The following information was posted with the attached DRAFT document:

Feb. 6, 2016

SP 800-166

DRAFT Derived PIV Application and Data Model Test Guidelines

Draft SP 800-166 contains the derived test requirements and test assertions for testing the Derived PIV Application and associated Derived PIV data objects. The tests verify the conformance of these artifacts to the technical specifications of SP 800-157. SP 800-157 specifies standards-based, secure, reliable, interoperable Public Key Infrastructure (PKI)-based identity credentials. Draft SP 800-166 is targeted at vendors of Derived PIV Applications, issuers of Derived PIV Credentials, and entities that will conduct conformance tests on these applications and credentials.

The public comment period closes on: **March 14, 2016**.
Send comments to piv_derived<at>nist.gov with “Comments on Draft SP 800-166” in the subject line.

Draft NIST Special Publication 800-166

Derived PIV Application and Data Model Test Guidelines

David Cooper
Hildegard Ferraiolo
Ramaswamy Chandramouli
Nabil Ghadiali
Jason Mohler
Steven Brady

This publication is available free of charge

COMPUTER SECURITY

National Institute of Standards and Technology
U.S. Department of Commerce

Draft NIST Special Publication 800-166

Derived PIV Application and Data Model Test Guidelines

David Cooper
Hildegard Ferraiolo
Ramaswamy Chandramouli
Computer Security Division
Information Technology Laboratory

Nabil Ghadiali
National Gallery of Art
Washington, DC

Jason Mohler
Steven Brady
Electrosoft Services, Inc.
Reston, VA

This publication is available free of charge

February 2016

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3541 *et seq*., Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on Federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other Federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-166
Natl. Inst. Stand. Technol. Spec. Publ. 800-166, 142 pages (February 2016)
CODEN: NSPUE2

This publication is available free of charge

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at http://csrc.nist.gov/publications.

Public comment period: *February 8, 2016* through *March 14, 2016*

All comments are subject to release under the Freedom of Information Act (FOIA).

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: pivtesting@nist.gov

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Abstract

NIST Special Publication (SP) 800-157 contains technical guidelines for the implementation of standards-based, secure, reliable, interoperable Public Key Infrastructure (PKI)-based identity credentials that are issued for mobile devices by federal departments and agencies to individuals who possess and prove control over a valid Personal Identity Verification (PIV) Card. This document, SP 800-166, contains the requirements and test assertions for testing the Derived PIV Application and associated Derived PIV data objects implemented on removable hardware tokens and within mobile devices. The tests reflect the design goals of interoperability and interface functions.

Keywords

authentication; derived PIV application; derived PIV application data model; derived PIV credential; derived test requirements (DTR); FIPS 201; implementation under test (IUT); mobile devices; Personal Identity Verification (PIV); test assertions; token command interface.

Acknowledgements

The authors (David Cooper, Hildegard Ferraiolo and Ramaswamy Chandramouli of NIST; Nabil Ghadiali of the National Gallery of Art; and Jason Mohler and Steven Brady of Electrosoft Services, Inc.), wish to thank their colleagues who reviewed drafts of this document and contributed to its development. Special gratitude to the General Services Administration (GSA) FIPS 201 Evaluation Program (GSA FIPS 201 EP) team for their review and contributions to the document.

Audience

This document is targeted at vendors of Derived PIV Applications, issuers of Derived PIV Credentials, and entities that will conduct tests on these applications and credentials. Readers are assumed to have a working knowledge of SP 800-157, FIPS 201 and other PIV guidelines, and applicable technologies. This document is intended to:

+ Enable developers of Derived PIV Applications to design their applications as specified in SP 800-157 for interface, data object container size and access requirements.

+ Enable issuers of Derived PIV Credentials to ensure that Derived PIV data objects conform to the requirements specified in SP 800-157.

+ Enable developers and issuers to develop self-tests as part of the development effort and issuance process.

+ Enable entities performing conformance tests on Derived PIV Applications and Derived PIV data objects to develop tests that cover the test suite provided in this document.

Table of Contents

1. INTRODUCTION 1

1.1 BACKGROUND 1
1.2 PURPOSE AND SCOPE 1
1.3 DOCUMENT OVERVIEW 2

2. TEST OVERVIEW 3

2.1 TEST ARCHITECTURE 3
2.2 DERIVED PIV APPLICATION TEST 4
2.3 DATA MODEL OF THE DERIVED PIV APPLICATION TESTS 6
2.4 TEST SETUP 7

3. TEST GUIDELINES STRUCTURE 8

3.1 DERIVED TEST REQUIREMENTS 8
3.2 TEST ASSERTIONS 8

4. CONFORMANCE CRITERIA 10

4.1 CONFORMANCE CRITERIA FOR DERIVED PIV APPLICATION ON REMOVABLE TOKENS 10
4.2 CONFORMANCE CRITERIA FOR DATA MODEL OF THE DERIVED PIV APPLICATION 10

5. TEST DOCUMENTATION 11

6. DERIVED TEST REQUIREMENTS FOR THE DERIVED PIV APPLICATION ON REMOVABLE TOKENS 12

6.1 TRANSPORT LAYER CONFORMANCE 12
6.2 DERIVED PIV APPLICATION DATA OBJECT ACCESS/STORAGE CONFORMANCE 13
6.3 DERIVED PIV APPLICATION COMMAND INTERFACE CONFORMANCE 15

7. DERIVED TEST REQUIREMENTS FOR DATA MODEL OF THE DERIVED PIV APPLICATION 27

7.1 BER-TLV CONFORMANCE 27
7.2 SIGNED DATA OBJECT CONFORMANCE 30
7.3 PKI CONFORMANCE 31

8. TEST ASSERTIONS FOR THE DERIVED PIV APPLICATION 40

8.1 TRANSPORT LAYER CONFORMANCE 40
8.2 DERIVED PIV APPLICATION DATA OBJECT ACCESS/STORAGE CONFORMANCE 41
8.3 DERIVED PIV APPLICATION COMMAND INTERFACE CONFORMANCE 43

9. TEST ASSERTIONS FOR THE DERIVED PIV APPLICATION DATA MODEL 87

9.1 BER-TLV CONFORMANCE 87
9.2 SIGNED DATA OBJECT CONFORMANCE 94
9.3 PKI CONFORMANCE 100

List of Appendices

APPENDIX A— TESTING OF DERIVED PIV CREDENTIALS ON EMBEDDED TOKENS 129

A.1 FUNCTIONAL TESTING 129

193 **A.2 DATA MODEL TESTING 129**
194 **APPENDIX B— ACRONYMS 130**
195 **APPENDIX C— GLOSSARY OF TERMS 131**
196 **APPENDIX D— REFERENCES 132**

197

198 **List of Figures**

199 FIGURE 1 - DERIVED PIV APPLICATION CONFORMANCE TEST ARCHITECTURE 3

200

201 **List of Tables**

202 TABLE 1 - ENCODING OF LENGTH FIELD 87

203

1. Introduction

1.1 Background

FIPS 201, *Personal Identity Verification (PIV) for Federal Employees and Contractors* [FIPS201], specified a common set of identity credentials for the purpose of Homeland Security Presidential Directive 12 [HSPD12] in a smart card form factor, known as the PIV Card. [FIPS201] originally required that all PIV credentials and associated keys be stored on the PIV Card, and although the use of the PIV Card for electronic authentication works well with traditional desktop and laptop computers, it is not optimized for mobile devices.[1]

In response to the growing use of mobile devices within the Federal government, [FIPS201] was revised to permit the issuance of an additional credential specifically for mobile devices. This PIV credential is called a Derived PIV Credential, for which the corresponding private key is stored in a cryptographic module within a mobile device. The use of this Derived PIV Credential is restricted to provide PIV-enabled authentication services on mobile devices in order to authenticate the credential holder to remote systems.

