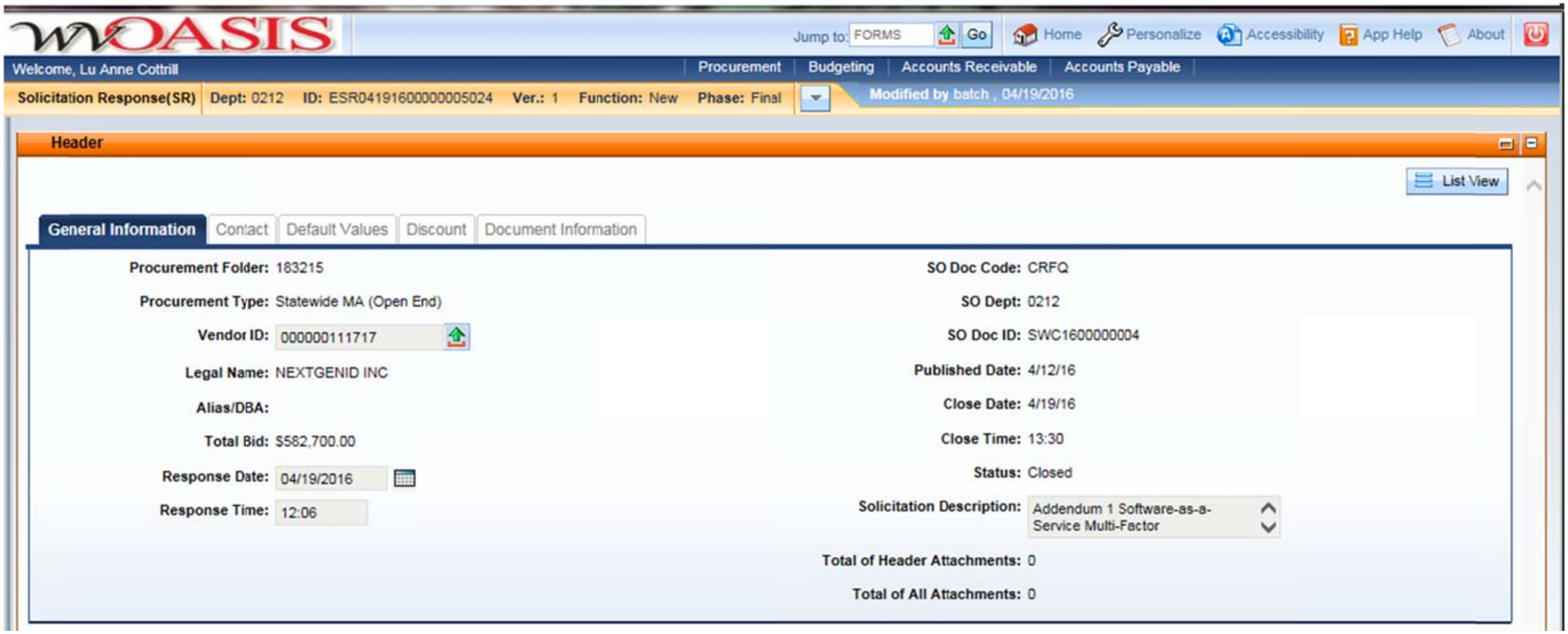
West Virginia
Purchasing Division

2019 Washington Street, East
Charleston, WV 25305
Telephone: 304-558-2306
General Fax: 304-558-6026
Bid Fax: 304-558-3970

The following documentation is an electronically-submitted vendor response to an advertised solicitation from the *West Virginia Purchasing Bulletin* within the Vendor Self-Service portal at ***wvOASIS.gov***. As part of the State of West Virginia’s procurement process, and to maintain the transparency of the bid-opening process, this documentation submitted online is publicly posted by the West Virginia Purchasing Division at ***WVPurchasing.gov*** with any other vendor responses to this solicitation submitted to the Purchasing Division in hard copy format.



Welcome, Lu Anne Cottrill

Solicitation Response(SR) Dept: 0212 ID: ESR04191600000005024 Ver.: 1 Function: New Phase: Final

Modified by batch , 04/19/2016

Procurement Folder:	183215
Procurement Type:	Statewide MA (Open End)
Vendor ID:	000000111717
Legal Name:	NEXTGENID INC
Alias/DBA:	
Total Bid:	$582,700.00
Response Date:	04/19/2016
Response Time:	12:06

SO Doc Code:	CRFQ
SO Dept:	0212
SO Doc ID:	SWC1600000004
Published Date:	4/12/16
Close Date:	4/19/16
Close Time:	13:30
Status:	Closed
Solicitation Description:	Addendum 1 Software-as-a-Service Multi-Factor
Total of Header Attachments:	0
Total of All Attachments:	0

Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Solicitation Response

Proc Folder : 183215

Solicitation Description : Addendum 1 Software-as-a-Service Multi-Factor Authentication

Proc Type : Statewide MA (Open End)

Date issued	Solicitation Closes	Solicitation No	Version
	2016-04-19 13:30:00	SR 0212 ESR04191600000005024	1

VENDOR

000000111717

NEXTGENID INC

FOR INFORMATION CONTACT THE BUYER

Stephanie L Gale

(304) 558-8801
stephanie.l.gale@wv.gov

Signature X	**FEIN #**	**DATE**

All offers subject to all terms and conditions contained in this solicitation

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
1	3.1.1 Software as a Service Capabilities (SaaS) Account	5000.00000	EA	$88.040000	$440,200.00

Comm Code	Manufacturer	Specification	Model #
43233200			

Extended Description :	
	Pricing shall be per "account" for a two (2) year initial period.

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
2	3.1.2.1 Optional Renewal of SaaS (One Year) Year "3"	5000.00000	EA	$9.500000	$47,500.00

Comm Code	Manufacturer	Specification	Model #
43233200			

Extended Description :	
	Pricing shall be per "account" for a one (1) year period.

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
3	3.1.2.2 Optional Renewal of SaaS (One Year) Year "4"	5000.00000	EA	$9.500000	$47,500.00

Comm Code	Manufacturer	Specification	Model #
43233200			

Extended Description :	
	Pricing shall be per "account" for a one (1) year period.

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
4	3.1.2.3 Optional Renewal of SaaS (One Year) Year "5"	5000.00000	EA	$9.500000	$47,500.00

Comm Code	Manufacturer	Specification	Model #
43233200			

Extended Description :	
	Pricing shall be per "account" for a one (1) year period.

Purchasing Divison
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Request for Quotation
21 — Info Technology

Proc Folder: 183215

Doc Description: Addendum 1 Software-as-a-Service Multi-Factor Authentication

Proc Type: Statewide MA (Open End)

Date Issued	Solicitation Closes	Solicitation No	Version
2016-03-24	2016-04-19 13:30:00	CRFQ 0212 SWC1600000004	2

BID RECEIVING LOCATION

BID CLERK
DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
2019 WASHINGTON ST E
CHARLESTON WV 25305
US

VENDOR

Vendor Name, Address and Telephone Number:

NextgenID, Inc.
13454 Sunrise Valley Drive
Suite 430
Herndon, VA 20171
703-429-8533

FOR INFORMATION CONTACT THE BUYER

Stephanie L Gale
(304) 558-8801
stephanie.l.gale@wv.gov

Signature X Michael S. Friedman, EVP FEIN # 20-3188829 DATE April 18, 2016

All offers subject to all terms and conditions contained in this solicitation

ADDITIONAL INFORMAITON:

Addendum #1 issued to:

Provide technical questions and reponses.

End of Addendum #1.

