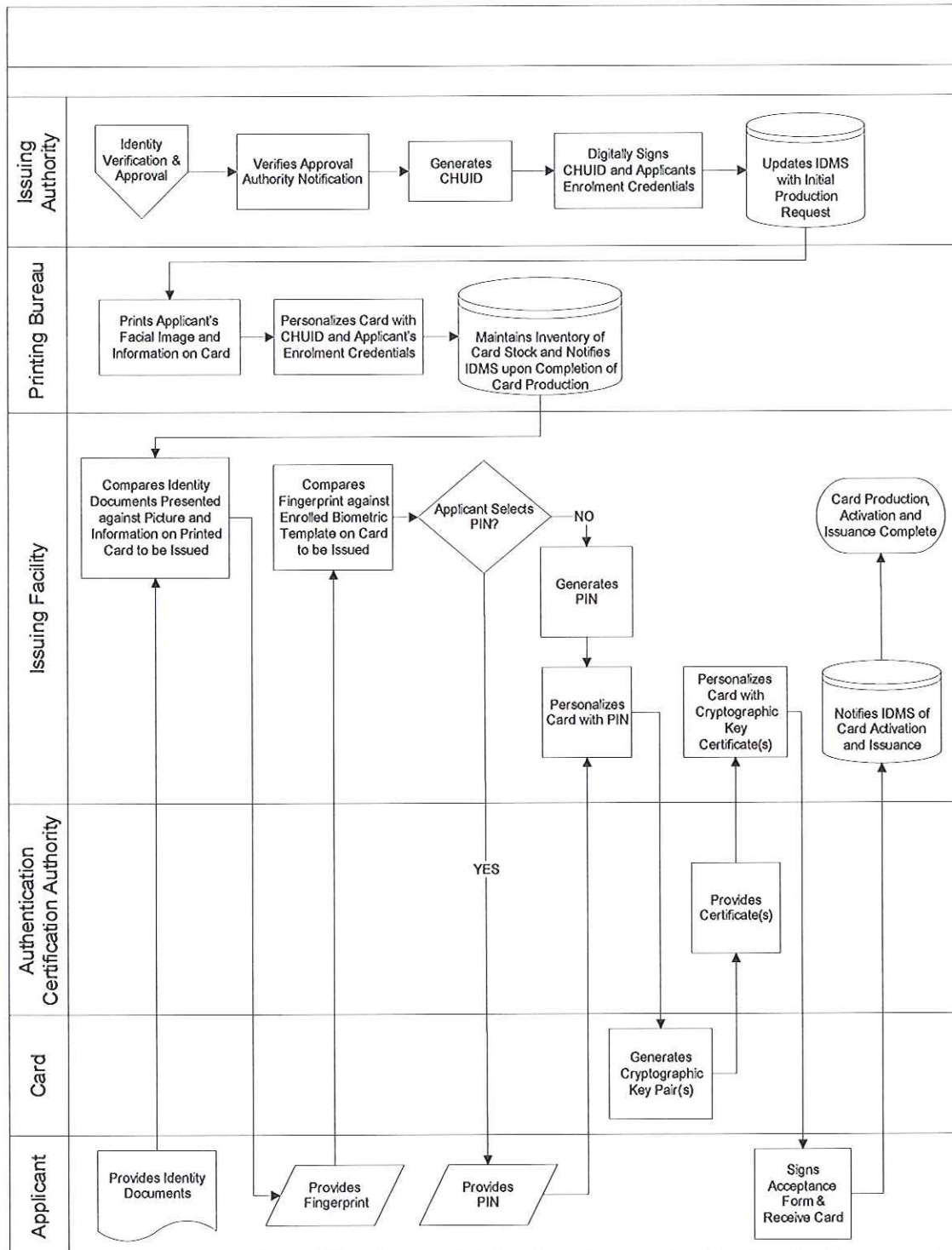


Figure 8 Identity Management Workflow Software



### 2.4.1.3 Equipment Recommendations

*The vendor should suggest equipment for both fixed and mobile issuance as well as catalogue of all hardware necessary for the system to be utilized to its fullest potential. The State or other jurisdictions will then select the hardware it wants.*

The TecSec system is designed to offer flexibility in the issuance phase as well as the broad spectrum of possible uses. The entire system has been designed not to require many unique pieces of equipment. By packaging the enrollment function into one stand-alone easy to use Kiosk, TecSec has eliminated the need to integrate and provision the many different peripheral devices necessary to accomplish user enrollment. Another design criterion has been to maximize the use of commercially available hardware and software. Therefore, very little life cycle cost is required to operate and logistically support the complete system.

In this section we catalogue several of the available products that can be purchased by the state for issuance and utilization in various environments. All equipment described is priced in Attachment C unless otherwise noted.

- Enrollment:
  - For user enrollment we have offered our fully articulated Enrollment Kiosk. This kiosk is optimized for high volume use in a fixed location. Recognizing that as the program expands, as outlined in Attachment D, there will likely be a need for lower volume fixed locations as well as portable enrollment equipment, TecSec has also offered three additional options.
  - To meet the need of a low volume fixed site, TecSec offers a non-articulated kiosk with essentially the same built-in data capture capability as the fully articulated version.







State of West Virginia  
RFQ No. HSE01154  
Identity Management Service Offering



- To meet the need of a portable unit for special events or temporary indoor locations, TecSec offers its tabletop enrollment device which is capable of collapsing into a suitcase for easy transportability. This device has the same capability as the Kiosks; however, several of the peripheral devices attach through cables rather than through incorporation into the cabinet.



- To meet the need of a high volume, temporary location, TecSec offers its fully articulated Kiosk installed in a purpose built vehicle containing independent electrical, internet connection, and the necessary security to store supplies. This vehicle can be driven to various locations within and without West Virginia as necessary.



- Activation
  - Commercial-off-the-shelf, Microsoft OS and Windows based desktop or portable computers. (Because these are commodities, they have not been priced in Attachment C.)
- 7816 Card Readers
  - Biometric/Fingerprint readers are required in order to capture a fingerprint and supply that captured fingerprint to the card for matching. TecSec recommends the following three commercially available models. In our estimation these three readers provide a reasonable balance between validated operational capability and price.
    - Precise Biometrics Model 250MC
  - For instances where a card reader is required and biometric capability is not critical, TecSec recommends the following readers:
    - Athena Model ASEIIIe
    - SDI Model 010 or Model 011
- Handheld Readers
  - TecSec recognizes that there will be a need for cards to be read in the field both in connected and stand-alone environments. While the TecSec Armored Card can work with any reader meeting the standard, we believe the best value can be obtained from the MAX ID Products. We recommend the MAX ID Model 300.
- Card Printers
  - TecSec recommends a DataCard SP75plus color printer/encoder. Other card printers and encoders are available and will function but DataCard has proven fully compatible with TecSec and card management software.





- Physical Access
  - The CBC card also has the capability to be utilized as part of a Physical Access Control System (PACS) provided the system has a head unit that is ISO 14443B compliant. Since the choice of head unit will necessarily depend on the underlying system, the location of the heads to be installed, and the ability to make use of previously installed readers, TecSec is not recommending any particular unit.
- Servers
  - TecSec systems are designed to run on Microsoft Windows based standard commercial servers. (Because these are commodities, they have not been priced in Attachment C.)

## 2.4.2 Attribute Management

### 2.4.2.1 On Card Authentication

*An attribute is a qualification, benefit, authorization, certification, license and/or privilege that is bound to that unique identity and can be electronically validated using the identity token and relying party digital infrastructure to also include times when power or communications is unavailable.*

When assuring an identity by using a hardware token, in this case a smart card, it is necessary to provide a mechanism that will assure the card only works for that person to whom it was issued. This process is necessary to prevent the card from being passed around, used by other person(s) and to assure that a lost card cannot operate inappropriately. The mechanism prescribed by the National Institute of Standards and Technology (NIST), as set forth in FIPS 201-2 DRAFT, is called Biometric Match on Card (BMOC). The placement of a mathematical value on the card, generated from a personal biometric, which can then be used to limit the cards usage to that one person to whom it was issued. The template must be stored on the card, and the computation of comparison must be made on the card itself. Privacy and confidentiality are a foundation of the solution.

The idea of sending a fingerprint from the card to a reader/server or central database for comparison is not viable and opens the door to significant security concerns. In addition, there is the simple fact that there are many places in the United States where network connectivity is simply not available. Everyone has experienced this lack of connectivity using cell phones. The card must work as a self-contained unit, in all circumstances. The TecSec Card is the only certified card offered that has the ability to provide an ANSI 378, Standards based, BMOC.

Similarly, access to a specific Attribute Container™ does not require access to anything other than the Armored Card™ itself and a reader. The Attribute Containers™, once established and provisioned, can be accessed and decrypted by anyone possessing the necessary permission set. For instance, if an Attribute Container™ on an individual card is restricted to Emergency Medical Technicians, anyone with the permission set of an Emergency Medical Technician will be able to read the contents of that container from a hand held device without the need to check a distant database for verification of permissions.





#### **2.4.2.1.1 Privilege Attribute Assignment & Management**

*Vendor to provide "Privilege/Attribute Assignment" software that Agency uses to assign privileges and attributes to Users. "Privilege/Attribute Management" software also is provided for authorized Agency representatives to synchronize the privilege and attribute information associated with Users with the same information in any handheld or other device to eventually include smart phones, and/or tablet platforms which an Agency may use to perform relying party electronic validations. This software should be installed on the Enrollment Station or Issuance Station provided as part of the Card service.*

This RFP for 5000 Citizen's Benefit Cards requires TecSec's limited version of its SILOS<sup>®</sup> Manager for creating Privilege/Attribute Containers<sup>™</sup>. The actual provisioning of the Attribute Containers<sup>™</sup> occurs during card activation and the software that manages the creation of the containers works in conjunction with the Card Management system and needs to operate at the centralized location. For larger scale applications, with many Attribute Containers<sup>™</sup> on a single card, TecSec utilizes a combination of the full version of its SILOS<sup>™</sup> Manager acting in combination with the TecSec Enterprise Builder<sup>™</sup>, a program designed to facilitate and manage the issuance of role based access credentials (see Attachment D for further explanation). For this initial program, TecSec is providing a Use License for the limited version of its SILOS<sup>®</sup> Manager, CKM<sup>®</sup>, and ancillary software for up to 5000 cards. This software will also allow the synchronization of the privilege and attribute information on the cards with certified hand held devices. TecSec has designed its CKM<sup>®</sup> technology to be able to move from the card form factor to a variety of mobile devices including smart phones and Tablet computers. TecSec has already transitioned its technology from card format to SIM chips and will have a Micro SD version by the end of the year. The TecSec PIV/CKM<sup>®</sup> technology combination offers the State of West Virginia a secure highway to the future of eGovernment, eHealth, and eCommerce and not a dead end road that may look nice when first started but does not go anywhere.