1.2 Purpose and Scope

The objective of this document is to provide test requirements and test assertions that could be used to validate the compliance/conformance of the following: (i) the Derived PIV Application and (ii) the Derived PIV data model. Because NIST SP 800-157, *Guidelines for Derived Personal Identity Verification (PIV) Credentials* [SP800-157], was developed for meeting interoperability goals of [FIPS201], the conformance tests in this document provide the assurance that the Derived PIV Application and associated derived PIV data objects that have passed these tests are conformant to the specification. This in turn facilitates procurement of [FIPS201]-products that are interoperable and meet the goals of [HSPD12].

[SP800-157] specifies the use of removable tokens with form factors that may be inserted into mobile devices, such as SD Cards, USB tokens, Universal Integrated Circuit Cards (UICC - the new generation of SIM cards), and non-removable tokens that are embedded in mobile devices. [SP800-157] does not define an application interface for embedded tokens, because these tokens are built into the mobile device and the interface to these tokens is natively supported. Since [SP800-157] doesn't specify application interface requirements for embedded tokens, testing the interfaces for embedded tokens is outside the scope of this document.[2] In addition, this document does not provide conformance tests for any other software, such as the back-end access control software, issuance software, or any specialized service provider software used for logical access.

[1] From [SP800-157] – A mobile device is a portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the devices to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, tablets, and e-readers.

[2] Guidelines on functional and data model testing for embedded tokens are covered in Appendix A.

1.3 Document Overview

The document is organized as follows:

- Section 2 provides a conceptual overview of the test architecture, the test setup and components, and the types of tests (Derived PIV Application and Data Model of the Derived PIV Application) covered within this document.
- Section 3 describes the structure of the test guidelines and explains Derived test requirements (DTR) and test assertions (TA) construction.
- Section 4 details the conformance criteria for each type of test.
- Section 5 explains the documentation necessary to conduct testing.
- Section 6 includes DTRs that apply to the Derived PIV Application based on specifications in [SP800-157].
- Section 7 includes DTRs that apply to the Data Model of the Derived PIV Application based on specifications in [SP800-157].
- Section 8 provides test assertions that are used to test the DTRs of the Derived PIV Application listed in Section 6.
- Section 9 provides test assertions that are used to test the DTRs of the Derived PIV Application data model listed in Section 7.
- Appendix A contains guidelines for functional and data model testing of Derived PIV Credentials on embedded (non-removable) tokens.
- Appendix B contains a list of acronyms used in the document.
- Appendix C contains a glossary of terms used in the document.
- Appendix D contains the list of documents used as references by this document.

2. Test Overview

2.1 Test Architecture

SP 800-166 covers the following two types of tests for removable tokens: (i) Derived PIV Application and (ii) Data Model of the Derived PIV Application. The conceptual architecture for these tests is highlighted with dashed lines and shown in Figure 1.

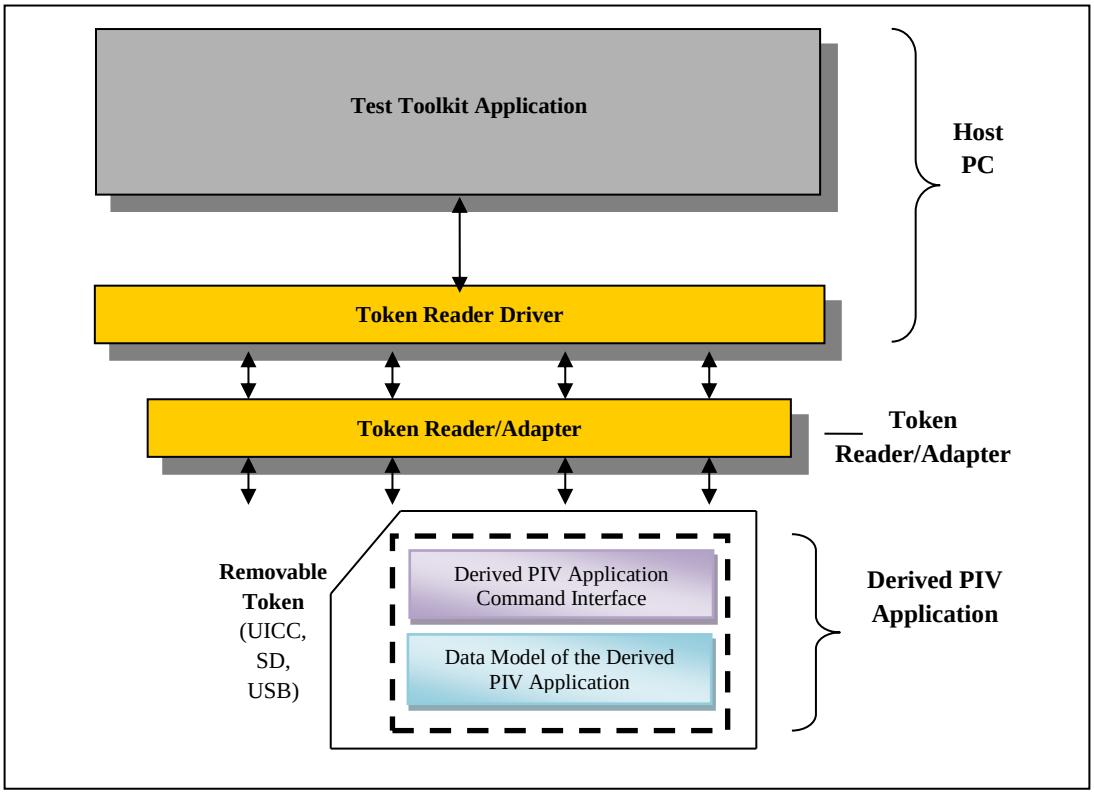

Figure 1 - Derived PIV Application Conformance Test Architecture

The Derived PIV Application resides on the removable hardware cryptographic token,[3] implements the commands in the Derived PIV Application command interface,[4] and provides access to data objects on the Derived PIV Application.

Given that [SP800-157] doesn't specify an application interface or an explicit data model for embedded tokens, vendors may implement Derived PIV Credentials on these devices in a manner of their choosing. Test entities may develop test assertions to test Derived PIV Credentials implemented on such tokens using functional testing developed specifically for the environment and application that they are being used within. Appendix A provides guidelines on testing Derived PIV Credentials (i.e., Derived PIV Authentication certificates) as well as other certificates (digital signature certificate, key management certificates, etc.) that may be stored on

[3] Token in this context refers to the secure element that contains the Derived PIV Application.
[4] The Derived PIV Application command interface is as defined in [SP800-157], Appendix B.2 - Derived PIV Application Token Command Interface.

embedded tokens.

2.2 Derived PIV Application Test

These tests are intended to ensure that tokens with Derived PIV Applications, sold and supplied by vendors, conform to the requirements specified in SP 800-157. In general, these tests cover the following:

+ Transport layer conformance, which ensures interoperability and portability of the Derived PIV Application token between mobile devices.

+ The Derived PIV Application data object access/storage conformance, which ensures that the application is set up and is conformant to [SP800-157] with regards to data object container sizes, data object identifiers, password requirements as well as the security conditions for accessing and storing each of the associated data objects.

+ The Derived PIV Application command interface as per [SP800-157], and includes the security conditions for executing each command in the interface with appropriate response statuses.