INVOICE TO	SHIP TO
ALL STATE AGENCIES VARIOUS LOCATIONS AS INDICATED BY ORDER	STATE OF WEST VIRGINIA VARIOUS LOCATIONS AS INDICATED BY ORDER
No City WV99999	No City WV 99999
US	US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	3.1.1 Software as a Service Capabilities (SaaS) Account	5000.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43233200			

Extended Description :

Pricing shall be per "account" for a two (2) year initial period.

INVOICE TO	SHIP TO
ALL STATE AGENCIES VARIOUS LOCATIONS AS INDICATED BY ORDER	STATE OF WEST VIRGINIA VARIOUS LOCATIONS AS INDICATED BY ORDER
No City WV99999	No City WV 99999
US	US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
2	3.1.2.1 Optional Renewal of SaaS (One Year) Year "3"	5000.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43233200			

Extended Description :

Pricing shall be per "account" for a one (1) year period.

INVOICE TO	SHIP TO
ALL STATE AGENCIES VARIOUS LOCATIONS AS INDICATED BY ORDER	STATE OF WEST VIRGINIA VARIOUS LOCATIONS AS INDICATED BY ORDER
No City WV99999	No City WV 99999
US	US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
3	3.1.2.2 Optional Renewal of SaaS (One Year) Year "4"	5000.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43233200			

Extended Description :

Pricing shall be per "account" for a one (1) year period.

INVOICE TO	SHIP TO
ALL STATE AGENCIES VARIOUS LOCATIONS AS INDICATED BY ORDER	STATE OF WEST VIRGINIA VARIOUS LOCATIONS AS INDICATED BY ORDER
No City WV99999	No City WV 99999
US	US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
4	3.1.2.3 Optional Renewal of SaaS (One Year) Year "5"	5000.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43233200			

Extended Description :

Pricing shall be per "account" for a one (1) year period.

SCHEDULE OF EVENTS

Line	Event	Event Date
1	Technical Questions Due	2016-04-05

NextgenID®

State of West Virginia
Request for Quotation

NextgenID Bid

To

West Virginia Purchasing Division

For

Software-as-a-Service (SaaS) Multi-Factor Authentication

Solicitation No.- CRFQ 0212 SWC1600000004

Submitted: 19 April 2016

NextgenID®

13454 Sunrise Valley Drive, Suite 430
Herndon, VA 20171

Table of Contents

1.0 Company Overview

NextgenID is a privately held company established in 2005. Our company is focused on providing end-to-end Trusted Identity Enrollment, Credentialing and Managed Service Offering (MSO) through a Software and a Service (SaaS) platform to Government clients in a turn-key IDaaS (Identity as a Service) hosted model. Since everything in the identity assurance trust chain begins with the secure and trusted enrollment of privileged users, NextgenID has designed and developed self-service (NIST levels 1, 2 and 3) enrollment product capabilities and assisted enrollment (NIST level 4) capabilities through the most proficient automated, menu-driven, credential enrollment solution in the industry - the NextgenID Multi-Biometric Enrollment (MBE) ID*Enroll KIOSK. This high speed, multi-assurance level enrollment KIOSK incorporates the industry's first Virtual In-person Proofing (VIP) capability using remote video technology to perform remote in-person enrollments; minimizing on-site staff and streamlining the Level 4 enrollment process to under 5 minutes per applicant.

NextgenID delivers trusted identity credentialing solutions that unify enrollment, issuance and management into an ID ecosystem for interoperability between and within State and Federated Government identity programs. These programs include Homeland Security First Responders, State Government Agencies and Federal Departments and Agencies. As a measure of past performance, NextgenID designed, built, and continues to operate under current contract, the State of West Virginia Personal Identity Verification – Interoperable (PIV-I) - NIST level 4 and Commercial Identity Verification (CIV) -NIST level 3 credential program through the Division of Homeland Security and Emergency Management.

Within the IDaaS Managed Services model, the NextgenID Program Office and staff can confidently implement new customers very efficiently and within a short period of time. Follow-on customers reap the benefits of the currently implemented programs policies, procedures, technical infrastructure, and performing personnel. This ensures that the technical solution is in full compliance and fully certified from end-product, system architecture and design, security, system functionality and feature set, system integration, documentation, customer support, applicant processing, through training and maintenance. The managed service includes a secure and certified data center compliant with National Institute of Science and Technology (NIST) certification requirements that houses the systems servers and data repositories.

NextgenID's Identity Management System in the state of West Virginia establishes a unique identity in accordance with Federal and other national standards defining high level (NIST Level 4) assurance and provides 2 and 3 factor authentication, data encryption, and digital signing of data functionality. NextgenID has maximized the use of 2 and 3 factor authentication, digital signing, and device and data encryption to protect privacy, user confidentiality, and the data integrity for digital transactions.

NextgenID has developed a NIST standards compliant federated smart card for West Virginia that includes all of the required elements for PIV-I credentials and a comparable CIV credential: multi-factor identity authentication, associated X.509 certificates for identity, encryption, digital signing, and card authentication, as well as the ability to associate specific attributes/organization roles to that identity. The NextgenID system also includes the ability to generate derived credentials for use with mobile devices such as mobile telephones and tablets. This smart card and the associated NextgenID managed service that administers the program, having successfully completed Federal Bridge interoperability testing, is cross certified on the Federal Bridge, certified to meet all NIST FIPS-201-2 and FIPS-140-2 requirements and is GSA approved. The program has been fully operational in the state of West Virginia for more than three years.

Through the use of these smart card credentials, user authentication can be achieved through multiple-factors such as PIN (6 to 8 digits), fingerprint (2 fingers), physical presence of the smart card credential, certificate validation and trust chain verification, and certificate revocation list validation. This data is securely stored within the smart card and serves as a "portable database" for each credential holder. Authentication may be achieved in "lights-out" (network down) situations with high degree (national acceptance) of assurance if or when this environmental issue arises.

The NextgenID system developed for West Virginia meets all State and Federal authentication requirements and meets Federal multi-factor authentication requirements specific to Federal criminal systems database and system usage. The system has the inherent capability to enable secure access to applications and systems and to facilitate a more secure single sign on capability with minimal integration with these systems. Many application and networks enterprise systems built within the last ten-years have integrated smart card capability in addition to accepting user based certificates for authentication..

Contact name for questions concerning information on products and services:

Michael Friedman
NextgenID
EVP – Contracts and Administration
13454 Sunrise Valley Drive, Suite 430, Herndon, VA 20171
Phone: 703-429-8533
Email: MFriedman@NextgenID.com

For information on the WV PIV-I Credentialing Program visit:

http://wv.nextgenidtrust.com/

2.0 Multifactor – Interoperability, Capabilities, and Enterprise Strategy

In 2008, the West Virginia Office of the CIO and several agencies became aware of and investigated ongoing federal and state activities to establish and extend high assurance, multifactor trust credentials to state and local governments. These efforts determined that all federal uniformed services, civilians, and contractors are required to use high assurance trust, multi-factor authentication, FIPS-201 based identity credentials for physical and logical access to facilities, networks, and secure data.

The federal government established FIPS-201 open standards, processes, testing, validation, and quality assurance mechanisms to promote security, certainty, and interoperability using broadly accepted national standards. The federal government developed policies to extend the value and interoperability to non-federal users through the PIV-I and CIV programs.