## **Attachment B: Mandatory Specification Checklist**

### **2.5 Attachment B; Mandatory Requirements**

#### **2.5.1 Products and Services: General Services Administration (GSA) FIPS 201-Approved Products and Services List (APL)**

##### **2.5.1.1 Enrollment Station**

*Collected data is transmitted over an encrypted connection to a central hosted storage facility, using an Agency-provided Internet connection, so no personally-identifiable information is stored locally on the Enrollment Station.*

The standards-based solution (including ANSI X9.69, X9.96 X9.112 and X9-73-2010) provided by TecSec establishes an environment where all data is protected by CKM<sup>®</sup> encryption and is only accessible to those individuals possessing the correct credentials and with the designated authorization to view the information.

Nothing on a TecSec Armored Card<sup>™</sup> can be read without the card first being activated by a biometric match performed on the card. Thus a lost or stolen card cannot reveal any personally identifiable data beyond that printed on its face in accordance with the design to be established by West Virginia. Second, since each application is only capable of decrypting and reading its permission set from its own discreet, encrypted, Attribute Container<sup>™</sup>, there is no possibility of obtaining any personally identifiable or other information other than that authorized. Third, since the Armored Card<sup>™</sup> performs a RAM flush between operations, there is no “leftover” personally identifiable information available in any common space on the card for a sophisticated hacker to access. Finally, any communications between the card and the centralized location where the encrypted enrollment record is stored will be encrypted with CKM<sup>®</sup>. In short, the TecSec Armored Card and the system proposed provide:

- Identity Protection – an individual’s identity is protected because no one can gain access to their private data without their permission.
- Security – no individual can gain access to any privilege to which they are not entitled. No agency or office can obtain information about another without express permission. Also, no application can interfere with another application on the system, or gain access to another application’s data.
- Consistency – individuals, agencies and offices can be assured of a state mandated level of assurance for each individual, properly bound to a credential.

In an overall context, security for information can be summed up as authorizing someone to have access to information and, additionally, enforcing access to information through rules, attributes or roles.





## Enrollment Station Hardware

The TecSec system includes a totally integrated enrollment kiosk that is comprised of compliant third party components. The FIPS 201 process of establishing an identity that can provide high assurance and interoperability is a crucial aspect of the standard. The adoption of PIV-I as enterprise policy for identity creation is an important step to the creation of a high assurance identity infrastructure.

TecSec will ensure compliance with all GSA testing and evaluation requirements for PIV-I credentials and FIPS 201 products and services. TecSec has carefully selected solution components that are either FIPS 201 approved or have been tested and are awaiting formal approval.

The following provides a list of these components specific to those requested in the RFP:

1. **A Laptop Computer with a Card Reader** (TecSec approach uses a self-contained kiosk not individual peripheral devices)

- **Digital Camera**

Facial image capture: Lumenera LC370 digital color camera

FIPS certification: N/A

- **Fingerprint Reader**

Fingerprint sensors (2 units – Left and right side of kiosk): Futronic FS50

FIPS certification: Yes

The FS50 can capture single finger, dual finger, and roll finger image. It was certified by the FBI to be compliant with PIV-071006 Image Quality Specification ([http://www.futronic-tech.com/download/FBI\\_PIVspec\\_071006.pdf](http://www.futronic-tech.com/download/FBI_PIVspec_071006.pdf)) for Single Finger Reader. The FS50 meets the US Federal Information Processing Standard 201(FIPS 201) for Personal Identification Verification (PIV) of Federal Employees and Contractors. It is also listed in the US General Services Administration (GSA) FIPS 201 Evaluation Program Approved Product List (<http://fips201ep.cio.gov/apl.php>).

- **An External Monitor**

Integrated touch screen monitor – integrated within the Kiosk

FIPS certification: N/A

- **Enrollment Capability Via Kiosk**

The TecSec solution includes an integrated biometric, breeder document and demographic capture kiosk to serve as an all-inclusive enrollment frontend to serve all required enrollees.



Our solution is a Common Biometrics Exchange Format Framework (CBEFF) compliant product suite. This is accomplished through the use of InterNational Committee for Information Technology Standards (INCITS) constructs for compliance.

Breeder documentation capture and automatic validation is achieved using a 3M ID-2 and ID-1 document size reader/scanners with AssureID verification libraries. The 3M readers are used throughout the world and within the United States by Immigration and Border Control Agencies. The AssureID software libraries includes library support to classify, read, and authenticate all documents in the AssureID library including international travel documents (ICAO and non-ICAO) and driver's licenses (all US active) and identifications cards from all geographic regions. The AssureID software is FIPS certified and approved.

#### **Standards Based:**

Biometrics and enrollment services are all about standards. The TecSec KIOSK is designed to meet the prevailing and applicable standards.

#### **Fingerprint:**

FBI, PIV-071006, FIPS 201, ANSI INCITS-378

#### **Face Image:**

ANSI INCITS-385, ICAO, ISO/IEC 19794-5

#### **Iris:**

ISO/IEC 19794/19785

#### **Document Scanner/Readers:**

FIPS, IATA: TAT and ATB ICAO 9303 ISO 14443B

#### **Data Security:**

ANSI X9.69, ANSI X9.73-2010

#### **Enrollment Station Software**

The Enrollment Kiosk is a collection of devices that collect identity information from the user (enrollee), packages it, and provides this data to an external Card Management System. There is no specific GSA category listed or defined for the software that coordinates this functionality. TecSec has configured its Enrollment Kiosk software to ensure that all communications with the Kiosk are encrypted using CKM<sup>®</sup> and that no personally identifiable information is stored in the Kiosk.

#### **Issuance Station**

The Issuance Station described in the RFP combines the functionality of card issuance and card activation. Accordingly, the equipment used in both functions is detailed below.





### **2.5.1.2 Issuance Station**

#### **Issuance Station Hardware**

- A laptop computer with a Card reader
  - Standard commercially available Microsoft Windows based laptop computer
  - FIPS certification – N/A
- Fingerprint reader
  - Precise Biometrics Model 250MCFIPS certification – FIPS 201, GSA APL
- PIN entry pad
  - Standard commercially available keyboard
  - FIPS certification – N/A
- Card printer
  - DataCard SP75Plus
  - FIPS Certification – FIPS 201, GSA APL

#### **Issuance Station Software: Appropriate Software**

The Issuance and Activation processes are controlled by Card Management Software. TecSec will be utilizing the Intercede MyID card management system which is fully certified under FIPS 201. In addition, TecSec will have an electronic interface with the Certificate Authority, integrating the issuance of Certificates into the card management process, which will be approved and certified by the Certificate Authority.

- Authorized Agency representatives use the Issuance Station to: Validate a User with his or her previously collected digital photograph, fingerprint data
- Print User's card
- Issue User's card
- Activate User's Card including a User selected PIN

The station also captures the User's digital signature confirming receipt of the Card.

The Issuance Station embeds an identity-authenticating Certificate on the Card, through which the User's identity and privileges/attributes can be confirmed by any interoperable identity validation system.

Also embedded are a digital signing Certificate, a key management Certification, and a card authentication Certificate for physical access purposes.



## 2.5.2 Operational Execution: Practice

*The Vendor must provide train the trainer assistance for usage of all issuance, attribute, and validation equipment/tool sets.*

TecSec will provide as part of this contract train the trainer assistance for all issuance, attribute and validation equipment as identified in this proposal. TecSec will develop and deliver a formal Training Plan for a train the trainer program to cover the operation of all delivered products. In addition, TecSec will conduct an initial two day training with the State designated trainers at a central location. In addition; TecSec will provide three day technical oversight and operator level training at each of the three DMV locations during equipment installations and initial operations. The proposed training schedule is included in the Master Program Schedule in Attachment A, Table 1.

The Train-the-Trainer program will consist of a workshop utilizing the following syllabus:

- System overview
  - Applicable handouts and material to familiarize the trainers with the overall system.
- Enrollment
  - Applicable handouts and hands-on Kiosk segment to train on the full use and capabilities of the enrollment kiosk including document verification and operator level maintenance procedures.
- Issuance
  - Applicable handouts and hands-on Issuance Station segment to train on the full use and capabilities of the Issuance Station unit including operator level maintenance procedures.
- Activation
  - Applicable handouts and hands-on Activation Station segment to train on the full use and capabilities of the Activation Station including operator level maintenance procedures.
- Attribute
  - Applicable handouts and system use segment to train on the functionality and operator level operations that can be performed with SILOS<sup>®</sup> Manager.

Enrollment and Issuance training for the initial Operators will be scheduled so as to be Just-in-Time training coinciding with go-live enrollment and issuance to the user community at each of the three DMV locations. In addition, TecSec will place personnel at the designated DMV's during the first week of operation to support the WV user staff first-hand to ensure smooth operation and a complete understanding of the system.





### **2.5.3 Products and Services: General Services Administration (GSA) FIPS 201 Approved Products & Services List (APL) and ANSI Standard criteria for attribute management**

*All products for attribute management will meet the requirements of ANSI standard X9.69 for multi-use purposes, which allows for the capability to link source databases.*

All TecSec attribute management is performed by the SILOS<sup>®</sup> Manager software and encrypted using CKM<sup>®</sup>. The TecSec approach to attribute management brings with it the following features, not available through any other solution:

- Key material not specific to individuals
- Addresses the one-to-many distribution problem of key management
- Ability to re-key without requiring decryption and re-encryption
- Ability to re-key without the need to re-issue cards
- Access privileges bound to data via cryptography
- Built-in key recovery performed by system owner
- Role-Based and Attribute Access Control (RBAC/ABAC)
- Content-based security
- Self-Protecting Data Objects
- Complementing PKI
- ANSI 385 Facial Match on Card

SILOS<sup>®</sup> Manager and CKM<sup>®</sup> both meet:

- X9.69 Framework For Key Management Extensions
- X9.96 Secure XML
- X9.112 Secure Wireless
- X9.73 – 2010 Cryptographic Message Syntax – ANS.1 & XML

### **2.5.4 Validation Management**

#### **2.5.4.1 Validation is the Electronic Verification of the Identity and Attributes**

TecSec products meet the PIV-I Validation Management criteria. TecSec will establish a secure link with a Certificate Authority and will obtain certification from the Certificate Authority on the integrity of the system prior to commencement of enrollment. .

#### **2.5.4.2 Products and Services**

##### **2.5.4.2 A Handheld Devices and Card Validation**



*Handhelds may be used alone or with other appropriately-equipped relying party devices, such as Enrollment or Issuance Stations to validate the identity of a User by confirming that the applicable Certificate has not been revoked (as of the last time the revocation list was checked) validate the privileges and attributes of a User.*

The handheld recommended by TecSec (MaxID 300) includes both a card reader and fingerprint reader and has a color screen that displays the user name, certificate status, privileges/attributes, and other information. In addition, this handheld has the ability to operate in either a stand-alone or connected environment. When connected, the handheld is capable of interfacing with any device or database that contains a Certificate Revocation List (CRL) for privilege and attribute validation.

