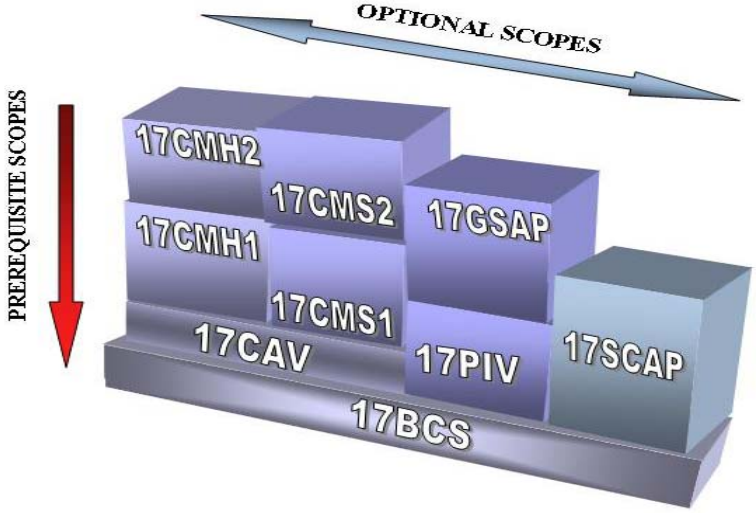
DATE: | **NVLAP LAB CODE:**

INFORMATION TECHNOLOGY SECURITY TESTING
TEST METHOD SELECTION LIST – CRYPTOGRAPHIC AND SECURITY TESTING

Instructions: The minimum level of required expertise is described as "Basic Cryptographic and Security (BCS)" testing and is considered the foundation of all scopes of accreditation for the Cryptographic and Security Testing LAP. However, BCS is not available as a standalone scope of accreditation. Another scope of accreditation must be selected; BCS will be included with any of the other scopes offered.



Legend:

17BCS	=	Basic Cryptographic and Security Testing
17CAV	=	Cryptographic Algorithm Validation Testing
17CMS1	=	Cryptographic Modules – Software 1 Testing (Security Levels 1 to 3)
17CMS2	=	Cryptographic Modules – Software 2 Testing (Security Levels 4 and above)
17CMH1	=	Cryptographic Modules – Hardware 1 Testing (Security Levels 1 to 3)
17CMH2	=	Cryptographic Modules – Hardware 2 Testing (Security Levels 4 and above)
17PIV	=	Personal Identity Verifier Testing
17GSAP	=	GSA-Precursor Testing
17SCAP	=	Security Content Automation Protocol Testing

Any scope of accreditation shown indented from the one or ones above it requires all scopes of accreditation listed above it (to the left) in the chain to be selected, too. For example, the selection of the 17CMH2 scope requires 17CMH1, 17CAV and 17BCS (the last is included automatically) scopes as well. Test methods that are part of each scope are printed for information only. Applicants do not have a choice of test methods under each scope (therefore there are no boxes to check).

DATE: | NVLAP LAB CODE:

INFORMATION TECHNOLOGY SECURITY TESTING
TEST METHOD SELECTION LIST – CRYPTOGRAPHIC AND SECURITY TESTING

NVLAP Test Method Code ***Test Method Designation***

☒ **17BCS** **Basic Cryptographic and Security Testing**

☐ **17CAV** **Cryptographic Algorithm Validation Testing**

17CAV/01 *NIST - Cryptographic Algorithm Validation System (CAVS) for all FIPS-approved and NIST-recommended security functions as required in FIPS PUB 140-2 Annex A (and all superseded versions) - see http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexa.pdf.*

☐ **17/CMS1** **Cryptographic Modules – Software 1 Testing (FIPS 140-2 or successor, Security Level 1 to 3)**

17CMS1/01 *All test methods in accordance with FIPS 140-1, except those listed in 17CMS2/01*

17CMS1/02 *All test methods in accordance with FIPS 140-2, except those listed in 17CMS2/02 and CAVS*