Around 2010, The West Virginia Office of the CIO, acting in conjunction with the West Virginia Department of Military Affairs and Public Safety reviewed use-cases and operations-driven requirements for multifactor authentication, information sharing, and general and secondary use cases including mandates, new policy and operational driven challenges, and interoperability issues and preferences requiring secure and multi-factors authentication. These use cases included:

- ➢ Identity Assurance, Permissions and Claims Management
- ➢ Logical Access to Networks and Information Systems
- ➢ Information Sharing, Situational Awareness, and Process Automation
- ➢ Digital Signature and Non-Reputation
- ➢ Encryption of Information at Rest and in Transit
- ➢ Physical Access & Physical Operations

Other Use Cases

- ▪ Continuous Diagnostics and Mitigation (CDM)
- ▪ Incident & Emergency Response
  - Emergency Response Official/First Responder Authentication Credentials
  - Incident Access & Management
  - Incident Scene Management and Tracking
  - Continuity of Operations and Emergency & Operations Center Access
- ▪ Administration Use Cases, Activities, & Processes
  - Parking and Transportation Operations

- Major Asset and Equipment Management/Control/Secure site operations
- Cashless Payments
- Time and Attendance Monitoring

After comprehensive analysis, West Virginia determined that a FIPS-201 Based PIV-I/CIV solution would be the most effective means of meeting West Virginia's needs across multiple user groups and use cases. Chief among the reasons was the recognition that a FIPS 201 based solution is the only technology that has the inherent capability to uniformly interface with existing and proposed federal systems allowing both physical and logical access. In addition, it is the only system that enables cross enterprise interoperability, digital signature, and the ability to encrypt data.

In 2010, the Department of Military Affairs and Public Safety, in partnership with the Office of the CIO, initiated implementation and validation of this enterprise approach which culminated in the 2011 issuance of a competitive RFP for a FIPS-201 based Level 3 and Level 4 credential program for West Virginia. This procurement resulted in contract HSE-01154-A. Under that contract, FIPS-201 based-credentials have been issued and are being used throughout West Virginia by law enforcement and other First Responders. The sole source renewal and expansion of this state-wide contract (HSE1600000001) is to make PIV-I (Level 4) and CIV (Level 3) credentials available to any other governmental constituency within West Virginia, especially those requiring multi-factor authentication for access.

While there are multiple near-term solutions for two-factor authentication including the solution sought through this solicitation, a FIPS-201 based solution is the only solution that will provide the preferable scalable, enterprise wide approach, that is compliant with the national standards necessary to meet today's interoperability and security requirements. While the federal government has not mandated the use of PIV-I and CIV credentials, it is clear from its policy actions that a FIPS-201 solution will soon be the only acceptable means of demonstrating multi-factor authentication.

3.0 General Requirements

The following sections correspond to the numbered sections within the West Virginia Request for Quotation - Section 3, General Requirements, of the Solicitation.

3.1 Mandatory Contract Item Requirements

In accordance with the requirement in the solicitation, NextgenID will provide the Contract Items listed below on an open-end and continuing basis.

3.1.1 Software as a Service Capabilities (SaaS)

NextgenID SaaS will include the following:

3.1.1.1 Must be listed in Gartner's 2014 Magic Quadrant for User Authentication

This requirement is either to establish the technical qualification of the offeror to perform the tasks required by this solicitation or to establish that the offeror has sufficient presence in the market to support West Virginia. Section 3.4.1.1 of the West Virginia Purchasing Division Procedures Handbook states that a specification based on a brand name must allow the use of an equivalent. In this instance, West Virginia has chosen to use a commercial rating system where inclusion is not based on meeting some set of minimum performance standards, rather it is based on a market definition established by Gartner. Indeed, Gartner itself states:

> *What does it mean if a vendor isn't included in a Magic Quadrant or MarketScope?* *It means that vendor did not meet the inclusion criteria defined for that Magic Quadrant or MarketScope. It does not imply that the vendor is not viable or not competitive. It might indicate that the vendor has a slightly different strategy or functional match, or that it addresses a different target market.*
>
> *(https://www.gartner.com/doc/2560415/gartner-evaluates-vendors-markets-magic?docdisp=share&srcId=1-4398736771)*

With respect to technical standards, NextgenID meets a significantly higher standard than that required by West Virginia for this solicitation. This solicitation seeks only Level 3 credentials and NextgenID is a qualified Level 4 provider. Qualification as a level 4 provider requires initial certification and audit to become operational, an independent annual audit to verify compliance with NIST Special Publication 800-63-2, and certification by the United States (US) General Services Administration (GSA) as an approved certified provider on the GSA Approved Products List (APL). (See Exhibit F for a copy of the letter from GSA verifying NextgenID as an approved provider of Level 4 credentials).

With respect to the ability to support West Virginia under this solicitation, NextgenID has been the exclusive provider of Level 4 credentials to West Virginia under the competitively awarded contract HSE-01154-A for the past four years. Further, under solicitation notice HSE1600000001, NextgenID has been approved for the sole source issuance of a follow on contract to be the provider of Level 3 and Level 4 credentials supporting the state-wide credentialing program under the West Virginia Credential Coordinator.

NextgenID's history with West Virginia and its certification as an approved provider of Level 4 credentials more than meets the underlying purpose of inclusion on the Gartner 2014 Magic Quadrant for User Identification.

3.1.1.2 Must be fully integrated with the existing Remote Access: Virtual Private Network (VPN) solution utilized by the State.

In response to prior queries with the WV Office of Technology, Technology Service Desk informed NextgenID that the State supports Cisco AnyConnect client software and Cisco products for VPN server solutions.

Cisco AnyConnect Secure Mobility Client supports smartcard and the NextgenID MFA Token authentication across the following platforms:

- Windows 10, 8.1, 8, and 7
- Mac OS X 10.8 and later
- Linux Intel (x64)

For support on any Cisco non-supported platforms or operating system versions, OpenVPN is an open-source software application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. OpenVPN supports dual-factor authentication configuration using client-side smart cards and the NextgenID MFA Token.

3.1.1.2.1 SOLUTION MUST ADHERE TO LEVEL 3 SPECIFICATIONS OF NIST SPECIAL PUBLICATION 800-63-2.

Under NIST Special Publication 800-63-2, the NextgenID SaaS solution qualifies as a Level 4 security assurance system. Our multi-factor authentication solution makes use of smartcard hardware security credentials coupled with soft tokens in the form of digital certificates to attain the "highest practical remote network authentication assurance". As stated in NIST 800-63-2, under the section describing the requirements necessary to attain each level, "Level 3 also permits any of the token methods of Level 4." (NIST, 2013, p. vii)

3.1.1.3 Must be configured for high-availability (HA).

As is required by NIST FIPS 201, the NextgenID system infrastructure fully meets the requirements for high- availability. The system provides a standards based, secure enterprise identity management capability implemented with high availability and disaster recovery. The system’s servers are hosted on redundant virtual machines. This architecture supports infrastructure services such as user verification and validation and as such requires a high standard of availability and performance to support the enterprise.

As a SaaS provider, NextgenID meets these high availability requirement needs through system architecture and operational support staffing. System architecture approaches include:

- Redundant servers
- Shared storage arrays
- Hot-swappable RAID drives
- System back-ups
- Disaster Recovery site
- Network monitoring

The additional means to high-availability comes in the form of system administrators dedicated to the maintenance and support of the system and day to day operations. Preventative maintenance is conducted to reduce potential problems and in response to early warning of potential issues.

Last, the NextgenID system is certified to NIST FIPS 201 standards required of Level 4 assurance providers. These standards ensure that high security and availability requirements are meet and maintained.

3.1.1.4 Must provide customer data protection through data-at-rest and data-in-transit encryption.

Both data-at-rest and data-in-transit are protected through the use of encryption in accordance with the Level 4 standards set out in NIST Publication FIPS-201-2. As a certified NIST Level 4 provider, the NextgenID SaaS must adhere to these standards. The information below is an excerpt from FIPS-201-2 specific to the mandatory cryptographic specifications adhered to by NextgenID.