Since the attributes reside in Attribute Containers™ on the Armored Card™, there is no need to query a remote database to validate a privilege/attribute other than to check for revocation. There is no charge to anyone for reading a card or accessing an Attribute Container™ and there is no limit on the number of validations that can be performed on appropriate third party hardware/software.

## **2.5.5 Support**

### **2.5.5.1 Installation and Training**

The Enrollment, Issuance, and Activation Stations will be loaded with applicable software and tested before shipping to the Agency designated locations. Once received on-site, TecSec personnel will install, test, and be provided with an Agency sign off and acceptance.

TecSec will provide as part of this contract train the trainer assistance for all issuance, attribute and validation equipment as identified in this proposal. TecSec will develop and deliver a formal Training Plan for a train the trainer program to cover the operation of all delivered products. In addition, TecSec will conduct an initial two day training with the State designated trainers at central location In addition; TecSec will provide three day technical oversight and operator level training at each of the three DMV locations during equipment installations and initial operations. The proposed training schedule is included in the Master Program Schedule in Attachment A, Table 1.

The Train-the-Trainer program will consist of a workshop utilizing the following syllabus:

- System overview
  - Applicable handouts and material to familiarize the trainers with the overall system.
- Enrollment
  - Applicable handouts and hands-on Kiosk segment to train on the full use and capabilities of the enrollment kiosk including document verification and operator level maintenance procedures.
- Issuance





- Applicable handouts and hands-on Issuance Station segment to train on the full use and capabilities of the Issuance Station unit including operator level maintenance procedures.
- Activation
  - Applicable handouts and hands-on Activation Station segment to train on the full use and capabilities of the Activation Station including operator level maintenance procedures.
- Attribute
  - Applicable handouts and system use segment to train on the functionality and operator level operations that can be performed with SILOS<sup>®</sup> Manager.

Enrollment and Issuance training for the initial Operators will be scheduled so as to be Just-in-Time training coinciding with go-live enrollment and issuance to the user community at each of the three DMV locations. In addition, TecSec will place personnel at the designated DMV's during the first week of operation to support the WV user staff first-hand to ensure smooth operation and a complete understanding of the system use.

#### **2.5.5.2 Documentation and Multi-platform Topology**

*Vendor will provide templates for the Agency to define lifecycle management processes, specifically for registration, enrollment, issuance, and revocation of User Cards.*

Subject to the limitations of the Consulting Services line item in Attachment C of this contract, TecSec will:

- Work with the Agency to define policy documentation conforming to TecSec's operational requirements and provide templates to define lifecycle management processes for registration, enrollment, issuance, activation, and revocation of Attribute Containers<sup>™</sup> resident on Armored Cards<sup>™</sup>.
- Work with the Agency to obtain policy documentation to support Certificate Authority Web Trust Audits.
- Assist the Agency to determine the requirements for the physical card topology and IPL allocation conforming to PIV-I requirements.

#### **2.5.5.3 Reporting**

If requested, TecSec will provide monthly status reports that will include the number of Users Sponsored, Enrolled, Cards Printed, and Cards Activated. In addition, if requested, TecSec will provide monthly reports of service level performance and service failures.

#### **2.5.5.4 Hardware and Software Maintenance**

TecSec will provide maintenance support for up to three years for defective hardware it supplies to the Agency. TecSec will have the option to repair or replace defective hardware. TecSec will provide maintenance for defective software it provides to the Agency for up to three years



provided that the Agency has not attempted to modify the software on its own or through a third party agent.

#### **2.5.5.5 Reporting of Security Breaches**

TecSec will notify the Division of Homeland Security of any breach attempts specifically targeted at the Agencies identity management service after becoming aware of the event. TecSec will act upon any security breach notification brought to our attention by the Agency as soon as possible. TecSec will cooperate with any investigation concerning the alleged breach and share findings with the Agency including intended solutions.

#### **2.5.5.6 Cards**

The TecSec Armored Card™ complies with:

- ISO/IEC 7810 [ISO7810]
- ISO/IEC 10373 [ISO10373]
- ISO/IEC 7816 for contact cards [ISO7816]
- ISO/IEC 14443B for contactless cards [ISO14443B]
- FIPS 201-1

Additional capabilities of the Armored Card™ include a biometric match-on-card within a contact (International Standards Organization or ISO 7816) as well as contactless (ISO 14443B) mode, Public Key Infrastructure (PKI ) support, Constructive Key Management (CKM®) support, and a contact mode for external application interface and support.

The TecSec Armored Card™ meets all required Standards and is warranted defect free for 90 days.

#### **2.5.5.7 Data Storage Facility Agency-transmitted**

*Agency-transmitted User identity data is to be stored at a secured, hosted facility for control purposes.*

The User identity data is to be stored at the secure TecSec hosting facility, located at 874 Fairmont Road, Suite F, Morgantown, WV 26501. TecSec established a local office in the Morgantown, WVA area to better serve the needs of the State of WV.

The facility is monitored by redundant video surveillance and has controlled entry systems. It is equipped with state-of-the-art technology encompassing all elements associated with a Data Center and a Disaster Recovery Site.

The facility is protected and provides for the following:

- Emergency power generator
- Uninterrupted power supply (UPS)
- Smoke/fire detection and fire suppression system





State of West Virginia  
RFQ No. HSE01154  
Identity Management Service Offering



- Dedicated air conditioning with environmental monitoring
- Redundant alarm system
- Visual monitoring systems
- Scalable rack space
- Secured entry

TecSec will provide the operating systems, security administration, facilities and infrastructure that will host the User information from enrollments under this contract in a manner consistent with industry standard practices, utilizing firewall products, and gateways. All communications and all data storage will be encrypted through the use of the TecSec patented CKM<sup>®</sup> technology that meets all the government certifications for data protection-coving data at rest, data in motion, and data over time. Because all data resides in an Attribute Container<sup>™</sup> on the card, agency transmitted User identity data will not be accessed by Agencies performing validation in the field.

In addition to the Morgantown, WV hosting facility, TecSec will set up a remote disaster-recovery location in a commercial hosting facility in Northern Virginia that has the same security features as the West Virginia facility. The Northern Virginia facility will be configured as a hot fail over system for the primary West Virginia system and will use the same CKM<sup>®</sup> encryption for data protection. Data will be protected through the use of regular backups (daily, weekly, quarterly, and yearly) and through the monitoring of infrastructure availability and resource utilization.



## TecSec Certifications

Table 3-1 TecSec FIPS 140-2 Testing Certificates - Algorithms

Certificate No.	Description (URL)	Platform/OS Tested	Date
131	RSA Validation Certificate ( <a href="http://csrc.nist.gov/cryptval/dss/rsaval.html">http://csrc.nist.gov/cryptval/dss/rsaval.html</a> )	Pentium III 933 MHz processor w/ Windows 2000	April 2006
163	Digital Signature Algorithm (DSA) Validation Certificate ( <a href="http://csrc.nist.gov/cryptval/dss/dsaval.htm">http://csrc.nist.gov/cryptval/dss/dsaval.htm</a> )	Pentium III 933 MHz processor w/ Windows 2000	April 2006
165	Digital Signature Algorithm (DSA) Validation Certificate ( <a href="http://csrc.nist.gov/cryptval/dss/dsaval.htm">http://csrc.nist.gov/cryptval/dss/dsaval.htm</a> )	Pentium III 933 MHz processor w/ Windows XP	April 2006
167	Keyed-Hash Message Authentication Code (HMAC) Validation Certificate ( <a href="http://csrc.nist.gov/cryptval/mac/hmacval.html">http://csrc.nist.gov/cryptval/mac/hmacval.html</a> )	Pentium III 933 MHz processor w/ Windows 2000	April 2006
181	Random Number Generator (RNG) Validation Certificate ( <a href="http://csrc.nist.gov/cryptval/rng/rngval.html">http://csrc.nist.gov/cryptval/rng/rngval.html</a> )	Pentium III 933 MHz processor w/ Windows 2000	April 2006
379	Advanced Encryption Standard Algorithm Validation Certificate ( <a href="http://csrc.nist.gov/cryptval/aes/aesval.html">http://csrc.nist.gov/cryptval/aes/aesval.html</a> )	Pentium III 933 MHz processor w/ Windows 2000	April 2006
422	Triple DES Modes of Operation Validation Certificate ( <a href="http://csrc.nist.gov/cryptval/des/tripledesval.html">http://csrc.nist.gov/cryptval/des/tripledesval.html</a> )	Pentium III 933 MHz processor w/ Windows 2000	April 2006
450	Secure Hash Standard (SHS) Validation Certificate ( <a href="http://csrc.nist.gov/cryptval/shs/shaval.htm">http://csrc.nist.gov/cryptval/shs/shaval.htm</a> )	Pentium III 933 MHz processor w/ Windows 2000	April 2006
116	RSA Validation Certificate ( <a href="http://csrc.nist.gov/cryptval/dss/rsaval.html">http://csrc.nist.gov/cryptval/dss/rsaval.html</a> )	Pentium III 933 MHz w/ Windows XP	January 2006
149	Keyed-Hash Message Authentication Code (HMAC) Validation Certificate ( <a href="http://csrc.nist.gov/cryptval/mac/hmacval.html">http://csrc.nist.gov/cryptval/mac/hmacval.html</a> )	Pentium III 933 MHz w/ Windows XP	January 2006
155	Digital Signature Algorithm (DSA) Validation Certificate ( <a href="http://csrc.nist.gov/cryptval/dss/dsaval.htm">http://csrc.nist.gov/cryptval/dss/dsaval.htm</a> )	Pentium III 933 MHz w/ Windows XP	January 2006
165	Random Number Generator (RNG) Validation Certificate ( <a href="http://csrc.nist.gov/cryptval/rng/rngval.html">http://csrc.nist.gov/cryptval/rng/rngval.html</a> )	Pentium III 933 MHz w/ Windows XP	January 2006





State of West Virginia  
RFQ No. HSE01154  
Identity Management Service Offering



345	Advanced Encryption Standard Algorithm Validation Certificate ( <a href="http://csrc.nist.gov/cryptval/aes/aesval.html">http://csrc.nist.gov/cryptval/aes/aesval.html</a> )	Pentium III 933 MHz w/ Windows XP	January 2006
407	Triple DES Modes of Operation Validation Certificate ( <a href="http://csrc.nist.gov/cryptval/des/tripledesval.html">http://csrc.nist.gov/cryptval/des/tripledesval.html</a> )	Pentium III 933 MHz w/ Windows XP	January 2006
420	Secure Hash Standard (SHS) Validation Certificate ( <a href="http://csrc.nist.gov/cryptval/shs/shaval.htm">http://csrc.nist.gov/cryptval/shs/shaval.htm</a> )	Pentium III 933 MHz w/ Windows XP	January 2006

Listed on web site <http://csrc.nist.gov/cryptval>

Table 3-2 TecSec FIPS 140-2 Testing Certificates – Cryptographic Module

Certificate No.	Description (URL)	Platform/OS Tested	Date
687 FIPS 140-2	CKM <sup>®</sup> Cryptographic Module by TecSec Incorporated (When operated in FIPS Mode) ( <a href="http://csrc.nist.gov/cryptval/140-1/1401vend.htm">http://csrc.nist.gov/cryptval/140-1/1401vend.htm</a> )	Windows 2000 and Windows XP (in single user mode)	July 2006

Table 3-3 TecSec FIPS 140-2 Testing Certificates - Hardware

Certificate No.	Description (URL)	Date
1118	TecSec PIV Eagle Card- Contactless ( <a href="http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm">http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm</a> )	April 2009
1120	TecSec PIV Eagle Card -Contact by TecSec, Atmel, CPI Card Group and Athena Smartcard ( <a href="http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm">http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm</a> )	April 2009



State of West Virginia  
RFQ No. HSE01154  
Identity Management Service Offering



## FIPS 140-2 Validation Certificate



The National Institute of Standards  
and Technology of the United States  
of America



The Communications Security  
Establishment of the Government  
of Canada

Certificate No. 687

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; hereby validate the FIPS 140-2 testing results of the Cryptographic Module identified as:

### CKM® Cryptographic Module by TecSec Incorporated (When operated in FIPS mode)

in accordance with the Derived Test Requirements for FIPS 140-2, Security Requirements for Cryptographic Modules. FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting *Sensitive Information* (United States) or *Protected Information* (Canada) within computer and telecommunications systems (including voice systems).