NOTE *The 17CMS1/01 test methods are not available for new products but only for products that have been already validated and must be retested for reasons outside the scope of this document.*

☐ **17CMS2** **Cryptographic Modules – Software 2 Testing FIPS 140-2 or successor, Security Level 4 and above)**

17CMS2/01 *Test methods for Software Security Level 4, in accordance with FIPS 140-1*

17CMS2/02 *Test methods for Software Security Level 4, in accordance with FIPS 140-2*

NOTE *The 17CMS2/01 test methods are not available for new products but only for products that have been already validated and must be retested for reasons outside the scope of this document.*

☐ **17CMH1** **Cryptographic Modules – Hardware 1 Testing (FIPS 140-2 or successor, Security Level 1 to 3)**

17CMH1/01 *All test methods in accordance with FIPS 140-1, except those listed in 17CMH2/01*

17CMH1/02 *All test methods in accordance with FIPS 140-2, except those listed in 17CMH2/02 and CAVS*

NOTE *The 17CMH1/01 test methods are not available for new products but only for products that have been already validated and must be retested for reasons outside the scope of this document.*

DATE: | | NVLAP LAB CODE: | |

INFORMATION TECHNOLOGY SECURITY TESTING
TEST METHOD SELECTION LIST – CRYPTOGRAPHIC AND SECURITY TESTING

NVLAP Test Method Code		*Test Method Designation*
☐	**17CMH2**	**Cryptographic Modules – Hardware 2 Testing (FIPS 140-2 or successor, Security Level 4 and above)**
	17CMH2/01	*Test methods for Physical Security Level 4, in accordance with FIPS 140-1*
	17CMH2/02	*Test methods for Physical Security Level 4, in accordance with FIPS 140-2*

NOTE *The 17CMH2/01 test methods are not available for new products but only for products that have been already validated and must be retested for reasons outside the scope of this document.*

☐	**17PIV**	**Personal Identity Verifier Testing (NPIVP, FIPS 201)**
	17PIV/01	*PIV Card Applications Conformance Test Suite for products meeting specifications in the Federal Information Processing Standard 201 and NIST Special Publication 800-73 or their successors*
	17PIV/02	*PIV Middleware Conformance Test Suite for products meeting specifications in the Federal Information Processing Standard 201 and NIST Special Publication 800-73 or their successors*
☐	**17GSAP**	**General Services Administration Precursor Testing (GSAP test methods, FIPS 201)**
	17GSAP/01	*FIPS 201 Evaluation Program - Electromagnetically Opaque Sleeve*
	17GSAP/02	*FIPS 201 Evaluation Program - Electronic Personalization*
	17GSAP/03	*FIPS 201 Evaluation Program - PIV Card*
	17GSAP/04	*FIPS 201 Evaluation Program - PIV Card Reader - Authentication Key*
	17GSAP/05	*FIPS 201 Evaluation Program - PIV Card Reader – Biometric*
	17GSAP/06	*FIPS 201 Evaluation Program - PIV Card Reader - CHUID (Contact)*
	17GSAP/07	*FIPS 201 Evaluation Program - PIV Card Reader - CHUID (Contactless)*
	17GSAP/08	*FIPS 201 Evaluation Program - PIV Card Reader – Transparent*
	17GSAP/09	*FIPS 201 Evaluation Program - Template Generator*