> *4.2.2 Cryptographic Specifications*
>
> *The PIV Card shall implement the cryptographic operations and support functions as defined in [SP 800-78] and [SP 800-73].*
>
> *The PIV Card must store private keys and corresponding public key certificates, and perform cryptographic operations using the asymmetric private keys. At a minimum, the PIV Card must store two asymmetric private keys and the corresponding public key certificates, namely the PIV Authentication key and the asymmetric Card Authentication key. The PIV Card must also store a digital signature key and a key management key, and the corresponding public key certificates, unless the cardholder does not have a government-issued email account at the time of credential issuance.*
>
> *The PIV Card may include an asymmetric private key and corresponding public key certificate to establish symmetric keys for use with secure messaging, as specified in [SP 800-73] and [SP 800-78]. Secure messaging enables data and commands transmitted between the card and an external entity to be both integrity protected and encrypted. Secure messaging may*

be used, for example, to enable the use of on-card biometric comparison as an authentication mechanism.

Once secure messaging has been established, a virtual contact interface may be established. Requirements for the virtual contact interface are specified in [SP 800-73]. Any operation that may be performed over the contact interface of the PIV Card may also be performed over the virtual contact interface. With the exception of the Card Authentication key and keys used to establish a secure messaging, the cryptographic private key operations shall be performed only through the contact interface or the virtual contact interface.

Symmetric cryptographic operations are not mandated for the contactless interface, but departments and agencies may choose to supplement the basic functionality with storage for a symmetric Card Authentication key and support for a corresponding set of cryptographic operations. For example, if a department or agency wants to utilize Advanced Encryption Standard (AES) based challenge/response for physical access, the PIV Card must contain storage for the AES key and support AES operations through the contactless interface. Algorithms and key sizes for each PIV key type are specified in [SP 800-78].

The PIV Card has both mandatory keys and optional keys:

- *The PIV Authentication key is a mandatory asymmetric private key that supports card and cardholder authentication for an interoperable environment.*
- *The asymmetric Card Authentication key is a mandatory private key that supports card authentication for an interoperable environment.*
- *The symmetric (secret) Card Authentication key supports card authentication for physical access, and it is optional.*
- *The digital signature key is an asymmetric private key supporting document signing, and it is mandatory, unless the cardholder does not have a government-issued email account at the time of credential issuance.*
- *The key management key is an asymmetric private key supporting key establishment and transport, and it is mandatory, unless the cardholder does not have a government-issued email account at the time of credential issuance. Optionally, up to twenty retired key management keys may also be stored on the PIV Card.*
- *The PIV Card Application Administration Key is a symmetric key used for personalization and post issuance activities, and it is optional.*
- *The PIV Card may include additional key(s) for use with secure messaging. These keys are defined in [SP 800-73] or [SP 800-78].*

All PIV cryptographic keys shall be generated within a [FIPS140] validated cryptographic module with overall validation at Level 2 or above. In addition to an overall validation of Level 2, the PIV Card shall provide Level 3 physical security to protect the PIV private keys in storage. The scope of the validation for the PIV Card shall include all cryptographic operations performed over both the contact and contactless interfaces (1) by the PIV Card Application, (2) as part of secure messaging as specified in this section, and (3) as part of remote post issuance updates as specified in Section 2.9.2. Specific algorithm testing requirements for the cryptographic operations performed by the PIV Card Application are specified in [SP 800-78].

Requirements specific to storage and access for each key are detailed below. Where applicable, key management requirements are also specified.

- *PIV Authentication Key. This key shall be generated on the PIV Card. The PIV Card shall not permit exportation of the PIV Authentication key. The cryptographic operations that use the PIV Authentication key shall be available only through the contact and the virtual contact interfaces of the PIV Card. Private key operations may be performed using an activated PIV Card without explicit user action (e.g., the PIN need not be supplied for each operation).*

  The PIV Card shall store a corresponding X.509 certificate to support validation of the public key. The X.509 certificate shall include the FASC-N in the subject alternative name extension using the pivFASC-N attribute to support physical access procedures. The X.509 certificate shall also include the UUID value from the GUID data element of the CHUID in the subject alternative name extension. The UUID shall be encoded as a uniform resource identifier (URI), as specified in Section 3 of [RFC4122]. The expiration date of the certificate must be no later than the expiration date of the PIV Card. The PIV Authentication certificate shall include a PIV NACI indicator (background investigation indicator) extension (see Appendix B.2); this non-critical extension indicates the status of the subject's background investigation at the time of card issuance. [23] *Section 5 of this document specifies the certificate format and the key management infrastructure for the PIV Authentication key.*

- *Asymmetric Card Authentication Key. The asymmetric Card Authentication key may be generated on the PIV Card or imported to the card. The PIV Card shall not permit exportation of the Card Authentication key. Cryptographic operations that use the Card Authentication key shall be available through the contact and the contactless interfaces of the PIV Card. Private key operations may be performed using this key without card activation (e.g., the PIN need not be supplied for operations with this key).*

The PIV Card shall store a corresponding X.509 certificate to support validation of the public key. The X.509 certificate shall include the FASC-N in the subject alternative name extension using the pivFASC-N attribute to support physical access procedures. The X.509 certificate shall also include the UUID value from the GUID data element of the CHUID in the subject alternative name extension. The UUID shall be encoded as a URI, as specified in Section 3 of [RFC4122]. The expiration date of the certificate must be no later than the expiration date of the PIV Card. Section 5 of this document specifies the certificate format and the key management infrastructure for asymmetric PIV Card Authentication keys.

- *Symmetric Card Authentication Key. The symmetric Card Authentication key may be imported onto the card by the issuer or be generated on the card. If present, the symmetric Card Authentication key shall be unique for each PIV Card and shall meet the algorithm and key size requirements stated in [SP 800-78]. If present, cryptographic operations using this key may be performed without card activation (e.g., the PIN need not be supplied for operations with this key). The cryptographic operations that use the Card Authentication key shall be available through the contact and the contactless interfaces of the PIV Card. This Standard does not specify key management protocols or infrastructure requirements.*

- *Digital Signature Key. The PIV digital signature key shall be generated on the PIV Card. The PIV Card shall not permit exportation of the digital signature key. If present, cryptographic operations using the digital signature key may only be performed using the contact and the virtual contact interfaces of the PIV Card. Private key operations may not be performed without explicit user action, as this Standard requires the cardholder to authenticate to the PIV Card each time it performs a private key computation with the digital signature key.* [24]

  The PIV Card shall store a corresponding X.509 certificate to support validation of the public key. The expiration date of the certificate must be no later than the expiration date of the PIV Card. Section 5 of this document specifies the certificate format and the key management infrastructure for PIV digital signature keys.

- *Key Management Key. This key may be generated on the PIV Card or imported to the card. If present, the cryptographic operations that use the key management key must only be accessible using the contact and the virtual contact interfaces of the PIV Card. Private key operations may* *be performed using an activated PIV Card without explicit user action (e.g., the PIN need not be supplied for each operation).*

The PIV Card shall store a corresponding X.509 certificate to support validation of the public key. Section 5 of this document specifies the certificate format and the key management infrastructure for key management keys.

- *PIV Card Application Administration Key. If present, the PIV Card Application Administration Key shall be imported onto the card by the issuer. If present, the cryptographic operations that use the PIV Card Application Administration Key must only be accessible using the contact interface of the PIV Card.*

[23] Other methods to indicate background investigative status will be explored in a future revision of this Standard.

[24] [NISTIR7863], Cardholder Authentication for the PIV Digital Signature Key, addresses the appropriate use of PIN caching related to digital signatures.

Data-in-transit is protected through the use of Secure Socket Layer (SSL) / Transport Layer Security (TLS) 1.2 encryption and a link between the SaaS and user computer. This link ensures that all data being passed between end points remains private and secure.

3.1.1.5 Must provide the State third party information security audits and be willing to share results of those audits.

As a certified NIST Level 4 issuer, the NextgenID SaaS is governed by NIST FIPS 201 and associated NIST publications that require annual audits AND immediate remediation of any issues to maintain cross certification to the Federal Bridge. Audits are conducted by certified and independent auditors with expertise specific to NIST FIPS 201, cryptography, system security and architecture.