Products which use the above identified cryptographic module may be labeled as complying with the requirements of FIPS 140-2 so long as the product, throughout its life cycle, continues to use the validated version of the cryptographic module as specified in this certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

This certificate includes details on the scope of conformance and validation authority signatures on the reverse.

TM: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S., or Canadian Governments





State of West Virginia  
RFQ No. HSE01154  
Identity Management Service Offering



FIPS 140-2 provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range and potential applications and environments in which cryptographic modules may be employed. The security requirements cover eleven areas related to the secure design and implementation of a cryptographic module. The scope of conformance achieved by the cryptographic modules as tested in the product identified as:

CKM® Cryptographic Module by TecSec Incorporated  
(Software Version: 2.0.0.11; Software)

COACT CAFE Laboratory, NVLAP Lab Code 200416-0 CRYPTIK Version 6.0			
and tested by the Cryptographic Module Testing accredited laboratory:			
is as follows:			
Cryptographic Module Specification:	Level 1	Cryptographic Module Ports and Interfaces:	Level 1
Roles, Services, and Authentication:	Level 1	Finite State Model:	Level 1
Physical Security: (Multi-Chip Standalone)	Level N/A	Cryptographic Key Management:	Level 1
EMI/EMC:	Level 1	Self-Tests:	Level 1
Design Assurance:	Level 1	Mitigation of Other Attacks:	Level N/A
Operational Environment:	Level 1	tested in the following configuration(s): Windows 2000 and Windows XP (in single user mode)	

The following FIPS approved Cryptographic Algorithms are used: AES (Certs. #345 and #379); Triple-DES (Certs. #407 and #422); SHA (Certs. #420 and #450); HMAC (Certs. #149 and #167); RNG (Certs. #165 and #181); RSA (Certs. #116 and #131); DSA (Certs. #155, #163, and #165)

The cryptographic module also contains the following non-FIPS approved algorithms: DES; Twofish; Blowfish; P-Square; RSA (key wrapping; key establishment methodology provides between 69 and 80 bits of encryption strength); Diffie-Hellman (key agreement; key establishment methodology provides between 56 and 80 bits of encryption strength); MD5; HMAC-MD5; CKM Key Construction

Overall Level Achieved: 1

Signed on behalf of the Government of the United States

Signature: [Signature]  
Dated: 14 July 2006

Chief, Computer Security Division  
National Institute of Standards and Technology

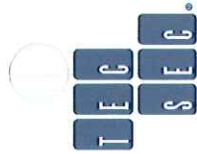
Signed on behalf of the Government of Canada

Signature: [Signature]  
Dated: 11 juillet 2006

Director, Industry Program Group  
Communications Security Establishment



State of West Virginia  
RFQ No. HSE01154  
Identity Management Service Offering



## FIPS 140-2 Validation Certificate



The National Institute of Standards  
and Technology of the United States  
of America



The Communications Security  
Establishment of the Government  
of Canada

Certificate No. 1118

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; hereby validate the FIPS 140-2 testing results of the Cryptographic Module identified as:

**TecSec PIV Eagle Card – Contactless by TecSec, Atmel,  
CPI Card Group and Athena Smartcard**

in accordance with the Derived Test Requirements for FIPS 140-2, Security Requirements for Cryptographic Modules. FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting *Sensitive Information* (United States) or *Protected Information* (Canada) within computer and telecommunications systems (including voice systems).

Products which use the above identified cryptographic module may be labeled as complying with the requirements of FIPS 140-2 so long as the product, throughout its life cycle, continues to use the validated version of the cryptographic module as specified in this certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

This certificate includes details on the scope of conformance and validation authority signatures on the reverse.

The A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S., or Canadian Governments.





State of West Virginia  
RFQ No. HSE01154  
Identity Management Service Offering



FIPS 140-2 provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range and potential applications and environments in which cryptographic modules may be employed. The security requirements cover eleven areas related to the secure design and implementation of a cryptographic module. The scope of conformance achieved by the cryptographic modules as tested in the product identified as:

TecSec PIV Eagle Card – Contactless by TecSec, Atmel, CPI Card Group and Athena Smartcard  
(Hardware Version: P/N Atmel AT90SC12872RCFT Revision M; Software Version: P/N TecSec Contactless PIV Applet Version 1.0 JCL;  
Firmware Version: P/N Athena ID Protect Duo Version 0107.7099.0105; Hardware)  
(PIV Card Application: Cert. #11)

InfoGard Laboratories, Inc., NVLAP Lab Code 100432-0  
CRYPTIK Version 7.0

and tested by the Cryptographic Module Testing accredited laboratory:  
is as follows:

Cryptographic Module Specification:	Level 3	Cryptographic Module Ports and Interfaces:	Level 3
Roles, Services, and Authentication:	Level 3	Finite State Model:	Level 3
Physical Security: (Single Chip)	Level 4	Cryptographic Key Management:	Level 3
EMI/EMC:	Level 3	Self-Tests:	Level 3
Design Assurance:	Level 3	Mitigation of Other Attacks:	Level N/A
Operational Environment:	Level N/A	tested in the following configuration(s):	N/A

The following FIPS approved Cryptographic Algorithms are used: Triple-DES (Cert. #598); Triple-DES MAC (Triple-DES Cert. #598, vendor affirmed); AES (Cert. #646); SHS (Cert. #680); RNG (Cert. #368); RSA (Cert. #296)

The cryptographic module also contains the following non-FIPS approved algorithms: RSA (key wrapping; key establishment methodology provides 80 or 112 bits of encryption strength)

Overall Level Achieved: 3

Signed on behalf of the Government of the United States

Signature: Doreen F. Doherty for W. Barker  
Dated: April 3, 2009

Chief, Computer Security Division  
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: [Signature]  
Dated: March 27, 2009

Director, Industry Program Group  
Communications Security Establishment Canada



State of West Virginia  
RFQ No. HSE01154  
Identity Management Service Offering



## FIPS 140-2 Validation Certificate



The National Institute of Standards  
and Technology of the United States  
of America



Certificate No. 1120



The Communications Security  
Establishment of the Government  
of Canada

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; hereby validate the FIPS 140-2 testing results of the Cryptographic Module identified as:

**TecSec PIV Eagle Card – Contact by TecSec, Atmel,  
CPI Card Group and Athena Smartcard**

in accordance with the Derived Test Requirements for FIPS 140-2, Security Requirements for Cryptographic Modules. FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting *Sensitive Information* (United States) or *Protected Information* (Canada) within computer and telecommunications systems (including voice systems).

Products which use the above identified cryptographic module may be labeled as complying with the requirements of FIPS 140-2 so long as the product, throughout its life cycle, continues to use the validated version of the cryptographic module as specified in this certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

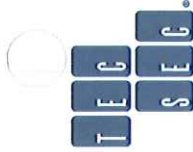
This certificate includes details on the scope of conformance and validation authority signatures on the reverse.

TM: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S., or Canadian Governments





State of West Virginia  
RFQ No. HSE01154  
Identity Management Service Offering



FIPS 140-2 provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range and potential applications and environments in which cryptographic modules may be employed. The security requirements cover eleven areas related to the secure design and implementation of a cryptographic module. The scope of conformance achieved by the cryptographic modules as tested in the product identified as:

*TecSec PIV Eagle Card – Contact by TecSec, Atmel, CPI Card Group and Athena Smartcard  
(Hardware Version: P/N Atmel AT90SC144144CT Revision G; Software Version: P/N TecSec Contact PIV Applet Version 1.01 JCT;  
Firmware Version: P/N Athena IDProtect XL Version 010A.7204.0004; Hardware)  
(PIV Card Application: Cert. #11)*

*InfoGard Laboratories, Inc., NVLAP Lab Code 100432-0  
CRYPTIK Version 7.0*

and tested by the Cryptographic Module Testing accredited laboratory:  
is as follows:

Cryptographic Module Specification:	Level 3	Cryptographic Module Ports and Interfaces:	Level 2
Roles, Services, and Authentication:	Level 3	Finite State Model:	Level 2
Physical Security: (Single Chip)	Level 4	Cryptographic Key Management:	Level 3
EMI/EMC:	Level 3	Self-Tests:	Level 2
Design Assurance:	Level 3	Mitigation of Other Attacks:	Level 2
Operational Environment:	Level N/A	tested in the following configuration(s):	N/A

The following FIPS approved Cryptographic Algorithms are used: Triple-DES (Cert. #592); Triple-DES MAC (Triple-DES Cert. #592, vendor affirmed); AES (Cert. #639); SHS (Cert. #674); RNG (Cert. #364); RSA (Cert. #292)

The cryptographic module also contains the following non-FIPS approved algorithms: RSA (key wrapping; key establishment methodology provides 80 or 112 bits of encryption strength)

**Overall Level Achieved: 2**

Signed on behalf of the Government of the United States

Signature: Don F. Dodson R. W. Barker  
Dated: April 3, 2009

Chief, Computer Security Division  
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: [Signature]  
Dated: March 31, 2009

Director, Industry Program Group  
Communications Security Establishment Canada



## Mandatory Specification Signature Page

I certify that we will meet all the mandatory deliverables/specifications of this Request for Proposal upon the award of the contract. Additionally, I agree to provide any additional documentation deemed necessary by the State of West Virginia to demonstrate compliance with said mandatory specifications.