The tests should be performed via test scripts that communicate directly with the hardware cryptographic token through the API of the associated reader drivers and includes the following categories of tests.

2.2.1 Transport Layer Conformance

Transport layer conformance tests ensure that an implementation on a specific removable hardware token (i.e., UICC or USB) is compliant with industry standards specified in [SP800-157] and that portability of the token is achieved across mobile devices.

2.2.2 Derived PIV Application Data Object Access/Storage Conformance

The Derived PIV Application data object access/storage conformance tests ensure that the Derived PIV Application is set up and configured per the requirements specified in [SP800-157]. It covers requirements that apply to the removable hardware cryptographic token and includes testing that covers containers for the following data objects:

+ The one mandatory data object as defined in [SP800-157]:
    - X.509 Certificate for Derived PIV Authentication
+ The twenty-five optional data objects, defined in [SP800-157]:
    - X.509 Certificate for Digital Signature
    - X.509 Certificate for Key Management
    - Discovery Object

- Key History Object
- 20 Retired X.509 Certificates for Key Management
- Security Object

The containers will be validated for the following conditions:

+ Presence of containers for the mandatory data object and all supported optional data objects as specified in the vendor documentation
+ Accessibility and storage of data objects using the appropriate BER-TLV tags (specified identifiers as per Section 4, Part 1 of NIST SP 800-73, *Interfaces for Personal Identity Verification* [SP800-73])
+ Appropriate container size allocations for each of the data objects
+ Data objects access rule (password vs. no password)
+ Security condition for data objects access/storage (cryptographic authentication)

2.2.3 Derived PIV Application Command Interface Conformance

These tests will validate that the implementation under test can successfully execute the commands in the Derived PIV Application token command interface as mandated by [SP800-157]. Successful execution constitutes the Derived PIV Application responding with appropriate data and response status words to the commands sent by a test system. It also involves setting state variables per the specification. For example, the criteria for successful execution of the SELECT command involve the following:

+ The response status word returned is '90 00'.
+ The application property template is returned with the correct format and content.
+ The “Derived PIV Application” is the value of “currently selected application” (state variable)

The Derived PIV Application token command interface test suite includes conformance tests for the following commands:

+ Data access commands.
  - SELECT
  - GET DATA
+ Authentication commands.
  - GENERAL AUTHENTICATE

- VERIFY
- CHANGE REFERENCE DATA
- RESET RETRY COUNTER

+ Credential initialization and administration commands.
  - PUT DATA
  - GENERATE ASYMMETRIC KEY PAIR

The token commands will be validated against the following conditions:

+ Precondition for use (password, cryptographic authentication).
+ Expected response status word.
+ Appropriate state variables set in the Derived PIV Application.

2.3 Data Model of the Derived PIV Application Tests

These tests are intended to ensure that issuers populate the containers within the Derived PIV Application with data objects that conform to [SP800-157], [SP800-73] and [SP800-78]. In general, these tests cover the following:

+ Data objects are formatted correctly,
+ Field values are in accordance with the specifications, and
+ Data consistency and value computations such as signatures are accurate.

The tests should be performed via test scripts that communicate directly with the hardware cryptographic token through the API of the associated reader drivers and includes the following categories of tests.

2.3.1 BER-TLV Format Conformance

These tests validate that the tags and lengths of various data objects conform to specifications in [SP800-157].

2.3.2 Signed Data Object Conformance

For the Security Object, the tests check to ensure that the fields in the signature block conform to the Cryptographic Message Syntax (CMS).

2.3.3 PKI Conformance

The PKI conformance tests ensure that the mandatory Derived PIV Authentication certificate,

the optional digital signature certificate, key management certificates, and the Derived PIV Credential Issuer's (content signing) certificate, conform to the certificate profiles as specified in the X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program [PROF]. Additionally, the Derived PIV Application is also tested to check if asymmetric keys are pairs (public and private components) and are using the appropriate cryptographic algorithms in accordance with NIST SP 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification* [SP800-78].

2.4 Test Setup

The test setup for the application and data model tests for the Derived PIV Application consists of the following components:

- Test toolkit application software that resides on a personal computer (PC) with a Universal Serial Bus (USB) port.
- Readers and appropriate drivers:
  - For implementations on an SD, MiniSD or microSD token:
    - A Secure Digital (SD) Memory Card Reader
    - A Memory Card Reader Adapter (for Mini, and Micro SD Cards)
  - For implementation on an UICC token
    - A PC/SC compliant UICC/SIM Card Reader
  - For implementations on micro USB:
    - A Universal Micro USB to USB Cable
- The implementation under test (IUT), which could be either:
  - A Derived PIV Application
  - The data object stored on a Derived PIV Application token[5]

[5] Individual credentials (e.g., Derived PIV Authentication certificate, digital signature certificate, key management certificate) and associated private keys on embedded tokens may also be tested for conformity using functional testing. Refer to Appendix A for details.

3. Test Guidelines Structure

3.1 Derived Test Requirements

Derived test requirements (DTRs) identify conformity conditions based on the normative specifications in [SP800-157] and any other referenced supporting publications (e.g., [FIPS201], [SP800-73], [SP800-78])

In general, each DTR consists of the following elements:

1. An Identifier, which is a code starting with 'DTR' (Identifiers follow a running sequence based on a logical grouping of requirements),

2. A DTR Description, which is a statement taken/derived from the specification. These DTR descriptions include explicit statements using the words "shall," "must," and other terms used to signify the importance of the requirement, and

3. For traceability, each DTR includes a reference to the section of [SP800-157], any other applicable specification such as [FIPS201], [SP800-73], [SP800-78] or [PROF] from which the DTR has been taken.

3.2 Test Assertions

A test assertion is an action or a set of actions that is performed to measure conformity to one or more DTRs. Test assertions provide procedures to guide the tester in executing and managing the test.

In general, each test assertion consists of the following elements:

1. An Identifier, which is a code starting with 'TA' (Identifiers follow a running sequence based on categories of tests),

2. The Purpose of the test,

3. For the purpose of traceability, each test assertion makes specific references to the related DTR(s). Overall there is a many-to-many relationship between test assertions and DTRs (i.e., one test assertion can map to many DTRs and one DTR can be mapped to many test assertions).

4. Vendor/Issuer Documentation, which specifies the information that is needed in order to be able to execute the test. In general, vendors submit documentation for testing the Derived PIV Application while issuers submit documentation for testing the Data Model of the Derived PIV Application.

5. Precondition(s), which describe starting conditions and any prerequisites,

6. Test Scenario, which explains the test procedure in steps,

7. Expected Result, which specifies the success criteria, and
8. Postcondition(s), which describes the final state after completion of the test scenario.

The test assertions for some of the DTRs do not have test scenarios. In such cases, documentation and/or test artifacts may be reviewed to determine compliance with the DTR.

4. Conformance Criteria

Conformance criteria are based on the compliance of the "conformity condition" under the test with the requirements defined in [SP800-157] or any other referenced special publication (e.g., [FIPS201], [SP800-73], [SP800-78]) The criterion for success for each test assertion is based on the type of test being conducted.