DATE: | | NVLAP LAB CODE: | |

INFORMATION TECHNOLOGY SECURITY TESTING
TEST METHOD SELECTION LIST – CRYPTOGRAPHIC AND SECURITY TESTING

NVLAP Test Method Code	*Test Method Designation*
17GSAP/10	*FIPS 201 Evaluation Program – Card Printer Station*
17GSAP/11	*FIPS 201 Evaluation Program – CHUID Authentication Reader (Contact)*
17GSAP/12	*FIPS 201 Evaluation Program - CHUID Authentication Reader (Contactless)*
17GSAP/13	*FIPS 201 Evaluation Program - Template Graphical Personalization*
17GSAP/14	*FIPS 201 Evaluation Program – Facial Image Capturing Camera*
☐ **17SCAP**	**Security Content Automation Protocol Testing (SCAP, CVE, CCE, CPE, CVSS, XCCDF and OVAL)**
17SCAP/01	*Common Vulnerabilities and Exposures (CVE)*
17SCAP/02	*Common Configuration Enumeration (CCE)*
17SCAP/03	*Common Platform Enumeration (CPE)*
17SCAP/04	*Common Vulnerability Scoring System (CVSS)*
17SCAP/05	*eXtensible Configuration Checklist Document Format (XCCDF)*
17SCAP/06	*Open Vulnerability Assessment Language (OVAL)*
17SCAP/07	*Security Content Automation Protocol (SCAP)*

Complete the Application Supplement on the next page.

INFORMATION TECHNOLOGY SECURITY TESTING
TEST METHOD SELECTION LIST – CRYPTOGRAPHIC AND SECURITY TESTING

APPLICATION SUPPLEMENT

QUALITY MANUAL (see NIST Handbook 150:2006, subclause 4.2)

Please provide NVLAP with a copy of your laboratory quality manual and supporting management system documentation, including test procedures, with your initial application and with each renewal application.

The documentation may accompany this application or may be sent at a later date; however, NVLAP will take no action on your application until the documentation is received.

PROFICIENCY TESTING (see NIST Handbook 150:2006, subclause 3.4)

For Cryptographic and Security Testing, a proficiency written exam is required prior to the initial on-site and an oral proficiency quiz is conducted as part of every on-site visit. At the end of the initial on-site, an operational proficiency test is provided the lab, which must be successfully evaluated prior to accreditation.

Each Validation Program examines the test reports of the laboratories as they are submitted over time. These examinations are also considered to be proficiency tests for the purposes of continuing accreditation.

Proficiency written exam – If the laboratory is applying for initial accreditation, once the assessor(s) determines that the management system meets the requirements, a written exam will be provided to the applicant laboratory, with a 5-business-day deadline for response, unless otherwise specified. This exam evaluates the laboratory personnel's technical expertise and knowledge of the governing standards and test methods applicable to the scope(s) of accreditation for which the laboratory is applying. The laboratory must score greater than 75% correct responses for the accreditation process to continue and the on-site visit to be scheduled.

Proficiency/round-table quiz during on-site – During the on-site visit, the laboratory's personnel will be quizzed and team dynamics observed for proficiency and expertise in the technical area for which the laboratory is applying for accreditation. Staff member interaction and knowledge distribution among team members are key factors monitored by the assessors. The laboratory staff must provide greater than 75% correct responses for the accreditation process to continue.

Proficiency Artifact and/or Operational Exam – Once the assessor(s) determines that the laboratory has satisfactorily completed the on-site visit, a proficiency artifact and/or operational exam is provided to the applicant laboratory (at the end of the initial on-site visit or after the on-site visit). Unless otherwise specified by NVLAP, the laboratory shall complete the test by the scope dependent deadline. The proficiency artifact and/or operational exam is designed to evaluate the laboratory's understanding of and competence to apply the Cryptographic and Security Testing conformance testing methodology specific to the scope(s) of accreditation the laboratory is applying for. The laboratory shall provide greater than 75% correct responses to

successfully complete the proficiency test. This proficiency artifact and/or operational exam only applies to initial accreditation.

ON-SITE ASSESSMENT (see NIST Handbook 150:2006, subclauses 3.2 and 3.3)

The typical on-site assessment for CST laboratories is two days in length. Experts from several areas may quiz the laboratory (see **Proficiency/round-table quiz during on-site** above) via direct interaction or teleconference during that time. This may add an extra half-day to the on-site, depending upon issues that need to be addressed subsequently to the oral quizzes.