### **TecSec Services , Inc.**

(Company)

  
Michael S. Friedman, VP Finance & Administration

(Representative Name, Title)

571-299-4105 / 571-299-4101

(Contact Phone and Fax Number)

September 7, 2011

(Date)





### **3 Attachment C: Cost Sheet/Revised Under Separate Cover**

Submitted under separate cover and sealed per bid instructions.



## **4 Attachment D: West Virginia State –Wide Citizens Benefit Card (CBC)**

### **Business Case**

The key principle expressed in “West Virginia Request for Proposal HSE 01154” is the unquestioned need to develop an affordable, high confidence, multi-use, biometric based trusted identity credential. In simple terms, what is needed is an affordable “Identity of Merit” credential that can be used safely by all citizens; one capable of the multiple secure electronic independent functions necessary for eGovernment, eCommerce, and eHealth. This need for high quality credentialing of state residents is becoming essential to meet the emerging national and international strategy of seamless and secure electronic commerce, as well as the efficient execution of governments’ roles and responsibilities. The realities of reduced state revenues, aging and often inflexible technical infrastructures, and the increased non-funded federal interest in developing counter-terrorist capabilities across the nation, have challenged the state’s ability to provide such a capability for its citizens.

The current practice of issuing a single identification card and security PIN for every unique need is no longer practical or affordable. TecSec has engineered and certified an innovative multifunction credential using our Armored Card™ which we call the Citizen’s Benefit Card (CBC). The foundation of an “Identity of Merit” is an individual’s biometric data, coupled with personal biographic information obtained from accepted records and documents. These are unique validated source documents such as a passport, birth certificate, Social Security card, or other approved designated forms of identification. The CBC can simultaneously support a variety of Attribute Containers™, each able to manage its own data without interference from the others. The biometric data, once captured, is electronically attached to the CBC, to establish a tamper proof, high confidence identification of an individual for use in transactions involving personal identification, benefits, state licenses, access control, and commerce.

The TecSec West Virginia CBC concept is a potentially large revenue generation program for the State. The program meets all of the West Virginia electronic identity requirements without the expense of the state developing and managing multiple complex electronic systems. As seen in the business case below, the State will be leasing Attribute Container™ space to different types of organizations across the State, Federal Government, and commercial world. As those relationships are developed, the citizen will be able to choose from a menu of attributes to be downloaded to an individual’s CBC, some at his cost and others at no direct cost to him.

### **The Business Case**

Today each citizen has multiple ID cards, e.g. a driver’s license, state ID cards, Medicare/Medicaid ID cards, physical access cards etc. Issuing multiple cards has the burden and expense of managing the relatively short life cycle of multiple card programs and the process of verifying the identity of the citizen each time a card is issued. With cost reduction in mind we begin with the notion of a single identity card supporting multiple Attribute Containers™ This single identity card is defined as the “Citizen’s Benefits Card” (CBC) which would potentially





State of West Virginia  
RFQ No. HSE01154  
Identity Management Service Offering



serve as a personal identity credential, EBT card, access card, etc. With cost avoidance in mind, our belief is that we must have a clean start, one with a high level of integrity, rather than relying on some of the existing databases such as the driver's license database, which has been shown by the National Association of State Chief Information Officers (NASCIO) as well as the American Association of Motor Vehicle Administrators (AAMVA) to contain significant errors in every state. We are starting with an identity event instead of building on top of the prior license database. NASCIO has already accepted that a driver's license was only meant to allow a person the right to drive a car, and not to be relied upon as a personal identification device. In addition, each CBC would have the citizen's biometric template bound to it. This feature would have the potential of supporting the reduction of fraud in several programs such as Medicaid, Medicare, WIC, etc. The feature would also enable cross checking between states if necessary. The single card, multiple application solution, greatly reduces fraud, eliminates duplication, and was found to have significant cost savings during the three year study done for the State of Connecticut.

In West Virginia, individual cards are issued for the following programs:

PROGRAM
Dept. of Health and Human Services
Food Stamps (Agriculture)
Families
Children
Adults
Public Healthcare
Long Term Care (State insurance)
Cash Assistance (State)
Adults
Children
Medicare Premium Assistance (State insurance)
Non Medical Emergency Transportation (State)
Childcare and Development Fund Subsidies
School Programs (State)
Clothing allowance (during SCA season only)
Food (Breakfast, Lunch & Nutrition) Programs
Low Income Energy Assistance Program (LIEAP) (State)
Medicaid for Children and Pregnant Women (Agriculture)
West Virginia Children's Health Insurance Program (WVCHIP) (State)
Woman and Infant Children (WIC)
Medicare
Medicaid
First Responders



State of West Virginia  
RFQ No. HSE01154  
Identity Management Service Offering



PROGRAM
State Employees
Drivers License
Other Licenses

The dollar cost of the benefits associated with the programs above represents nearly \$2B annually. We understand from federal statistics that nearly 20% of the total annual appropriation for medical benefits is spent on fraudulent or unaccounted for cases. In the case of West Virginia, that translates to ~\$400M/year in questionable payments. Fraud poses a loss of valuable state resources. It is widely accepted that the cost of issuing multiple cards to improve accountability is not efficient; therefore, many identification initiatives go unfunded both at the state and federal level.

From these issues alone, it is relatively easy to see that significant savings may be realized by West Virginia through:

- Issuing a single CBC (approximately 1.4M cards) with the ability to support multiple independent secure attributes/applications;
- Correctly identifying and attributing benefits to qualified individuals, organizations, and providers (thus reducing the potential for and the overall incidence of fraud); and
- Reducing the time and resources required to establish an identity while at the same time enhancing the likelihood that an individual is who he claims to be.
- Reducing the cost of supporting multiple infrastructures for individually issued cards.
- Improved privacy and security for the citizens' transactions.
- **Improved convenience for the citizens.**

Each citizen would be issued a single CBC that supports multiple applications, stored in individual encrypted Attribute Containers<sup>™</sup> which enables the card to be used for multiple independent purposes. Each Attribute Container<sup>™</sup> would likely have a different owning agency, allowing existing organizational and contractual relationships to be maintained, and all data is constrained to the existing owner.

The burden of having to issue a separate card for each application owner (e.g. state or federal agency), in order to maintain information privacy and control is removed. The citizen starts with a highly reliable, secure credential that can provide multiple physical or logical access capabilities.

With TecSec's advanced card, one can gain all these benefits at a price well below that of multiple single application cards of the past. All the information on the new generation of TecSec's multi-application capable cards is secure, because each Attribute Container<sup>™</sup> is independently and cryptographically maintained by the application owner within its allocated storage space; only those with the appropriate permissions have access to the information.

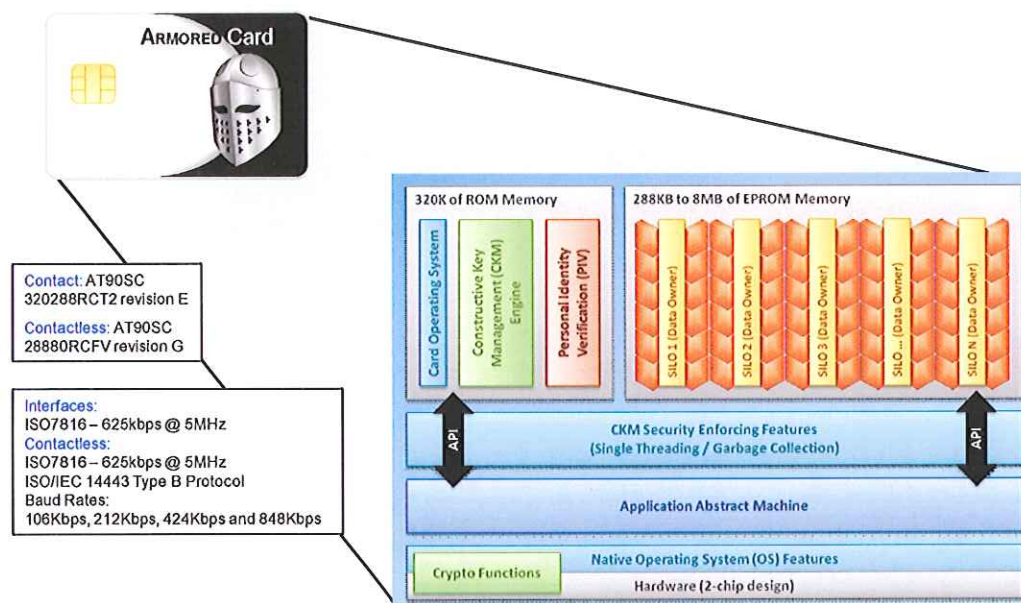




Figure 9 is a graphic description of the CBC including its internal operating schema such as card operating system, personal identification, Attribute Container™ and cryptography functions.

The CBC has the appearance of a credit card but contains two silicon chips. One chip is used when the card is physically inserted into a reader (“contact mode”) and one for when the card is within range of a reader (“contactless mode”).

## Card Architecture Overview



**Figure 9 Armored Card Architecture Overview**

Most significantly the opportunity exists for West Virginia to generate income, over and above any actual cost associated with the CBC, in partnership with TecSec. The income will be derived through the leasing of Attribute Container™ repository space, by the kilobyte, on the CBC to Federal Agencies, State Organizations, and the private business community all of whom have a requirement to credential their users/participants. Some of those organizations potentially include:

- The Centers for Medicare and Medicaid Services (CMS)
- Veterans Administration, Veterans Health Administration
- Department of Transportation
- Department of Agriculture
- Department of Homeland Security



State of West Virginia  
RFQ No. HSE01154  
Identity Management Service Offering



- Security/Immigration ID systems (Green cards, etc)
- TSA, TWIC, Registered Traveler, etc.
- FEMA (FRAC)
- Department of State (Passport and Identification Programs)
- Health Insurance Companies
- Banks and Financial Institutions
- Credit Card Companies
- Campus ID Programs
- Companies whose personnel must respond to disaster/emergency situations.

Commercial interest in leasing space on the CBC is not speculative. TecSec is aware of two formal expressions of interest:

- Alleghany Power suggested at a National Capital meeting chaired by former WV Secretary Spears that it wished to have its personnel's attributes in a first responder repository for which they would pay the state.
- Exxon Oil suggested at the same meeting that it would like its personnel to have a CBC. Their thinking was that if the State conducts identity assurance and background checks including such things as immigration checks, it would be far cheaper for them to rely on the Identity of Merit established by the State than to conduct those checks themselves.

TecSec has also received many more informal expressions of interest ranging from Wal-Mart, whose initial interest lies in leveraging its participation in the Food Stamps program to the Retail Merchants Association which wants to use the card as a payment vehicle.