4.1 Conformance Criteria for Derived PIV Application on Removable Tokens

The Derived PIV Application tests validate conformance to [SP800-157] of a Derived PIV Application developed by a vendor. The criterion for success is documented as part of the expected result or the required vendor documentation for each test assertion. Overall conformance of a removable token's Derived PIV Application is based on passing the following three categories of tests:

1. Transport layer conformance tests,
2. Derived PIV Application data object access/storage conformance tests, and
3. Derived PIV Application command interface conformance tests

4.2 Conformance Criteria for Data Model of the Derived PIV Application

The data model tests validate the data objects that are loaded onto a conformant Derived PIV Application's removable token by an issuer. The criterion for success is documented as part of the expected result or the required issuer documentation for each test assertion. Overall conformance of the data model of the Derived PIV Application is based on passing the following three categories of tests:

1. BER-TLV format conformance tests,
2. Signed Data Object conformance tests, and
3. PKI conformance tests

Testing entities may also validate individual credentials (e.g., Derived PIV Authentication certificate, digital signature certificate, key management certificate) stored on embedded (non-removable) tokens. As described in Appendix A, in many cases it will also be possible to perform functional testing of the corresponding private keys.

5. Test Documentation

There are two sets of documentation that are part of the compliance testing process: vendor/issuer provided and testing entity generated. These documentations apply to both: (i) Derived PIV Application tests and (ii) Data Model of the Derived PIV Application tests.

The vendor/issuer documentation consists of the following:

+ **Technical documentation:** Technical details for the Derived PIV Application and its data model (as implemented). It includes, at a minimum, all the required information necessary to meet individual test assertions as documented in Section 8 (Test Assertions for the Derived PIV Application) or Section 9 (Test Assertions for the Data Model of the Derived PIV Application) of this document, depending on which tests are being performed.

+ **Security-related information:** (a) Derived PIV Application Password, (b) Password Unblocking Key (PUK), (c) cryptographic algorithms supported by the application, and (d) the number of unsuccessful attempts using: (i) wrong Derived PIV Application Password and (ii) wrong PUK.

The testing entity documents are generated during testing and report test results. They include:

+ **Test logs:** A test log is kept for each test run on any component and is used to summarize the results of all the tests run.

+ **Test reports:** These provide the background (environmental information) for each of the test assertions as well as summary of outcomes from test runs (from test logs) associated with each test assertion.

6. Derived Test Requirements for the Derived PIV Application on Removable Tokens

This section lists requirements that apply to a Derived PIV Application resident on a removable token, such as an SD card, USB token, or UICC, that may be inserted into mobile devices. The requirements are aimed towards vendors of Derived PIV Applications to ensure that these applications are implemented correctly and are in accordance to the specification.

6.1 Transport Layer Conformance[6]

6.1.1 UICC

DTR No:	DTR Description	Spec. Reference
DTR-06.01.01.01	For a Universal Integrated Circuit Card (UICC) used to host a Derived PIV Application, the UICC shall implement the GlobalPlatform Card Secure Element Configuration v1.0 [GPSE].	• [SP800-157], Section 3.3.1.2 - Removable UICC with Cryptographic Module

6.1.2 USB

DTR No:	DTR Description	Spec. Reference
DTR-06.01.02.01	For a USB Integrated Circuit(s) Card Device (ICCD) used to host a Derived PIV Application, the ICCD shall comply with the Universal Serial Bus Device Class - Smart Card ICCD Specification for USB Integrated Circuit(s) Card Devices [ICCDSPEC].	• [SP800-157], Section 3.3.1.3 - USB Token with Cryptographic Module
DTR-06.01.02.02	USB tokens with cryptographic modules that support a Derived PIV Application shall be compliant with the specifications in SP 800-96, *PIV Card to Reader Interoperability Guidelines* [SP800-96], for APDU support for contact card readers.	• [SP800-157], Section 3.3.1.3 - USB Token with Cryptographic Module
DTR-06.01.02.03	The APDUs for the Derived PIV Application (as specified in Appendix B of [SP800-157]) shall be transported to the secure element using the Bulk-Out command pipe and the responses shall be received from the secure element using the Bulk-In command pipe.	• [SP800-157], Section 3.3.1.3 - USB Token with Cryptographic Module

[6] This document does not include test requirements for the SD card transport layer, since there are no requirements specified in [SP800-157].

6.2 Derived PIV Application Data Object Access/Storage Conformance

6.2.1 General

DTR No:	DTR Description	Spec. Reference
DTR-06.02.01.01	The Derived PIV Application shall only support a contact interface.	• [SP800-157], Appendix B.1.2.1 - Derived PIV Application Data Object Containers and associated Access Rules
DTR-06.02.01.02	There shall be at most one Derived PIV Application on any hardware cryptographic token.	• [SP800-157], Appendix B.2 - Derived PIV Application Token Command Interface • [SP800-73], Part 2, Section 3.1.1 - SELECT Card Command
DTR-06.02.01.03	The AID of the Derived Personal Identity Verification Application shall be: 'A0 00 00 03 08 00 00 20 00 01 00'.	• [SP800-157], Appendix B.1.1 - Derived PIV Application Identifier

6.2.2 Derived PIV Application Data Objects and Representation

DTR No:	DTR Description	Spec. Reference
DTR-06.02.02.01	The Derived PIV Application shall contain an X.509 Certificate for Derived PIV Authentication container and optionally the following containers: (i) X.509 Certificate for Digital Signature, (ii) X.509 Certificate for Key Management, (iii) Discovery Object, (iv) Key History Object, (v) up to 20 Retired X.509 Certificates for Key Management and (vi) Security Object.	• [SP800-157], Appendix B.1.2 - Derived PIV Application Data Model Elements • [SP800-73], Part 1, Appendix A - PIV Data Model, Table 10
DTR-06.02.02.02	The minimum capacity for the X.509 Certificate for Derived PIV Authentication shall be 1905 bytes.	• [SP800-73], Part 1, Appendix A - PIV Data Model, Table 7

DTR No:	DTR Description	Spec. Reference
DTR-06.02.02.03	The minimum capacity for the X.509 Certificate for Digital Signature shall be 1905 bytes.	• [SP800-73], Part 1, Appendix A - PIV Data Model, Table 7
DTR-06.02.02.04	The minimum capacity for the X.509 Certificate for Key Management shall be 1905 bytes.	• [SP800-73], Part 1, Appendix A - PIV Data Model, Table 7
DTR-06.02.02.05	The minimum capacity for the Discovery Object shall be 19 bytes.	• [SP800-73], Part 1, Appendix A - PIV Data Model, Table 7
DTR-06.02.02.06	The minimum capacity for the Key History Object shall be 128 bytes.	• [SP800-73], Part 1, Appendix A - PIV Data Model, Table 7
DTR-06.02.02.07	The minimum capacity for each Retired X.509 Certificate for Key Management shall be 1905 bytes.	• [SP800-73], Part 1, Appendix A - PIV Data Model, Table 7
DTR-06.02.02.08	The minimum capacity for the Security Object container shall be 3000 bytes.	• [SP800-157], Appendix B.1.2.1 - Derived PIV Application Data Object Containers and associated Access Rules
DTR-06.02.02.09	The status words that may be returned on the Derived PIV Application command interface are as specified in Section 5.6 of [SP800-73], Part 1.	• [SP800-157], Appendix B.4.3 - Derived PIV Application Status Words
DTR-06.02.02.10	"Basic encoding rules – tag length value" (BER-TLV) tags for the various mandatory and optional data objects within the Derived PIV Application are the same as for the corresponding data objects (mapped as per the Table B-1 of [SP800-157]) of the PIV Card Application as described in Section 4 of [SP800-73], Part 1.	• [SP800-157], Appendix B.1.3 - Derived PIV Application Data Objects Representation
DTR-06.02.02.11	Key reference values used on the Derived PIV Application interfaces shall be in accordance with Table 6-1 of [SP800-78] and Table 4a and Table 4b of [SP800-73], Part 1 with the mappings defined in Table B-2 of [SP800-157].	• [SP800-157], Appendix B.1.4.1 - Derived PIV Application Key References and Security Conditions of Use