The SaaS is also architected with audit control points and logs of data transactions specific to process and processing event flows. Operation controls utilize real-time surveillance video, physical access control and logs, physical security barriers and two party administrative controls. This provides very robust and auditable data to verify system, operator, and administrative requirements.

NextgenID adheres to the annual audit requirement and will provide the State with the annual audit results.

3.1.1.6 The vendor must provide documentation outlining the use of any third party cloud services used by the vendor for the State.

The NextgenID SaaS and associated systems and software do not use any third party cloud services.

3.1.1.7 The vendor shall notify the State concerning the discovery of critical vulnerability and security incidents that potentially jeopardize the confidentiality, integrity and availability of the SaaS. Notification shall be implemented and confirmed within twenty-four (24) hours following confirmation of the event.

NextgenID will notify the State within twenty four hours of the discovery of any critical vulnerability and security incidents that potentially jeopardize the confidentiality, integrity, and availability of the SaaS using a methodology satisfactory to the State.

3.1.1.8 Multi-factor Authentication Support.

3.1.1.8.1 REMOTE ACCESS /VIRTUAL PRIVATE NETWORK (VPN)

As stated in section 3.1.1.2, the NextgenID system supports the State’s VPN products and in addition provides multi-factor authentication through the use of a smart card or the NextgenID MFA Token. The multi-factor authentications are:

- The MFA Token - *Something you have*
- PIN – *Something you know*
- Fingerprint – *Something you are*

3.1.1.8.2 MICROSOFT OUTLOOK, FOREFRONT, REMOTE DESKTOP PROTOCOL, ACTIVE DIRECTORY FEDERATION SERVICES (ADFS) AND OFFICE 365

The NextgenID solution will support two factor login / access to applications like Microsoft Outlook, Forefront, ADFS, Office 365, and other applications using the native support for smart card authentication. When a program attempts to make use of a stored certificate for the purpose of logon, attaching a digital signature, or other user authentication, a PIN will be required to access the soft credential from the smartcard.

3.1.1.8.3 UNIX - SECURE SOCKET SHELL (SSH)

SSH supports public key authentication. SSH client programs can be configured use local or token based (i.e. smart card) certificates. Examples of applications that allow smart card authentication for a SSH session include PuTTY with plugins and SecureCRT

3.1.1.9 Second Factor Authentication Requirements.

3.1.1.9.1 NO-COST, VENDOR-PROVIDED MOBILE PHONE APPLICATION COMPATIBLE WITH THE LATEST APPLE, ANDROID, AND WINDOWS MOBILE PHONE OPERATING SYSTEMS.

NextgenID will provide a mobile application that generates a code as a second factor that supports Android, Apple and Windows mobile phone operating systems.

3.1.1.9.2 NON-PROPRIETARY HARDWARE TOKENS.

The smart card credentials offered by NextgenID comply with FIPS 201 (*Personal Identity Verification (PIV) of Federal Employees and Contractors*) standards and therefore can be read by any compliant smart card reader and the identity from the card may be accessed from Windows, OS X, and Linux computers.

3.1.1.9.3 SHORT MESSAGE SERVICE (SMS) PASSCODE AUTHENTICATION.

NextgenID will provide a service for SMS transmission of authentication codes as a second factor.

3.1.1.9.4 SYSTEM-GENERATED BACKUP CODES.

The NextgenID system is able to generate backup codes to be used as a second factor when the mobile application or SMS codes are unavailable.

3.1.1.10 Account Management Capabilities

3.1.1.10.1 MULTI-FACTOR AUTHENTICATION ACCESS CONTROL FOR ACCOUNT MANAGEMENT CONSOLE.

SaaS account management console functions (all account management) require log-on through the use of PKI multi-factor authentication controls.

All System Administrators are issued smart card credentials that are used through role-based security controls to access the system. In addition to this control, physical access to the server environment is provided through a physical access control system.

3.1.1.10.2 REPORTING CAPABILITY FOR AUTHENTICATION LOGGING AND ADMINISTRATIVE ACTIONS.

NextgenID maintains detailed logs and audit reports of actions performed within our systems. All tasks performed by administrative personnel including access control and administrative console logons are recorded and logged for future reference. Logs contain specifics of an event such as time the action was taken, who performed the task, and the completion status of each entry.

NextgenID also uses an administrative ticket system which details the nature of work to be performed by system administrators. Tickets are completed before every entry into our secure data storage and management areas and provide an additional layer of logging and transparency.

3.1.1.10.3 ADMINISTRATIVE MANAGEMENT CONSOLE APPLICATION PROGRAMING INTERFACE (API).

The Administrative Management Console is built upon an Application Programming Interface (API). The API defines the proper way to request services from the Administrative Management Console and underlying services. The Administrative Management Console is the tool used to perform functions relating to reporting, auditing, and user management.

3.1.1.11 Self-service Portal Capabilities

As part of NextgenID's SaaS offering, we will provide a self-service portal for authorized West Virginia users to initiate the process of obtaining credentials. Persons wanting to obtain credentials will need to supply information upon registering that can be used to validate the person's right to have credentials based on an underlying source of data provided by West Virginia. The supplied information used to verify registration will be appropriate personal data elements unique to the applicant. This procedure is necessary both to keep unauthorized persons from obtaining West Virginia credentials and to prevent unauthorized individuals from obligating West Virginia to pay for credentials it did not intend to issue.

The self-service portal provided will have the capability for custom branding by individual state departments or other organizational entities.

3.1.1.12 Subscription and Services

3.1.1.12.1 ENTERPRISE EDITION SUBSCRIPTION "OR EQUAL"

The NextgenID SaaS, middleware and phone application will be provided to the State as a Enterprise subscription.

The NextgenID MFA Token is provided on a per user basis.

3.1.1.12.2 VENDOR MUST BILL UPON A PER USER ACCOUNT, PER MONTH BASIS

NextgenID will bill the State of West Virginia on a monthly per user account basis. Refer to Exhibit A for pricing details.

3.1.1.13 Training

NextgenID will provide training materials in digital format addressing administrative and operational functions including end-user functionality of the provided system. Training materials will be updated periodically and made current at no cost to the state during the life of the contract.

NextgenID will provide the State permission to use these materials in learning management systems utilized by the State.

3.1.1.14 Support Services

NextgenID provides non-critical support via phone, email, and instant messenger (chat) during standard business hours (Monday – Friday 9am – 5pm EST).

NextgenID provides critical support via phone, email, and instant messenger (chat) 24/7.

A phone call, email, or instant message related to a new topic will generate a help desk ticket.

Ticket escalation will be provided based on the product and severity of the help request.

3.1.2 Renewal of SaaS

NextgenID will provide continued support in accordance with the contract terms and contract pricing provided in this proposal for the contract option years 3, 4, and 5.

4.2 Pricing Pages

NextgenID's pricing pages are attached as Exhibit A.

4.3 Software Licenses

NextgenID's software licenses are attached as Exhibit B.

4.4 Maintenance Terms and Conditions or other Requirements.

Pricing Clarification:

Pricing is based on a 24 month model. Each credential issued, regardless of when in the contract, will be billed at the price quoted for contract years one and two for a period of twenty four months. If that credential is extended beyond 24 months, it will be billed at the price quoted for years 3, 4, and 5 for all successive years. For example, a credential issued on the first day of the contract will be billed at the rate of $3.67 per month for the first 24 months of the contract. Assuming the contract is extended for all three option years, months 25 through 60 of that credential will be billed at $0.79 per month. Similarly, a credential issued on month 13 of the contract will be billed at the rate of $3.67 per month for months 13 through 36 and at the rate of $0.79 per month for months 37 through 60. A credential first issued at month 40 will be billed at the rate of $3.67 per month for months 40 through 60.