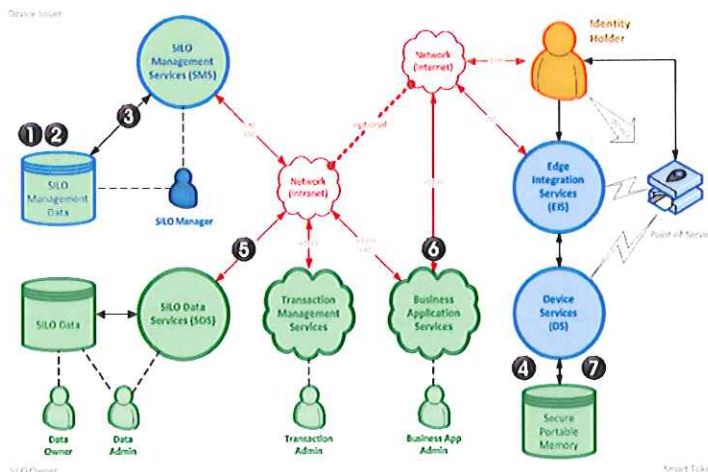
Figure 10 describes how "Data Owners" link to the CBC card. It is important to note that government agencies and commercial users establish a secure electronic link to the CBC's Trusted Identity through the use of the SILOS<sup>®</sup> Manager. The Data Owners will be authorized to place data on the State owned CBC. The data owner is capable of reading only the Attribute Containers<sup>™</sup> that it leases and is not able to read other Attribute Containers<sup>™</sup> that may be on the card. To protect the privacy of the individual citizen, the State of West Virginia will only be able to decrypt Attribute Containers<sup>™</sup> that it owns and not the entire data on the card. The data owner will be charged an annual fee for each Attribute Container<sup>™</sup> utilized. It is the lease of Attribute Containers<sup>™</sup> that provides the revenue necessary to generate the annual financial return to West Virginia.





## Linking Data Owners to the Trusted Identity Platform

- 1 The Data Owner registers their SILO Template with SILO Management Services (\$'s) ... The SILO Template defines the amount of SILO space needed.
- 2 The Data Owner reserves SILO space on a set of Devices (\$'s)
- 3 When the Identity Holder activates their Device, SILO Management Services check to see if there are any SILO reservations for that Device
- 4 If a reservation is found, SILO Management Services create and initialize a SILO using the registered SILO Template (\$'s)
- 5 SILO Management Services send the key information to SILO Data Services so that the Data Owner can take control of the SILO
- 6 The Data Owner prompts the Identity Holder to provide any additional information needed to personalize the SILO
- 7 SILO Data Services takes control of the SILO on the Device and writes Data (e.g. credentials)



### Notes on the Figure:

- SILO Management Services manage definition of SILO Templates and Reservations
- Transaction Management Services process any financial transactions when \$'s are used
- Business Application Services can communicate with SILO Data and SILO Data Services

Figure 10 Data Owners Linked to the Trusted Identity Platform

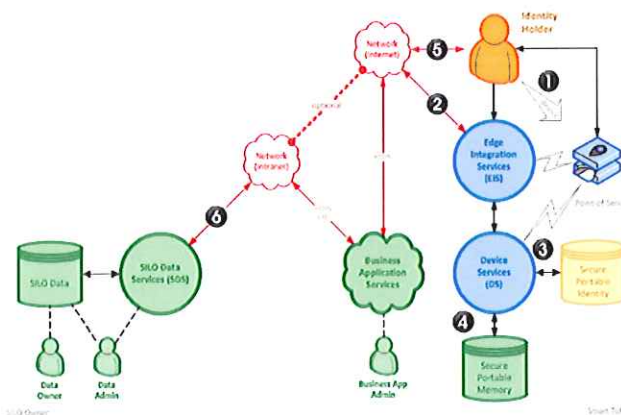
Figure 11 outlines the steps enabling a West Virginia citizen to use the CBC in eGovernment, eHealth, and eCommerce applications. This capability is the central value of the CBC credential's utility that is provided to the individual State citizen. Routine use by the citizen generates the state, federal, and commercial demand for Attribute Containers<sup>TM</sup>.



## Using Data through the Trusted Identity Platform



- 1 Login: when an Identity Holder wants to use a Business Application, the Identity Holder presents their Device to gain access to services
- 2 Login: the Business Application recognizes the Device, and prompts the Identity Holder to release the Data on their Device
- 3 Login: the Identity Holder authenticates to the Device and the Identity Holder's authentication information is securely matched against the information stored on the Device
- 4 After authentication, the Business Application retrieves Data from the SILO on the user's Device
- 5 The Business Application grants appropriate privileges to the Identity Holder. The Identity Holder interacts with the Business Application directly to use services
- 6 Optional: The Business Application may trigger updates to the Identity Holder's data in the SILO on their Device, if needed (e.g. expiration, revocation, privilege update, etc.)



TecSec Incorporated  
Copyright 2011 All Rights Reserved

Date:  
8

Figure 11 Using Data through the Trusted Identity Platform

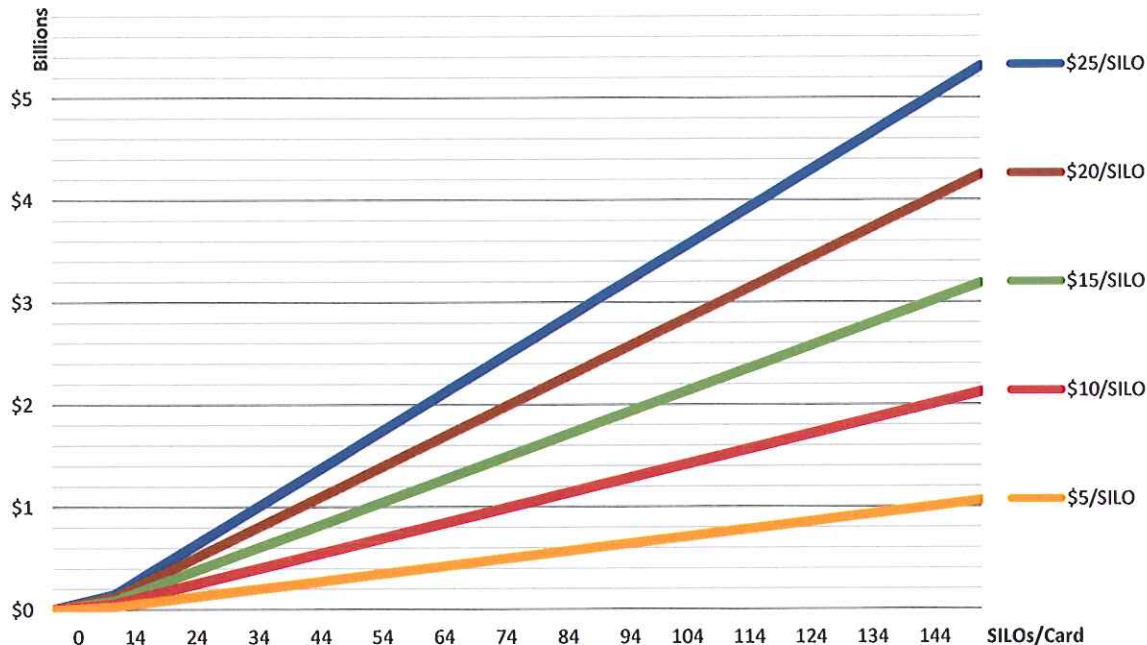
## Revenue Model

The following charts show the various revenue possibilities to West Virginia. Specific financial metrics will need to be determined in conjunction with the State of West Virginia, balancing the desire to produce revenue against the willingness of the customer organizations to pay. Preliminary discussions with several Federal Agencies suggest that a charge of approximately \$5-\$10 per kilobyte of space per year will be acceptable because such a fee would significantly reduce the program costs currently being experienced. TecSec anticipates that the average Attribute Container™ will require 2KB of space.





## SILOS Revenue \*



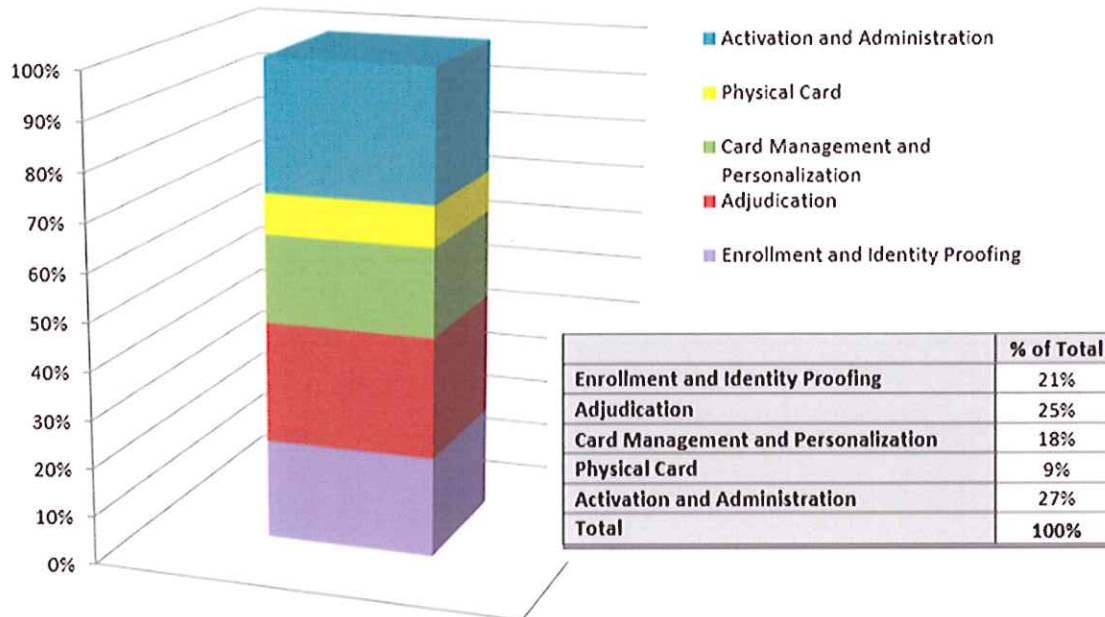
\* 288K Armored Card  
2K/SILO = 144 Total SILOs/Card  
Card Population of 1,475,218 [Licensed Drivers over 16]

**Figure 12 Potential Annual Revenue from Attribute Container™**

Figure 12 shows the potential annual revenue attainable through Attribute Container™ leases. The current Armored Card™ suggested for use as the CBC has 288k of available space for Attribute Containers™. Future TecSec CBC cards already designed will contain 8 Mbs of memory which greatly expands the available space for Attribute Containers™ leasing. TecSec believes that the combination of memory space and potential demand for Attribute Containers™ produces an extraordinary financial opportunity for the State of West Virginia. TecSec will work with West Virginia to develop marketing plans, policies, and procedures for the CBC program.



## Typical Card Program Allocation



**Figure 13 Typical Card Program Allocation**

Figure 13 is a breakdown of the estimated average cost to fully administer and issue a smart card program. Note that the cost of the card is a small portion of the overall program cost. The value of the CBC program is that the citizen's "Identity of Merit" is obtained once and the resultant credential is used multiple ways. Rather than issue a new card, the CBC is populated with Attribute Containers™ by using the card for numerous functions, the costs of Enrolling and Identity Verification, Adjudication, Card Management, Personalization, and Activation become one-time nonrecurring costs for the life of the card. By using all 25 WV DMV's, the TecSec business model will have the entire 1,475,000 CBC cards issued within a 5 year period.