DTR No:	DTR Description	Spec. Reference
DTR-06.02.02.12	The algorithm identifiers for the cryptographic algorithms that may be recognized on the Derived PIV Application interfaces are the asymmetric and symmetric identifiers specified in Table 6-2 and Table 6-3 of [SP800-78]. The cryptographic mechanism identifiers that may be recognized on the Derived PIV Application interfaces are those specified in Table 5 of [SP800-73], Part 1.	• [SP800-157], Appendix B.1.4.2 - Derived PIV Application Cryptographic Algorithm and Mechanism Identifiers
DTR-06.02.02.13	The Derived PIV Application Password shall be between 6 and 8 bytes in length. The Derived PIV Application shall enforce the minimum length requirement of six bytes for the Derived PIV Application Password (i.e., shall verify that at least the first six bytes of the value presented to the token command interface are in the range [0x30 – 0x39, 0x41 – 0x5A, 0x61 – 0x7A]).	• [SP800-157], Appendix B.2.1 - Authentication of an Individual
DTR-06.02.02.14	If the actual length of the Derived PIV Application Password is less than 8 bytes, it shall be padded to 8 bytes with 'FF' when presented to the token command interface. The 'FF' padding bytes shall be appended to the actual value of the password.	• [SP800-157], Appendix B.2.1 - Authentication of an Individual
DTR-06.02.02.15	The bytes comprising the Derived PIV Application Password shall be limited to values 0x30 – 0x39, 0x41 – 0x5A, and 0x61 – 0x7A, the ASCII values for the decimal digits '0' – '9', upper case characters 'A' – 'Z', and lower case characters 'a' – 'z' respectively.	• [SP800-157], Appendix B.2.1 - Authentication of an Individual

6.3 Derived PIV Application Command Interface Conformance

6.3.1 General

DTR No:	DTR Description	Spec. Reference
DTR-06.03.01.01	The command interface for the Derived PIV Application shall implement all of the card commands supported by the PIV Card Application as described in [SP800-73], Part 2, which include: SELECT, GET DATA, VERIFY, CHANGE REFERENCE DATA, RESET RETRY COUNTER, GENERAL AUTHENTICATE, PUT DATA, GENERATE ASYMMETRIC KEY PAIR.	• [SP800-157], Appendix B.2 - Derived PIV Application Token Command Interface

DTR No:	DTR Description	Spec. Reference
DTR-06.03.01.02	Token commands indicated with a 'Yes' in the Command Chaining column in Table 2 of [SP800-73], Part 2 shall support command chaining for transmitting a data string too long for a single command as defined in [ISO7816-4].	• [SP800-73], Part 2, Section 3 - PIV Card Application Card Command Interface

509

510 ### 6.3.2 SELECT Command

DTR No:	DTR Description	Spec. Reference
DTR-06.03.02.01	The Derived PIV Application can be selected as the current application on the removable hardware cryptographic token by providing the full AID as follows: 'A0 00 00 03 08 00 00 20 00 01 00'.	• [SP800-157], Appendix B.1.1 - Derived PIV Application Identifier
DTR-06.03.02.02	The token platform shall support a default selected application. In other words, there shall be a currently selected application immediately after a cold or warm reset. This application is the default selected application. The default application may be the Derived PIV Application, or it may be another application.	• [SP800-157], Appendix B.2 - Derived PIV Application Token Command Interface
DTR-06.03.02.03	Upon selection, the Derived PIV Application shall return the application property template described in Table 3 of [SP800-73], Part 2, with the exception that the returned AID is the AID listed in Appendix B.1.1 of [SP800-157].	• [SP800-157], Appendix B.2 - Derived PIV Application Token Command Interface • [SP800-73], Part 2, Section 3.1.1 - SELECT Card Command
DTR-06.03.02.04	The Derived PIV Application can also be made the currently selected application by providing a right-truncated version – that is, without the two-byte version number, '01 00' – in the data field of the SELECT command 'A0 00 00 03 08 00 00 20 00'	• [SP800-157], Appendix B.2 - Derived PIV Application Token Command Interface • [SP800-73], Part 2, Section 3.1.1 - SELECT Card Command
DTR-06.03.02.05	The complete AID, including the two-byte version, of the Derived PIV Application that became the currently selected application upon	• [SP800-157], Appendix B.2 - Derived PIV

DTR No:	DTR Description	Spec. Reference
	successful execution of the SELECT command (using the full or right-truncated PIV AID) shall be returned in the application property template.	Application Token Command Interface • [SP800-73], Part 2, Section 3.1.1 - SELECT Card Command
DTR-06.03.02.06	If the currently selected application is the Derived PIV Application when the SELECT command is sent and the AID in the data field of the SELECT command is either the AID of the Derived PIV Application or its right-truncated version thereof, then the Derived PIV Application shall continue to be the currently selected application and the setting of all security status indicators in the Derived PIV Application shall be unchanged.	• [SP800-157], Appendix B.2 - Derived PIV Application Token Command Interface • [SP800-73], Part 2, Section 3.1.1 - SELECT Card Command
DTR-06.03.02.07	If the currently selected application is the Derived PIV Application when the SELECT command is sent and the AID in the data field of the SELECT command is an invalid AID, then the Derived PIV Application shall remain the currently selected application and the Derived PIV Application security status indicator shall remain unchanged.	• [SP800-157], Appendix B.2 - Derived PIV Application Token Command Interface • [SP800-73], Part 2, Section 3.1.1 - SELECT Card Command
DTR-06.03.02.08	If the currently selected application is the Derived PIV Application when the SELECT command is given and the AID in the data field of the SELECT command is not the Derived PIV Application (nor the right-truncated version thereof), but a valid AID supported by the token, then the Derived PIV Application shall be deselected and the Derived PIV Application security status indicators in the Derived PIV Application shall be set to FALSE.	• [SP800-157], Appendix B.2 - Derived PIV Application Token Command Interface • [SP800-73], Part 2, Section 3.1.1 - SELECT Card Command

6.3.3 GET DATA Command

DTR No:	DTR Description	Spec. Reference
DTR-06.03.03.01	The GET DATA command retrieves the data content of the single data object whose tag is given in the data field.	• [SP800-157], Appendix B.2 - Derived PIV Application Token

DTR No:	DTR Description	Spec. Reference
		Command Interface • [SP800-73], Part 2, Section 3.1.2 - GET DATA Card Command
DTR-06.03.03.02	The L_c value is '05' for all Derived PIV data objects except for the 0x7E interindustry tag (Discovery Object), which has an L_c value of '03'.	• [SP800-157], Appendix B.2 - Derived PIV Application Token Command Interface • [SP800-73], Part 2, Section 3.1.2 - GET DATA Card Command
DTR-06.03.03.03	The GET RESPONSE command is used in conjunction with GET DATA to accomplish the reading of larger Derived PIV data objects.	• [SP800-73], Part 2, Section 3.1.2 - GET DATA Card Command

6.3.4 GENERAL AUTHENTICATE Command

DTR No:	DTR Description	Spec. Reference
DTR-06.03.04.01	The GENERAL AUTHENTICATE command shall be used with the Derived PIV authentication keys ('9A' and '9B') using cryptographic algorithms from Table 6-2 of [SP800-78] to authenticate the token or a token application to the client application (INTERNAL AUTHENTICATE), to authenticate an entity to the token (EXTERNAL AUTHENTICATE), and to perform a mutual authentication between the token and an entity external to the token (MUTUAL AUTHENTICATE).	• [SP800-157], Appendix B.2 - Derived PIV Application Token Command Interface • [SP800-73], Part 2, Section 3.2.4 - GENERAL AUTHENTICATE Card Command
DTR-06.03.04.02	The GENERAL AUTHENTICATE command shall be used with the digital signature key ('9C') (if implemented) to realize the signing functionality on the Derived PIV Application programming interface using cryptographic algorithms specified in Table 3-1 of [SP800-78].	• [SP800-157], Appendix B.2 - Derived PIV Application Token Command Interface • [SP800-73], Part 2, Section 3.2.4 - GENERAL AUTHENTICATE Card Command