Other:

None.

6.0 Delivery and Return

NextgenID will deliver standard orders within thirty (30) working days after orders are received and emergency orders within five (5) working days from receipt.

8. Miscellaneous

8.3 Reports

NextgenID will provide quarterly and on demand reports and annual summaries to the Agency showing the Agency's items purchased, quantities of items purchased and the total dollar value of the items purchased.

8.4 Contract Manager

The NextgenID contract manager is:

Michael Friedman
EVP, General Counsel
13454 Sunrise Valley Drive, Suite 430
Herndon, VA 20171
Phone: 703-429-8533
Email: MFriedman@NextgenID.com

8.5 Attachments

- Pricing as Exhibit A
- End User License Agreement for Middleware as Exhibit B
- Vendor Preference Certificate is attached as Exhibit C.
- Purchasing Affidavit is attached as Exhibit D.
- Addendum Acknowledgement Form is attached as Exhibit E.
- GSA Certification of NextgenID as a Level 4 Provider as Exhibit F
- Product Information on the NextgenID MFA Token as Exhibit G

Exhibit A - Multi-Factor Authentication (SaaS)

Pricing Sheet

Line Item Number	Item Name	Description	Alternative Item SKU	Alternative Item Name and Description	Unit of Measure	Quantity	Unit Price	Extended Unit Price
3.1		**Mandatory Contract Item Requirments**						
3.1.1	**Software as a Service Capabilities (SaaS) Account**	All items listed under "Software as a Service Capabilities (3.1.1)". Two (2) year initial implementation contract.	NGID-MFA-T-1	NextgenID MFA Token	Each	5000	$88.04	$440,180.00 ~~0.00~~
3.1.2		**Renewal of Software as a Service Capabilities (SaaS)**						
3.1.2.1	**Software as a Service Capabilities (SaaS) Account**	**OPTIONAL RENEWAL YEAR 3**	NGID-MFA-R-1	NextgenID MFA Token Renewal Year 1	Each	5000	$9.50	$47,500.00 ~~0.00~~
3.1.2.2	**Software as a Service Capabilities (SaaS) Account**	**OPTIONAL RENEWAL YEAR 4**	NGID-MFA-R-2	NextgenID MFA Token Renewal Year 2	Each	5000	$9.50	$47,500.00 ~~0.00~~
3.1.2.3	**Software as a Service Capabilities (SaaS) Account**	**OPTIONAL RENEWAL YEAR 5**	NGID-MFA-R-3	NextgenID MFA Token Renewal Year 3	Each	5000	$9.50	$47,500.00 ~~0.00~~
						Total Bid Price		$582,680.00 ~~0.00~~

Notes:\

- Unit prices above to be charged to the State on a monthly basis.
- This pricing sheet is subject to the interpretive note in Section 4.4 of the NextgenID proposal.

Exhibit B

NextgenID®

END USER LICENSE AGREEMENT

NOTICE: THIS SOFTWARE IS LICENSED, NOT SOLD, TO YOU, AND NEXTGENID OWNS OR HAS THE RIGHT TO SUBLICENSE ALL COPYRIGHT, TRADE SECRET, PATENT, AND OTHER PROPRIETARY RIGHTS IN THE NEXTGENID SOFTWARE. YOU MAY NOT USE THIS SOFTWARE UNLESS YOU AGREE TO ENTER INTO THIS END USER LICENSE AGREEMENT.

ACCEPTANCE: By installing the software and using it in conjunction with the NextgenID MFA Token, you are agreeing to the terms of this Software License Agreement (Agreement). Please read this Agreement carefully. If you do not accept the following terms, you are not granted any right to use either the software or the NextgenID MFA Token and you should return both to NextgenID in accordance with the terms of your purchase agreement. Acceptance of this Agreement is necessary to access the Software product, and constitutes a technological measure that effectively controls access to a work pursuant to the anti-circumvention provisions of The Digital Millennium Copyright Act, 17 U.S.C. §1201 et seq.

This is an Agreement between you, either individually or as a representative of your company or institution (LICENSEE), and NextgenID Inc., 13454 sunrise Valley Drive, Suite 420, Herndon, VA 20171.

1. DEFINITIONS.

The Software Product is licensed (not sold) to LICENSEE hereunder, and LICENSOR owns or has rights to sublicense all copyright, trade secret, patent and other proprietary rights in the Software Product. The term "Software Product" includes all licensed copies of the computer programs and any associated documentation of the middleware used to enable the functionality of a properly licensed NextgenID MFA Token. The Software Product and the NextgenID MFA Token combined are referred to as the Licensed Technology.

2. GRANT OF LICENSE.

LICENSOR grants to LICENSEE a non-exclusive non-transferable license to install the Software Product and any updates provided to you on any device under your operational control for use solely in conjunction with a valid NextgenID MFA Token. LICENSOR reserves the right to update the Software Product from time to time in its sole discretion, including adding, changing, or removing functionalities and features.

3. EXPORT AND IMPORT LICENSES.

LICENSEE shall not export the Licensed Technology without obtaining both the express written approval of NextgenID and the necessary governmental approvals.

4. DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS.

a. Limitations on Reverse Engineering, Decompilation, Disassembly, and Modification. LICENSEE shall not allow any person to reverse engineer, decompile, or disassemble this Software Product. LICENSEE shall not modify or prepare derivative works or versions of the Software Product or any element of the License Technology, except as may be set forth in the Prior Agreement.

b. Transfer of Licensed Technology. LICENSEE shall not sell, loan, rent, lease, or otherwise transfer any of the Licensed Technology, or portions thereof, to others, except in accordance with specific terms agreed to in a separate written agreement.

c. Transfer of Rights. LICENSEE does not have the authority to transfer any rights granted under this Agreement.

d. Termination. Without prejudice to any other rights, NextgenID may immediately terminate this Agreement if LICENSEE fails to comply with its terms and conditions. In such event, absent an extension or succeeding end-user license, LICENSEE shall cease use immediately and either return the Licensed Technology or certify in writing its removal and deletion form any and all devices hosting or using the Software Product.

e. The Licensed Technology is a product, which houses mechanisms for the protection of access to information and or data. The protective systems implanted in the NextgenID Product(s) and Service(s) represent what NextgenID believes to be a high level of the most recent generation of technological protection. NextgenID cannot, however, guaranty that the Licensed Technology is able to prevent or protect the information or data against deliberate acts of third parties seeking to evade or destroy these protective systems. Consequently, this license is granted and accepted with the understanding that such acts can take place and that NextgenID will have no responsibility for protecting against these deliberate acts and without incurring any liability in the event such an act is successful.

5. DUTIES OF LICENSEE

The duties and obligations of LICENSEE, including the consideration provided by LICENSEE to NextgenID in exchange for the grant of license stated above, are set forth in the Separate Agreement, which is acknowledged and incorporated in its entirety herein.

6. INTELLECTUAL PROPERTY RIGHTS.

Licensed Technology is protected by U.S. copyright laws and international treaty provisions, as well as by issued U.S. patents and U.S. trade secret law. LICENSEE shall not copy the printed materials included in the Licensed Technology. NextgenID owns all title and intellectual property in and to the total software product, including but not limited to any elements incorporated therein. No rights to ownership of any intellectual property are transferred by this Agreement.

7. PRODUCT SUPPORT.

NextgenID, or its subsidiaries and affiliates, shall provide product support per the terms of the separate written agreement.

8. US GOVERNMENT RESTRICTED RIGHTS.

The Licensed Technology is provided to the US Government only with restricted rights. Use, duplication, or disclosure by the US Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs (c)(1) and (2) of the Commercial Computer Software -Restricted Rights at 48 CFR 52.227-19, as applicable. Manufacturer is NextgenID Incorporated, 13454 Sunrise Valley Drive, Suite 420, Herndon, VA 20171.