Making Identity as a Service Affordable  
... the value of PIV with CKM

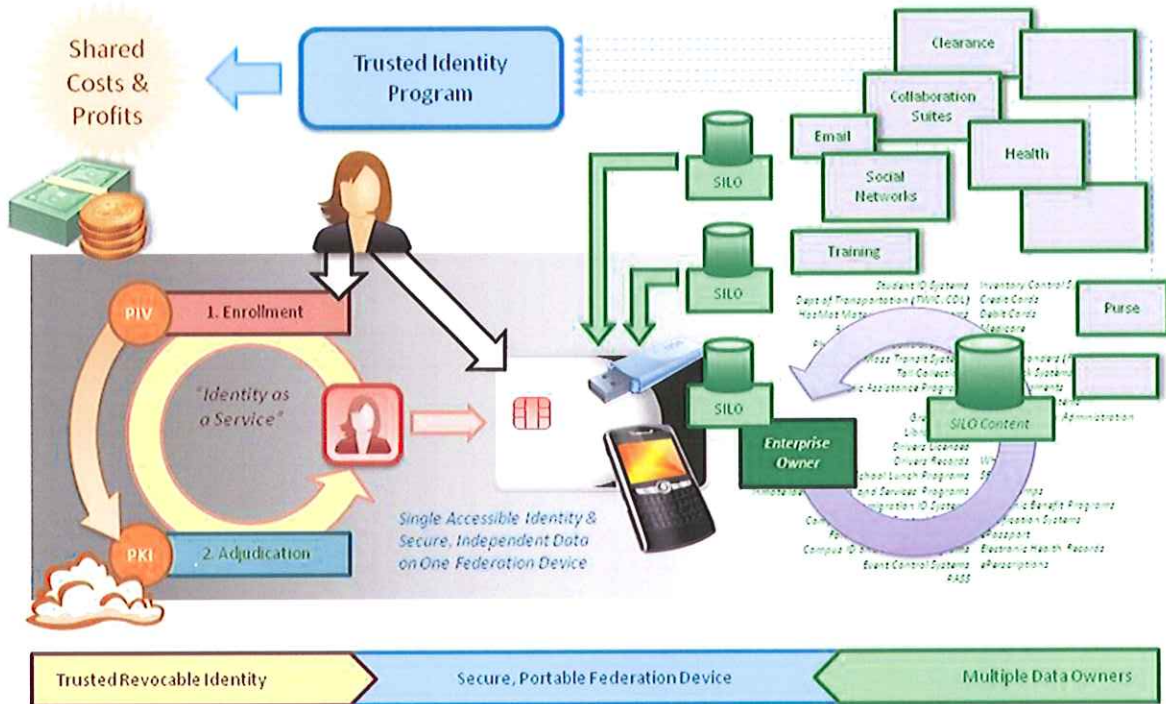


Figure 14 Making Identity as a Service Affordable

## TECSEC PROPOSES TO THE STATE OF WEST VIRGINIA

- To design, develop, and deliver to the West Virginia government a secure, state of the art, PIV-I card system meeting all federal and state security and interoperability standards.
- Provide the hardware and software necessary to issue WVCBC cards at West Virginia DMV locations and/or other locations deemed by the state as card issuing facilities.
- Operate an independent Quality Control system to ensure a continued trouble free card program. Solve technical problems when encountered.
- Provide blank TecSec Armored Cards™ and miscellaneous supplies sufficient to issue one card to each qualified citizen. Cards will be issued over the agreed life of the program.
- To establish, operate, and maintain a data base for the secure repository of biometric characteristics. This capability prevents the multiple issuances of identity cards to the same person. This system will include, for security purposes, a real time backup database located at a geographically separate facility from the main database.



- To support the marketing, leasing, and maintaining a secure space on the card to federal, state, local, and commercial organizations legitimately needing PIV-I services using the TecSec patented CKM<sup>®</sup> encryption system.
- To provide an electronic billing system for the sale of each Attribute Containers<sup>™</sup>.
- To develop a cost structure that provides for the sharing of revenue between the State and TecSec after recovery of program costs.
- To develop an equitable structure for sharing of the benefits of fraud reduction between the State and TecSec.

**During the Implementation of this Program TecSec Anticipates the State of West Virginia to:**

- Assume ownership of WVCBC card program.
- Issue Armored Cards<sup>™</sup> using West Virginia DMV employees and facilities or equivalent.
- Provide appropriate executive orders, regulations, and legislation to require state agency migration to the use of the card.
- Support back-end integration with legacy systems within the State. Market WVCBC concept to the citizens of West Virginia to encourage the use of the card.
- Foster public support and confidence in the security and privacy of the system.
- Market the CBC concept to all likely federal, state, local, and commercial entities.
- Implementation of card readers and a collaborative process with the stakeholders' business process, which supports the use of this card's physical and logical capabilities.
- Realize savings from reduced card issuing expenses.

## **SUMMARY**

It is the intent of TecSec to assist West Virginia to implement a State-wide CBC program. We believe that a large portion of the necessary funding can be obtained through pre-lease of the space on the CBC to Federal Agencies, e.g. VA, Agriculture Department, HHS/CMS, Homeland Security, and from other Federal and commercial sources. Grant funding to improve health care or improve health care distribution processes and Homeland Security programs, such as counter terrorism initiatives, Real ID support, and implementation of HSPD-20, which mandates credentials for First Responders, should be available and accessible to the program. Assuming a public/private partnership between the state and TecSec for this program is established, TecSec will work with state planners to actively identify, write, and submit requirements for new grants to aid in defraying program costs.

As a model and leader in the field of biometrics, the State of West Virginia should be the first to embrace this innovative solution to increasing identity requirements and shrinking state revenues. TecSec looks forward to establishing a public/private partnership with West Virginia to launch the West Virginia Citizens Benefit Card program.





## 5 Signed Addendums

EXHIBIT 10

REQUISITION NO: HSE01154

ADDENDUM ACKNOWLEDGEMENT

I HEREBY ACKNOWLEDGE RECEIPT OF THE FOLLOWING CHECKED  
ADDENDUM(S) AND HAVE MADE THE NECESSARY REVISIONS TO MY  
PROPOSAL, PLANS AND/OR SPECIFICATION, ETC.

ADDENDUM NO.'S:

NO. 1 ..... ✓

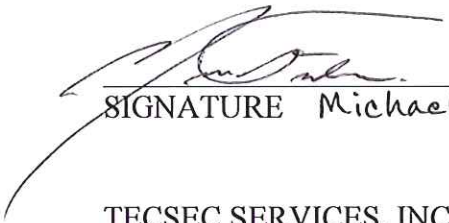
NO. 2 ..... ✓

NO. 3 ..... ✓

NO. 4 .....

NO. 5 .....

I UNDERSTAND THAT FAILURE TO CONFIRM THE RECEIPT OF THE  
ADDENDUM(S) MAY BE CAUSE FOR REJECTION OF BIDS. VENDOR  
MUST CLEARLY UNDERSTAND 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.

  
SIGNATURE Michael FRIEDMAN

TECSEC SERVICES, INCORPORATED  
COMPANY

September 7, 2011  
DATE





State of West Virginia  
Department of Administration  
Purchasing Division  
2019 Washington Street East  
Post Office Box 50130  
Charleston, WV 25305-0130

## Request for Quotation

RFQ NUMBER

HSE01154

PAGE

1

ADDRESS CORRESPONDENCE TO ATTENTION OF:

TARA LYLE  
304-558-2544

V  
E  
N  
D  
O  
R

\*321134852 571-299-4105  
TECSEC SERVICES INC  
12950 WORLDGATE DR STE 100  
HERNDON VA 20170

S  
H  
I  
P  
T  
O

HOMELAND SECURITY & EMERGENCY  
MANAGEMENT, DIVISION OF  
BUILDING 1, ROOM EB80  
1900 KANAWHA BOULEVARD, EAST  
CHARLESTON, WV  
25305-0360 304-558-5380

DATE PRINTED	TERMS OF SALE	SHIP VIA	F.O.B.	FREIGHT TERMS		
07/19/2011						
BID OPENING DATE: 08/16/2011		BID OPENING TIME 01:30PM				
LINE	QUANTITY	UOP	CAT. NO.	ITEM NUMBER	UNIT PRICE	AMOUNT
ADDENDUM NO. 1						
1. TO CLARIFY THE MANDATORY PRE-BID MEETING. THE MEETING IS SCHEDULED FOR MONDAY, JULY 25, 2011 AT 10:00 AM IN THE PURCHASING DIVISION CONFERENCE ROOM LOCATED AT 2019 WASHINGTON STREET, EAST CHARLESTON, WV 25305.						
2. ADDENDUM ACKNOWLEDGEMENT IS ATTACHED. THIS DOCUMENT SHOULD BE SIGNED AND RETURNED WITH YOUR BID. FAILURE TO SIGN AND RETURN MAY RESULT IN DISQUALIFICATION OF YOUR BID.						
0001	1	LS		655-78		
IDENTIFICATION SYSTEM						
***** THIS IS THE END OF RFQ HSE01154 ***** TOTAL:						
SEE REVERSE SIDE FOR TERMS AND CONDITIONS						
SIGNATURE			TELEPHONE		DATE	
TITLE		FEIN		ADDRESS CHANGES TO BE NOTED ABOVE		

WHEN RESPONDING TO RFQ, INSERT NAME AND ADDRESS IN SPACE ABOVE LABELED 'VENDOR'



State of West Virginia  
Department of Administration  
Purchasing Division  
2019 Washington Street East  
Post Office Box 50130  
Charleston, WV 25305-0130

## Request for Quotation

RFQ NUMBER

HSE01154

PAGE

1

ADDRESS CORRESPONDENCE TO ATTENTION OF:

TARA LYLE  
304-558-2544

\*321134852 571-299-4105  
TECSEC SERVICES INC  
12950 WORLDGATE DR STE 100

HERNDON VA 20170

HOMELAND SECURITY & EMERGENCY  
MANAGEMENT, DIVISION OF  
BUILDING 1, ROOM EB80  
1900 KANAWHA BOULEVARD, EAST  
CHARLESTON, WV  
25305-0360 304-558-5380

DATE PRINTED	TERMS OF SALE	SHIP VIA	F.O.B.	FREIGHT TERMS
08/12/2011				

BID OPENING DATE: 08/30/2011 BID OPENING TIME 01:30PM

LINE	QUANTITY	UOP	CAT. NO.	ITEM NUMBER	UNIT PRICE	AMOUNT
ADDENDUM NO. 2						
1. TO MOVE THE BID OPENING DATE FROM 08/16/2011 TO 08/30/2011.						
2. MANDATORY PRE-BID SIGN-IN SHEETS ATTACHED.						
3. ADDENDUM ACKNOWLEDGEMENT IS ATTACHED. THIS DOCUMENT SHOULD BE SIGNED AND RETURNED WITH YOUR BID. FAILURE TO SIGN AND RETURN MAY RESULT IN DISQUALIFICATION OF YOUR BID.						
END OF ADDENDUM NO. 2						
0001	1	LS		655-78		
IDENTIFICATION SYSTEM						
***** THIS IS THE END OF RFQ HSE01154 ***** TOTAL:						
RECEIVED AUG 15 2011 BY: _____						