DTR No:	DTR Description	Spec. Reference
DTR-06.03.04.03	The GENERAL AUTHENTICATE command shall be used with the key management key ('9D') (if implemented) and the retired key management keys ('82' – '95') (if implemented) to realize key establishment schemes specified in [SP800-78] (ECDH and RSA).	• [SP800-157], Appendix B.2 - Derived PIV Application Token Command Interface • [SP800-73], Part 2, Section 3.2.4 - GENERAL AUTHENTICATE Card Command
DTR-06.03.04.04	The GENERAL AUTHENTICATE command supports command chaining to permit the uninterrupted transmission of long command data fields to the Derived PIV Application. If a token command other than the GENERAL AUTHENTICATE command is received by the Derived PIV Application before the termination of a GENERAL AUTHENTICATE chain, then the Derived PIV Application shall rollback to the state it was in immediately prior to the reception of the first command in the interrupted chain. In other words, an interrupted GENERAL AUTHENTICATE chain has no effect on the Derived PIV Application.	• [SP800-157], Appendix B.2 - Derived PIV Application Token Command Interface • [SP800-73], Part 2, Section 3.2.4 - GENERAL AUTHENTICATE Card Command
DTR-06.03.04.05	For cryptographic operations with larger keys, e.g., RSA 2048, the GET RESPONSE command is used to return the complete result of the cryptographic operation.	• [SP800-157], Appendix B.2 - Derived PIV Application Token Command Interface • [SP800-73], Part 2, Section 3.2.4 - GENERAL AUTHENTICATE Card Command

6.3.5 VERIFY Command

DTR No:	DTR Description	Spec. Reference
DTR-06.03.05.01	Key reference '80' shall be able to be verified by the Derived PIV Application VERIFY command.	• [SP800-157], Appendix B.2 - Derived PIV Application Token

DTR No:	DTR Description	Spec. Reference
		Command Interface • [SP800-73], Part 2, Section 3.2.1 - VERIFY Card Command
DTR-06.03.05.02	When the key reference is '80' and the current value of the retry counter associated with the key reference is zero, then the comparison shall not be made, and the Derived PIV Application shall return the status word '69 83'.	• [SP800-157], Appendix B.2 - Derived PIV Application Token Command Interface • [SP800-73], Part 2, Section 3.2.1 - VERIFY Card Command
DTR-06.03.05.03	When the key reference is '80' and the authentication data in the command data field does not satisfy the criteria in Appendix B.2.1 of [SP800-157], then the token command shall fail and the Derived PIV Application shall return either the status word '6A 80' or '63 CX'. If status word '6A 80' is returned, the security status and the retry counter of the key reference shall remain unchanged. If status word '63 CX' is returned, the security status of the key reference shall be set to FALSE and the retry counter associated with the key reference shall be decremented by one.	• [SP800-157], Appendix B.2 - Derived PIV Application Token Command Interface • [SP800-73], Part 2, Section 3.2.1 - VERIFY Card Command
DTR-06.03.05.04	When the key reference is '80' and the authentication data in the command data field is properly formatted and does not match reference data associated with the key reference, then the token command shall fail, the Derived PIV Application shall return the status word '63 CX', the security status of the key reference shall be set to FALSE, and the retry counter associated with the key reference (i.e., '80') shall be decremented by one.	• [SP800-157], Appendix B.2 - Derived PIV Application Token Command Interface • [SP800-73], Part 2, Section 3.2.1 - VERIFY Card Command
DTR-06.03.05.05	If P1='FF', and L_c and the command data field are absent, the command shall reset the security status of the key reference in P2. The security status of the key reference specified in P2 shall be set to FALSE and the retry counter associated with the key reference shall remain unchanged.	• [SP800-73], Part 2, Section 3.2.1 - VERIFY Card Command

DTR No:	DTR Description	Spec. Reference
DTR-06.03.05.06	If the token command succeeds, then the security status of the key reference (i.e., '80') shall be set to TRUE and the retry counter associated with the key reference shall be set to the reset retry value associated with the key reference.	• [SP800-73], Part 2, Section 3.2.1 - VERIFY Card Command

517

518 ### 6.3.6 CHANGE REFERENCE DATA Command

DTR No:	DTR Description	Spec. Reference
DTR-06.03.06.01	Only reference data associated with key references '80' and '81' specific to the Derived PIV Application (i.e., local key references) may be changed by the Derived PIV Application CHANGE REFERENCE DATA command. The PIV Card Application may allow the reference data associated with other key references to be changed by the PIV Card Application CHANGE REFERENCE DATA, if PIV Card Application will only perform the command with other key references if the requirements specified in Section 2.9.2 of FIPS 201-2 are satisfied.	• [SP800-157], Appendix B.2 - Derived PIV Application Token Command Interface • [SP800-73], Part 2, Section 3.2.2 - CHANGE REFERENCE DATA Card Command
DTR-06.03.06.02	If any key reference value is specified that is not supported by the card, the Derived PIV Application shall return the status word '6A 88'.	• [SP800-157], Appendix B.2 - Derived PIV Application Token Command Interface • [SP800-73], Part 2, Section 3.2.2 - CHANGE REFERENCE DATA Card Command
DTR-06.03.06.03	Key reference '80' reference data shall be changed by the Derived PIV Application CHANGE REFERENCE DATA command. The ability to change reference data associated with key references '81' using the Derived PIV Application CHANGE REFERENCE DATA command is optional.	• [SP800-157], Appendix B.2 - Derived PIV Application Token Command Interface • [SP800-73], Part 2, Section 3.2.2 - CHANGE REFERENCE DATA Card Command

DTR No:	DTR Description	Spec. Reference
DTR-06.03.06.04	If the current value of the retry counter associated with the key reference is zero, then the reference data associated with the key reference (i.e., '80' or '81') shall not be changed and the Derived PIV Application shall return the status word '69 83'.	• [SP800-157], Appendix B.2 - Derived PIV Application Token Command Interface • [SP800-73], Part 2, Section 3.2.2 - CHANGE REFERENCE DATA Card Command
DTR-06.03.06.05	If the authentication data in the command data field does not match the current value of the reference data or if either the authentication data or the new reference data in the command data field of the command does not satisfy the criteria in Appendix B.2.1 of [SP800-157] (for the Derived PIV Application Password) or the criteria in Section 2.4.3 of [SP800-73], Part 2 (for the PUK), the Derived PIV Application shall not change the reference data associated with the key reference and shall return either status word '6A 80' or '63 CX'.	• [SP800-157], Appendix B.2 - Derived PIV Application Token Command Interface • [SP800-73], Part 2, Section 3.2.2 - CHANGE REFERENCE DATA Card Command
DTR-06.03.06.06	If the authentication data in the command data field satisfies the criteria in Appendix B.2.1 of [SP800-157] (for the Derived PIV Application Password) or the criteria in Section 2.4.3 of [SP800-73], Part 2 (for the PUK), and matches the current value of the reference data, but the new reference data in the command data field of the command does not satisfy the criteria in Appendix B.2.1 of [SP800-157] (for the Derived PIV Application Password) or the criteria in Section 2.4.3 of [SP800-73], Part 2 (for the PUK), the Derived PIV Application shall return status word '6A 80'.	• [SP800-157], Appendix B.2 - Derived PIV Application Token Command Interface • [SP800-73], Part 2, Section 3.2.2 - CHANGE REFERENCE DATA Card Command
DTR-06.03.06.07	If the authentication data in the command data field does not match the current value of the reference data, but both the authentication data and the new reference data in the command data field of the command satisfy the criteria in Appendix B.2.1 of [SP800-157] (for the Derived PIV Application Password) or the criteria in Section 2.4.3 of [SP800-73], Part 2 (for the	• [SP800-157], Appendix B.2 - Derived PIV Application Token Command Interface • [SP800-73], Part 2, Section 3.2.2 - CHANGE