9. NO WARRANTY TO LICENSEE.

NEXTGENID PROVIDES LICENSEE NO WARRANTIES, CONDITIONS, GUARANTEES, OR REPRESENTATIONS AS TO THE MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR ANY OTHER WARRANTIES CONDITIONS, GUARANTEES, OR REPRESENTATIONS, EXPRESS, IMPLIED, ORAL OR IN WRITING, REGARDING THE LICENSED TECHNOLOGY, ITS PERFORMANCE, OR OTHERWISE RELATED TO THIS AGREEMENT. UNDER NO CIRCUMSTANCES SHALL THE LIABILITY OF NEXTGENID, OR ITS SUBSIDIARIES AND AFFILIATES, EXCEED THE AMOUNTS PAID BY THE LICENSEE UNDER THIS AGREEMENT. IN NO EVENT WILL NEXTGENID'S LIABILITY OF ANY KIND INCLUDE ANY SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, INCLUDING LOST PROFITS, EVEN IF NEXTGENID HAS KNOWLEDGE OF THE POTENTIAL LOSS OR DAMAGE.

Exhibit C

Rev. 04/14

State of West Virginia
VENDOR PREFERENCE CERTIFICATE

Certification and application* is hereby made for Preference in accordance with ***West Virginia Code***, §5A-3-37. (Does not apply to construction contracts). ***West Virginia Code***, §5A-3-37, provides an opportunity for qualifying vendors to request (at the time of bid) preference for their residency status. Such preference is an evaluation method only and will be applied only to the cost bid in accordance with the ***West Virginia Code***. This certificate for application is to be used to request such preference. The Purchasing Division will make the determination of the Vendor Preference, if applicable.

1. **Application is made for 2.5% vendor preference for the reason checked:**

____ Bidder is an individual resident vendor and has resided continuously in West Virginia for four (4) years immediately preceding the date of this certification; **or,**

____ Bidder is a partnership, association or corporation resident vendor and has maintained its headquarters or principal place of business continuously in West Virginia for four (4) years immediately preceding the date of this certification; or 80% of the ownership interest of Bidder is held by another individual, partnership, association or corporation resident vendor who has maintained its headquarters or principal place of business continuously in West Virginia for four (4) years immediately preceding the date of this certification; **or,**

____ Bidder is a nonresident vendor which has an affiliate or subsidiary which employs a minimum of one hundred state residents and which has maintained its headquarters or principal place of business within West Virginia continuously for the four (4) years immediately preceding the date of this certification; **or,**

2. **Application is made for 2.5% vendor preference for the reason checked:**

____ Bidder is a resident vendor who certifies that, during the life of the contract, on average at least 75% of the employees working on the project being bid are residents of West Virginia who have resided in the state continuously for the two years immediately preceding submission of this bid; **or,**

3. **Application is made for 2.5% vendor preference for the reason checked:**

____ Bidder is a nonresident vendor employing a minimum of one hundred state residents or is a nonresident vendor with an affiliate or subsidiary which maintains its headquarters or principal place of business within West Virginia employing a minimum of one hundred state residents who certifies that, during the life of the contract, on average at least 75% of the employees or Bidder's affiliate's or subsidiary's employees are residents of West Virginia who have resided in the state continuously for the two years immediately preceding submission of this bid; **or,**

4. **Application is made for 5% vendor preference for the reason checked:**

____ Bidder meets either the requirement of both subdivisions (1) and (2) or subdivision (1) and (3) as stated above; **or,**

5. **Application is made for 3.5% vendor preference who is a veteran for the reason checked:**

____ Bidder is an individual resident vendor who is a veteran of the United States armed forces, the reserves or the National Guard and has resided in West Virginia continuously for the four years immediately preceding the date on which the bid is submitted; **or,**

6. **Application is made for 3.5% vendor preference who is a veteran for the reason checked:**

____ Bidder is a resident vendor who is a veteran of the United States armed forces, the reserves or the National Guard, if, for purposes of producing or distributing the commodities or completing the project which is the subject of the vendor's bid and continuously over the entire term of the project, on average at least seventy-five percent of the vendor's employees are residents of West Virginia who have resided in the state continuously for the two immediately preceding years.

7. **Application is made for preference as a non-resident small, women- and minority-owned business, in accordance with *West Virginia Code* §5A-3-59 and *West Virginia Code of State Rules*.**

____ Bidder has been or expects to be approved prior to contract award by the Purchasing Division as a certified small, women- and minority-owned business.

Bidder understands if the Secretary of Revenue determines that a Bidder receiving preference has failed to continue to meet the requirements for such preference, the Secretary may order the Director of Purchasing to: (a) reject the bid; or (b) assess a penalty against such Bidder in an amount not to exceed 5% of the bid amount and that such penalty will be paid to the contracting agency or deducted from any unpaid balance on the contract or purchase order.

By submission of this certificate, Bidder agrees to disclose any reasonably requested information to the Purchasing Division and authorizes the Department of Revenue to disclose to the Director of Purchasing appropriate information verifying that Bidder has paid the required business taxes, provided that such information does not contain the amounts of taxes paid nor any other information deemed by the Tax Commissioner to be confidential.

Under penalty of law for false swearing (West Virginia Code, §61-5-3), Bidder hereby certifies that this certificate is true and accurate in all respects; and that if a contract is issued to Bidder and if anything contained within this certificate changes during the term of the contract, Bidder will notify the Purchasing Division in writing immediately.

Bidder: NextgenID, Inc.

Signed: Michael S. Friedman

Date: April 18, 2016

Title: EVP, General Counsel

Exhibit D

RFQ No. SWC1600000004

STATE OF WEST VIRGINIA
Purchasing Division

PURCHASING AFFIDAVIT

MANDATE: Under W. Va. Code §5A-3-10a, 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: (1) the debt owed is an amount greater than one thousand dollars in the aggregate; or (2) the debtor is in employer default.

EXCEPTION: The prohibition listed above does not apply where a vendor has contested any tax administered pursuant to chapter eleven of the W. Va. 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.

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.

"Employer default" means having an outstanding balance or liability to the old fund or to the uninsured employers' fund or being in policy default, as defined in W. Va. Code § 23-2c-2, failure to maintain mandatory workers' compensation coverage, or failure to fully meet its obligations as a workers' compensation self-insured employer. An employer is not in employer default if it has entered into a repayment agreement with the Insurance Commissioner and remains in compliance with the obligations under the repayment agreement.

"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 exceed five percent of the total contract amount.

AFFIRMATION: By signing this form, the vendor's authorized signer affirms and acknowledges under penalty of law for false swearing (*W. Va. Code* §61-5-3) that neither vendor nor any related party owe a debt as defined above and that neither vendor nor any related party are in employer default as defined above, unless the debt or employer default is permitted under the exception above.

WITNESS THE FOLLOWING SIGNATURE:

Vendor's Name: NextgenID, Inc.

Authorized Signature: ______________ Date: April 18, 2016
Dario Berini, COO

State of Virginia

County of Fairfax, to-wit:

Taken, subscribed, and sworn to before me this 18th day of April, 2016.

My Commission expires June 30, 2019.

AFFIX SEAL HERE

Michael S. Friedman
Commonwealth of Virginia
Notary Public
Commission No. 120138
My Commission Expires 6/30/2019

NOTARY PUBLIC ______________
Michael S. Friedman

Exhibit E

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: SWC1600000004

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:
(Check the box next to each addendum received)

[X] Addendum No. 1

[ ] Addendum No. 2

[ ] Addendum No. 3

[ ] Addendum No. 4

[ ] Addendum No. 5

[ ] Addendum No. 6

[ ] Addendum No. 7

[ ] Addendum No. 8

[ ] Addendum No. 9

[ ] Addendum No. 10

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that 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.