SEE REVERSE SIDE FOR TERMS AND CONDITIONS

SIGNATURE	TELEPHONE	DATE
TITLE	FEIN	ADDRESS CHANGES TO BE NOTED ABOVE

WHEN RESPONDING TO RFQ, INSERT NAME AND ADDRESS IN SPACE ABOVE LABELED 'VENDOR'





State of West Virginia  
Department of Administration  
Purchasing Division  
2019 Washington Street East  
Post Office Box 50130  
Charleston, WV 25305-0130

## Request for Quotation

RFQ NUMBER

HSE01154

PAGE

1

ADDRESS CORRESPONDENCE TO ATTENTION OF:

TARA LYLE

304-558-2544

\*321134852 571-299-4105

TECSEC SERVICES INC

12950 WORLDGATE DR STE 100

HERNDON VA 20170

HOMELAND SECURITY & EMERGENCY  
MANAGEMENT, DIVISION OF  
BUILDING 1, ROOM EB80  
1900 KANAWHA BOULEVARD, EAST  
CHARLESTON, WV  
25305-0360 304-558-5380

DATE PRINTED	TERMS OF SALE	SHIP VIA	F.O.B.	FREIGHT TERMS
08/19/2011				

BID OPENING DATE:

09/07/2011

BID OPENING TIME 01:30PM

LINE	QUANTITY	UOP	CAT NO.	ITEM NUMBER	UNIT PRICE	AMOUNT
ADDENDUM NO. 3						
1. QUESTIONS AND ANSWERS ARE ATTACHED.						
2. TO MOVE THE BID OPENING FROM 08/30/2011 TO						
09/07/2011.						
3. REVISED ATTACHMENT A ATTACHED.						
4. REVISED ATTACHMENT C ATTACHED.						
5. ADDENDUM ACKNOWLEDGEMENT IS ATTACHED. THIS						
DOCUMENT SHOULD BE SIGNED AND RETURNED WITH YOUR						
BID. FAILURE TO SIGN AND RETURN MAY RESULT						
IN DISQUALIFICATION OF YOUR BID.						
END OF ADDENDUM NO. 3						
0001	1	LS		655-78		
IDENTIFICATION SYSTEM						
***** THIS IS THE END OF RFQ HSE01154 ***** TOTAL:						

SEE REVERSE SIDE FOR TERMS AND CONDITIONS

SIGNATURE	TELEPHONE	DATE
TITLE	FEIN	ADDRESS CHANGES TO BE NOTED ABOVE

WHEN RESPONDING TO RFQ, INSERT NAME AND ADDRESS IN SPACE ABOVE LABELED 'VENDOR'



WV-96  
Rev. 10/07

# AGREEMENT ADDENDUM

In the event of conflict between this addendum and the agreement, this addendum shall control:

1. **DISPUTES** - Any references in the agreement to arbitration or to the jurisdiction of any court are hereby deleted. Disputes arising out of the agreement shall be presented to the West Virginia Court of Claims.
2. **HOLD HARMLESS** - Any clause requiring the Agency to indemnify or hold harmless any party is hereby deleted in its entirety.
3. **GOVERNING LAW** - The agreement shall be governed by the laws of the State of West Virginia. This provision replaces any references to any other State's governing law.
4. **TAXES** - Provisions in the agreement requiring the Agency to pay taxes are deleted. As a State entity, the Agency is exempt from Federal, State, and local taxes and will not pay taxes for any Vendor including individuals, nor will the Agency file any tax returns or reports on behalf of Vendor or any other party.
5. **PAYMENT** - Any references to prepayment are deleted. Payment will be in arrears.
6. **INTEREST** - Should the agreement include a provision for interest on late payments, the Agency agrees to pay the maximum legal rate under West Virginia law. All other references to interest or late charges are deleted.
7. **RECOUPMENT** - Any language in the agreement waiving the Agency's right to set-off, counterclaim, recoupment, or other defense is hereby deleted.
8. **FISCAL YEAR FUNDING** - Service performed under the agreement may be continued in succeeding fiscal years for the term of the agreement, contingent upon funds being appropriated by the Legislature or otherwise being available for this service. In the event funds are not appropriated or otherwise available for this service, the agreement shall terminate without penalty on June 30. After that date, the agreement becomes of no effect and is null and void. However, the Agency agrees to use its best efforts to have the amounts contemplated under the agreement included in its budget. Non-appropriation or non-funding shall not be considered an event of default.
9. **STATUTE OF LIMITATION** - Any clauses limiting the time in which the Agency may bring suit against the Vendor, lessor, individual, or any other party are deleted.
10. **SIMILAR SERVICES** - Any provisions limiting the Agency's right to obtain similar services or equipment in the event of default or non-funding during the term of the agreement are hereby deleted.
11. **ATTORNEY FEES** - The Agency recognizes an obligation to pay attorney's fees or costs only when assessed by a court of competent jurisdiction. Any other provision is invalid and considered null and void.
12. **ASSIGNMENT** - Notwithstanding any clause to the contrary, the Agency reserves the right to assign the agreement to another State of West Virginia agency, board or commission upon thirty (30) days written notice to the Vendor and Vendor shall obtain the written consent of Agency prior to assigning the agreement.
13. **LIMITATION OF LIABILITY** - The Agency, as a State entity, cannot agree to assume the potential liability of a Vendor. Accordingly, any provision limiting the Vendor's liability for direct damages to a certain dollar amount or to the amount of the agreement is hereby deleted. Limitations on special, incidental or consequential damages are acceptable. In addition, any limitation is null and void to the extent that it precludes any action for injury to persons or for damages to personal property.
14. **RIGHT TO TERMINATE** - Agency shall have the right to terminate the agreement upon thirty (30) days written notice to Vendor. Agency agrees to pay Vendor for services rendered or goods received prior to the effective date of termination.
15. **TERMINATION CHARGES** - Any provision requiring the Agency to pay a fixed amount or liquidated damages upon termination of the agreement is hereby deleted. The Agency may only agree to reimburse a Vendor for actual costs incurred or losses sustained during the current fiscal year due to wrongful termination by the Agency prior to the end of any current agreement term.
16. **RENEWAL** - Any reference to automatic renewal is hereby deleted. The agreement may be renewed only upon mutual written agreement of the parties.
17. **INSURANCE** - Any provision requiring the Agency to insure equipment or property of any kind and name the Vendor as beneficiary or as an additional insured is hereby deleted.
18. **RIGHT TO NOTICE** - Any provision for repossession of equipment without notice is hereby deleted. However, the Agency does recognize a right of repossession with notice.
19. **ACCELERATION** - Any reference to acceleration of payments in the event of default or non-funding is hereby deleted.
20. **CONFIDENTIALITY** - Any provision regarding confidentiality of the terms and conditions of the agreement is hereby deleted. State contracts are public records under the West Virginia Freedom of Information Act.
21. **AMENDMENTS** - All amendments, modifications, alterations or changes to the agreement shall be in writing and signed by both parties. No amendment, modification, alteration or change may be made to this addendum without the express written approval of the Purchasing Division and the Attorney General.

ACCEPTED BY:

STATE OF WEST VIRGINIA

Spending Unit: \_\_\_\_\_

Signed: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

VENDOR

Company Name: TECSEC SERVICES, INC.

Signed: \_\_\_\_\_

Title: VP - FINANCE & Administration

Date: 2 September 2011



RFQ No. HSE01154STATE OF WEST VIRGINIA  
Purchasing Division**PURCHASING AFFIDAVIT**

West Virginia Code §5A-3-10a states: No contract or renewal of any contract may be awarded by the state or any of its political subdivisions to any vendor or prospective vendor when the vendor or prospective vendor or a related party to the vendor or prospective vendor is a debtor and the debt owed is an amount greater than one thousand dollars in the aggregate.

**DEFINITIONS:**

"Debt" means any assessment, premium, penalty, fine, tax or other amount of money owed to the state or any of its political subdivisions because of a judgment, fine, permit violation, license assessment, defaulted workers' compensation premium, penalty or other assessment presently delinquent or due and required to be paid to the state or any of its political subdivisions, including any interest or additional penalties accrued thereon.

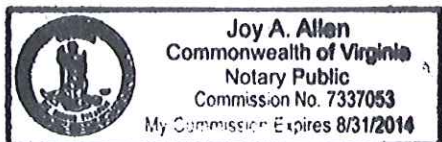
"Debtor" means any individual, corporation, partnership, association, limited liability company or any other form or business association owing a debt to the state or any of its political subdivisions. "Political subdivision" means any county commission; municipality; county board of education; any instrumentality established by a county or municipality; any separate corporation or instrumentality established by one or more counties or municipalities, as permitted by law; or any public body charged by law with the performance of a government function or whose jurisdiction is coextensive with one or more counties or municipalities. "Related party" means a party, whether an individual, corporation, partnership, association, limited liability company or any other form or business association or other entity whatsoever, related to any vendor by blood, marriage, ownership or contract through which the party has a relationship of ownership or other interest with the vendor so that the party will actually or by effect receive or control a portion of the benefit, profit or other consideration from performance of a vendor contract with the party receiving an amount that meets or exceeds five percent of the total contract amount.

**EXCEPTION:** The prohibition of this section does not apply where a vendor has contested any tax administered pursuant to chapter eleven of this code, workers' compensation premium, permit fee or environmental fee or assessment and the matter has not become final or where the vendor has entered into a payment plan or agreement and the vendor is not in default of any of the provisions of such plan or agreement.

Under penalty of law for false swearing (*West Virginia Code §61-5-3*), it is hereby certified that the vendor affirms and acknowledges the information in this affidavit and is in compliance with the requirements as stated.

**WITNESS THE FOLLOWING SIGNATURE**Vendor's Name: TECSEC SERVICES, INCORPORATEDAuthorized Signature: [Signature] Date: 2 Sept 2011State of VIRGINIACounty of FAIRFAX, to-wit:Taken, subscribed, and sworn to before me this 2<sup>nd</sup> day of SEPTEMBER, 2011.My Commission expires August 31<sup>st</sup>, 2014

AFFIX SEAL HERE

NOTARY PUBLIC [Signature]

ATTACHMENT  
P.O.# N/A

This agreement constitutes the entire agreement between the parties, and there are no other terms and conditions applicable to the licenses granted hereunder.

Agreed

 2 Sept 2011  
Signature Michael Date  
FRIEDMAN

VP Finance and Administration  
Title

TECSEC SERVICES, INCORPORATED  
Company Name

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Title