DTR No:	DTR Description	Spec. Reference
	PUK), the Derived PIV Application shall return status word '63 CX'.	REFERENCE DATA Card Command
DTR-06.03.06.08	If status word '6A 80' is returned, the security status and retry counter associated with the key reference shall remain unchanged.	• [SP800-157], Appendix B.2 - Derived PIV Application Token Command Interface • [SP800-73], Part 2, Section 3.2.2 - CHANGE REFERENCE DATA Card Command
DTR-06.03.06.09	If status word '63 CX' is returned, the security status of the key reference shall be set to FALSE and the retry counter associated with the key reference shall be decremented by one.	• [SP800-157], Appendix B.2 - Derived PIV Application Token Command Interface • [SP800-73], Part 2, Section 3.2.2 - CHANGE REFERENCE DATA Card Command

519

520 ### 6.3.7 RESET RETRY COUNTER Command

DTR No:	DTR Description	Spec. Reference
DTR-06.03.07.01	The only key reference allowed in the P2 parameter of the RESET RETRY COUNTER command is the Derived PIV Application Password (i.e., key reference '80'). The PIV Card Application may allow the reference data associated with other key references to be changed by the PIV Card Application RESET RETRY COUNTER, if PIV Card Application will only perform the command with other key references if the requirements specified in Section 2.9.2 of FIPS 201-2 are satisfied. If a key reference is specified in P2 that is not supported by the card, the Derived PIV	• [SP800-157], Appendix B.2 - Derived PIV Application Token Command Interface • [SP800-73], Part 2, Section 3.2.3 - RESET RETRY COUNTER Card Command

DTR No:	DTR Description	Spec. Reference
	Application shall return the status word '6A 88'.	
DTR-06.03.07.02	If the current value of the PUK's retry counter is zero then the password's retry counter shall not be reset and the Derived PIV Application shall return the status word '69 83'.	• [SP800-157], Appendix B.2 - Derived PIV Application Token Command Interface • [SP800-73], Part 2, Section 3.2.3 - RESET RETRY COUNTER Card Command
DTR-06.03.07.03	If the reset retry counter authentication data (PUK) in the command data field of the command does not match reference data associated with the PUK then the Derived PIV Application shall return the status word '63 CX'.	• [SP800-157], Appendix B.2 - Derived PIV Application Token Command Interface • [SP800-73], Part 2, Section 3.2.3 - RESET RETRY COUNTER Card Command
DTR-06.03.07.04	If the new reference data (password) in the command data field of the command does not satisfy the criteria in Appendix B.2.1 of [SP800-157], then the Derived PIV Application shall return the status word '6A 80'.	• [SP800-157], Appendix B.2 - Derived PIV Application Token Command Interface • [SP800-73], Part 2, Section 3.2.3 - RESET RETRY COUNTER Card Command
DTR-06.03.07.05	If the reset retry counter authentication data (PUK) in the command data field of the command does not match reference data associated with the PUK and the new reference data (password) in the command data field of the command does not satisfy the criteria in Appendix B.2.1 of [SP800-157], then the Derived PIV Application shall return either status word '6A 80' or '63 CX'.	• [SP800-157], Appendix B.2 - Derived PIV Application Token Command Interface • [SP800-73], Part 2, Section 3.2.3 - RESET RETRY COUNTER Card Command

DTR No:	DTR Description	Spec. Reference
DTR-06.03.07.06	If the Derived PIV Application returns status word '6A 80' then the retry counter associated with the password shall not be reset, the security status of the password's key reference shall remain unchanged, and the PUK's retry counter shall remain unchanged.	• [SP800-157], Appendix B.2 - Derived PIV Application Token Command Interface • [SP800-73], Part 2, Section 3.2.3 - RESET RETRY COUNTER Card Command
DTR-06.03.07.07	If the Derived PIV Application returns status word '63 CX', then the retry counter associated with the password shall not be reset, the security status of the password's key reference shall be set to FALSE, and the PUK's retry counter shall be decremented by one.	• [SP800-157], Appendix B.2 - Derived PIV Application Token Command Interface • [SP800-73], Part 2, Section 3.2.3 - RESET RETRY COUNTER Card Command
DTR-06.03.07.08	If the token command succeeds, then the password's retry counter shall be set to its reset retry value. Optionally, the PUK's retry counter may be set to its initial reset retry value. The security status of the password's key reference shall not be changed.	• [SP800-157], Appendix B.2 - Derived PIV Application Token Command Interface • [SP800-73], Part 2, Section 3.2.3 - RESET RETRY COUNTER Card Command

6.3.8 PUT DATA Command

DTR No:	DTR Description	Spec. Reference
DTR-06.03.08.01	The PUT DATA command shall completely replace the data content of a single data object in the Derived PIV Application with new content.	• [SP800-157], Appendix B.2 - Derived PIV Application Token Command Interface • [SP800-73], Part 2, Section 3.2.5 - PUT

DTR No:	DTR Description	Spec. Reference
		DATA Card Command

523

524 ### 6.3.9 GENERATE ASYMMETRIC KEY PAIR Command

DTR No:	DTR Description	Spec. Reference
DTR-06.03.09.01	The GENERATE ASYMMETRIC KEY PAIR command initiates the generation and storing in the token of the reference data of an asymmetric key pair, i.e., a public key and a private key. The public key of the generated key pair is returned as the response to the command.	• [SP800-157], Appendix B.2 - Derived PIV Application Token Command Interface • [SP800-73], Part 2, Section 3.2.6 - GENERATE ASYMMETRIC KEY PAIR Command
DTR-06.03.09.02	If there is reference data currently associated with the key reference, it is replaced in full by the generated data.	• [SP800-157], Appendix B.2 - Derived PIV Application Token Command Interface • [SP800-73], Part 2, Section 3.2.6 - GENERATE ASYMMETRIC KEY PAIR Command

525

7. Derived Test Requirements for Data Model of the Derived PIV Application

This section lists requirements that apply to the Data Model of the Derived PIV Application. They are aimed towards issuers of tokens to ensure that Derived PIV Application data objects are formatted correctly and field values are in accordance to the specification.