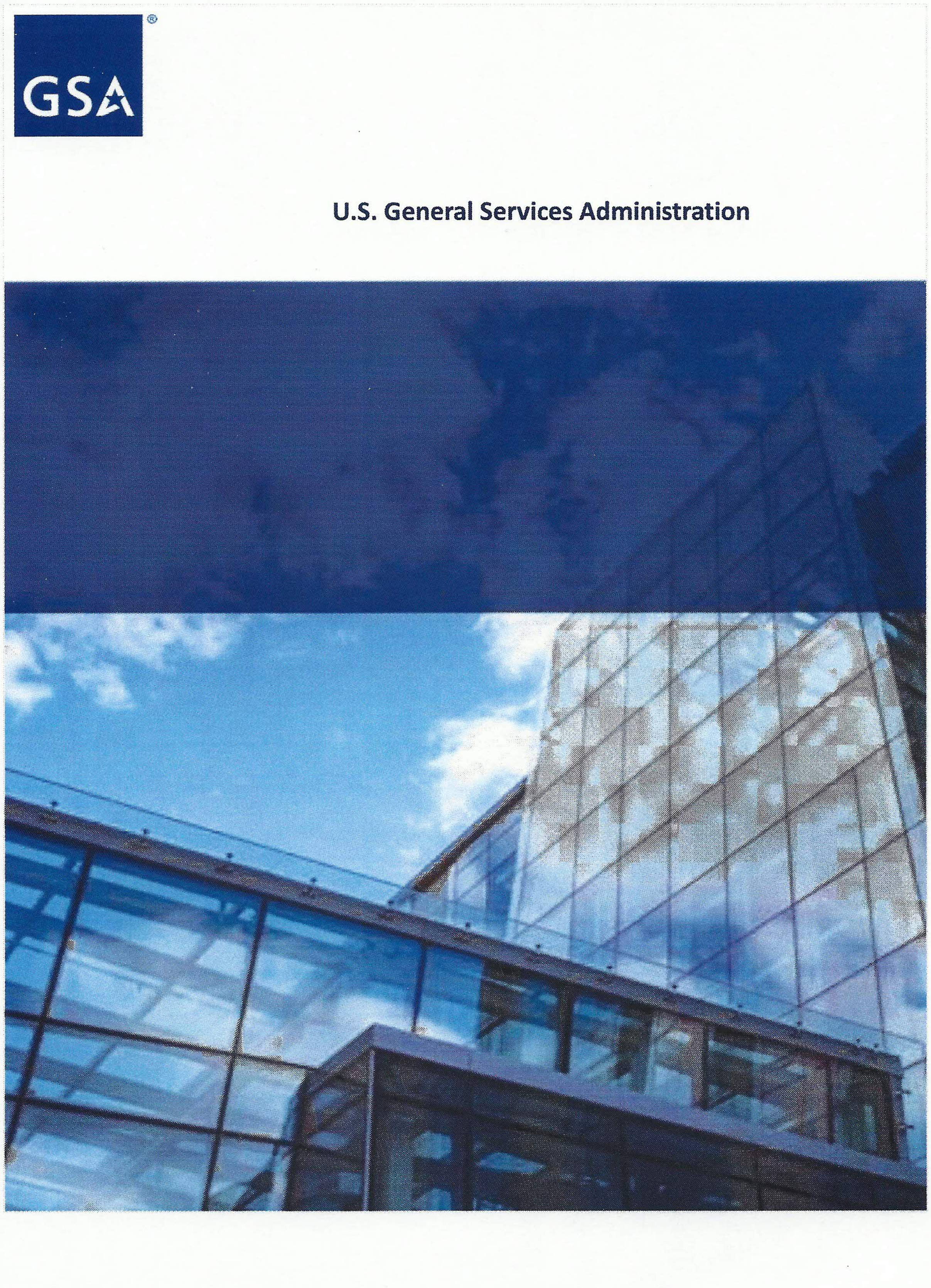
NextgenID, Inc.
Company

Authorized Signature
Michael S. Friedman, EVP

April 18, 2016
Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.

Exhibit F



GSA

U.S. General Services Administration

MEMORANDUM FOR RECORD

FROM: Chi Hickey
Chair, Federal PKI Policy Management Authority

SUBJECT: Federal PKI Recognition of NextGenID as a PIV-I Provider

NextGenID is recognized as a provider of PIV-I registration, enrollment and card issuance services in partnership with Carillon Information Security, an Approved FPKI Provider in the PIV-I Individual Card and PIV-I Vendor categories (see http://idmanagement.gov/fpki-approved-providers).

In 2002, the U.S. Federal Government established the Federal Bridge Certification Authority (FBCA), a non-hierarchical hub for facilitating trust among independently established public key infrastructure (PKI) domains. Originally established to facilitate trust among Federal organizations running organization-specific PKI enterprises, it soon became apparent that the FBCA was well-suited to facilitating trust between Federal organizations and industry. As a result, the FBCA extended its trust community to include the CertiPath Bridge Certification Authority (CBCA) in 2006. Like the FBCA, the CBCA is a non-hierarchical hub that facilitates trust among independent PKI domains. The trust relationship between the FBCA and the CBCA has continued in good standing since the 2006 cross-certification, which provides U.S. Federal Government recognition of the CBCA as a credentialing authority operating on behalf of industry at levels of assurance commensurate with those established by the FBCA.

The CBCA has extended PIV-I cross certification to Carillon Information Security Incorporated, as a result of which, Carillon Information Security is recognized as an FPKI Approved Provider. NextGenID provides registration, enrollment, and card issuance services in partnership with Carillon Information Security and adheres to all policy and operational requirements as specified by the Federal PKI for organizations operating in this capacity.

Please do not hesitate to contact me if you have any additional questions.

Chi Hickey

FPKIPA Co-Chair

Chi.Hickey@GSA.GOV

CHI HICKEY

Digitally signed by CHI HICKEY
DN: c=US, o=U.S. Government,
ou=General Services Administration,
cn=CHI HICKEY,
0.9.2342.19200300.100.1.1=4700100282
6503
Date: 2015.12.16 14:26:09 -05'00'

Exhibit G

NextgenID MFA Token

The NextgenID MFA Token is a smart card based token that supports Public Key Infrastructure, and is based on global standards such as ISO7816 and PKCS#15. It can be used for various tasks requiring strong cryptography, e.g. logging securely into Windows and VPN's, encrypting e-mail, authentication, and electronic signatures. The NextgenID MFA Token is available in multiple configurations in terms of speed, data model, and security to support all levels of NIST FIPS 140-2.

In addition to the standard PIN authentication, NGID MFA Token also supports fingerprint match-on-card biometric comparison. This allows the NextgenID MFA Token to be used when three factor authentication is required.

Technical details of the NGID-MFA-T-1

Common features

- 512 - 2048 bit RSA cryptographic operations with on card key generation
- ECC - ECDSA: Curve P-224, P-256, P-384 cryptographic operations with on card key generation
- Secure random number generator (FIPS 140-2)
- DES, 3DES, AES128, AES256 symmetric encryption algorithms
- SHA-256, SHA-1 and MD5 one-way hash algorithms

Supported standards and specifications

- ISO/IEC 7816
- PKCS#7, #11, #12, and #15
- PIV compatible option also available

Other features

- 80K - 145K EEPROM memory (Other sizes on request)
- NXP JCOP 2.4.2R3 with JavaCard™ 3.0
- Supports a large number of software products
- Supports CSP for Microsoft™ CryptoAPI or PKCS#11 Token Interface using NextgenID PKI Middleware