7.1 BER-TLV Conformance

7.1.1 General

DTR No:	DTR Description	Spec. Reference
DTR-07.01.01.01	Before the card is issued, data objects that are created but not used shall be set to zero-length value.	• [SP800-73], Part 1, Section 4.1.1 - Data Object Content

7.1.2 X.509 Certificate for Derived PIV Authentication

DTR No:	DTR Description	Spec. Reference
DTR-07.01.02.01	The X.509 Certificate for Derived PIV Authentication shall include all the Tag-Length-Value (TLV) elements in Table 10 of [SP800-73], Part 1 in the order listed.	• [SP800-157], Appendix B.1.2 - Derived PIV Application Data Model Elements • [SP800-73], Part 1, Appendix A - PIV Data Model, Table 10

7.1.3 X.509 Certificate for Digital Signature

DTR No:	DTR Description	Spec. Reference
DTR-07.01.03.01	If implemented, the X.509 Certificate for Digital Signature data object shall include all the TLV elements in Table 15 of [SP800-73], Part 1 in the order listed.	• [SP800-157], Appendix B.1.2 - Derived PIV Application Data Model Elements • [SP800-73], Part 1, Appendix A - PIV Data Model, Table 15

538

539 ### 7.1.4 X.509 Certificate for Key Management

DTR No:	DTR Description	Spec. Reference
DTR-07.01.04.01	If implemented, the X.509 Certificate for Key Management data object shall include all the TLV elements in Table 16 of [SP800-73], Part 1 in the order listed.	• [SP800-157], Appendix B.1.2 - Derived PIV Application Data Model Elements • [SP800-73], Part 1, Appendix A - PIV Data Model, Table 16

540

541 ### 7.1.5 Discovery Object

DTR No:	DTR Description	Spec. Reference
DTR-07.01.05.01	If implemented, the Discovery Object shall include all the TLV elements in Table 18 of [SP800-73], Part 1 in the order listed.	• [SP800-157], Appendix B.1.2 - Derived PIV Application Data Model Elements • [SP800-73], Part 1, Appendix A - PIV Data Model, Table 18
DTR-07.01.05.02	If the Discovery Object is implemented, the first byte of the PIN Usage Policy shall be set to 0x40.	• [SP800-157], Appendix B.1.2 - Derived PIV Application Data Model Elements
DTR-07.01.05.03	If the Discovery Object is implemented, the second byte of the PIN Usage Policy shall be set to 0x00.	• [SP800-73], Part 1, Section 3.3.2 – Discovery Object

542

543 ### 7.1.6 Key History Object

DTR No:	DTR Description	Spec. Reference
DTR-07.01.06.01	If implemented, the Key History Object shall include all the TLV elements in Table 19 of [SP800-73], Part 1 in the order listed.	• [SP800-157], Appendix B.1.2 - Derived PIV Application Data

DTR No:	DTR Description	Spec. Reference
		Model Elements • [SP800-73], Part 1, Appendix A - PIV Data Model, Table 19

544

545 ### 7.1.7 Retired X.509 Certificates for Key Management

DTR No:	DTR Description	Spec. Reference
DTR-07.01.07.01	If implemented, the Retired X.509 Certificate for Key Management data objects shall include all the TLV elements in Tables 20 - 39 of [SP800-73], Part 1 in the order listed.	• [SP800-157], Appendix B.1.2 - Derived PIV Application Data Model Elements • [SP800-73], Part 1, Appendix A - PIV Data Model, Table 20-Table 39

546

547 ### 7.1.8 Security Object

DTR No:	DTR Description	Spec. Reference
DTR-07.01.08.01	If implemented, the Security Object shall include all the TLV elements in Table 12 of [SP800-73], Part 1 in the order listed.	• [SP800-157], Appendix B.1.2 - Derived PIV Application Data Model Elements • [SP800-73], Part 1, Appendix A - PIV Data Model, Table 12
DTR-07.01.08.02	The Security Object shall be present in the Derived PIV Application if either the Discovery Object or the Key History object is present, and shall be absent otherwise.	• [SP800-157], Appendix B.1.2 - Derived PIV Application Data Model Elements
DTR-07.01.08.03	All unsigned data objects (i.e., the Discovery Object and the Key History object) within the Derived PIV Application shall be included in the Security Object.	• [SP800-157], Appendix B.1.2 - Derived PIV Application Data Model Elements

548
549 ## 7.2 Signed Data Object Conformance

550 ### 7.2.1 Security Object

DTR No:	DTR Description	Spec. Reference
DTR-07.02.01.01	The message digests produced as a result of a hash function on the contents of a Discovery Object and/or the Key History Object, if implemented, shall be identical to that data object's message digest contained in the Security Object.	• [SP800-157], Appendix B.1.2 - Derived PIV Application Data Model Elements • [SP800-73], Part 1, Section 3.1.7 – Security Object
DTR-07.02.01.02	The Security Object shall contain an asymmetric digital signature as specified in RFC 5652, Cryptographic Message Syntax [RFC5652].	• [SP800-73], Part 1, Section 3.1.7 – Security Object
DTR-07.02.01.03	The digital signature is implemented as a SignedData Type.	• [SP800-73], Part 1, Section 3.1.7 – Security Object
DTR-07.02.01.04	The value of the version field of the SignedData content type shall be v3.	• [SP800-73], Part 1, Section 3.1.7 – Security Object
DTR-07.02.01.05	The digestAlgorithms field of the SignedData content type shall be in accordance with Table 3-2 of [SP800-78].	• [SP800-73], Part 1, Section 3.1.7 – Security Object
DTR-07.02.01.06	The eContentType of the encapContentInfo shall be id-icao-ldsSecurityObject (OID = 1.3.27.1.1.1).	• [SP800-73], Part 1, Section 3.1.7 – Security Object
DTR-07.02.01.07	The eContent of the encapContentsInfo field shall contain the encoded contents of the ldsSecurity object.	• [SP800-73], Part 1, Section 3.1.7 – Security Object
DTR-07.02.01.08	The signature field of the Security Object, tag 0xBB, shall include the Derived PIV Credential Issuer's (content signing) certificate.	• [SP800-157], Appendix B.1.2 - Derived PIV Application Data Model Elements
DTR-07.02.01.09	The digestAlgorithm field specified in the SignerInfo field is in accordance with Table 3-2 of [SP800-78].	• [SP800-73], Part 1, Section 3.1.7 – Security Object

DTR No:	DTR Description	Spec. Reference
DTR-07.02.01.10	The signatureAlgorithm field in the SignerInfo field is specified as follows: for RSA with PKCS #1 v1.5 padding, the signatureAlgorithm field shall specify the rsaEncryption OID (as per Section 3.2 of [RFC3370]), and for ECDSA and RSA with PSS padding, the signatureAlgorithm shall be in accordance with Table 3-3 of [SP800-78].	• [SP800-73], Part 1, Section 3.1.7 – Security Object
DTR-07.02.01.11	The SignedData content type shall include the digital signature.	• [SP800-73], Part 1, Section 3.1.7 – Security Object

551

552 ## 7.3 PKI Conformance

553 ### 7.3.1 X.509 Certificate for Derived PIV Authentication

DTR No:	DTR Description	Spec. Reference
DTR-07.03.01.01	The signature field in the certificate shall specify an algorithm from Table 3-3 of [SP800-78] in the AlgorithmIdentifier field.	• [SP800-78], Section 3.2.1 - Specification of Digital Signatures on Authentication Information
DTR-07.03.01.02	If RSA with PSS padding is used, the parameters field of the AlgorithmIdentifier type shall assert SHA-256 (OID = 2.16.840.1.101.3.4.2.1). For RSA with PKCS #1 v1.5 padding, the parameters field is populated with NULL. For ECDSA, the parameters field is absent.	• [PROF], Worksheet titled - Derived PIV Authentication Certificate Profile
DTR-07.03.01.03	The subjectPublicKeyInfo field shall assert an algorithm in the AlgorithmIdentifier in accordance with Table 3-4 of [SP800-78].	• [SP800-78], Section 3.2.2 - Specification of Public Keys In X.509 Certificates
DTR-07.03.01.04	If the public key algorithm is elliptic curve, then the parameters field contains the namedCurve choice populated with the OID for Curve P-256 (1.2.840.10045.3.1.7).	• [PROF], Worksheet titled - Derived PIV Authentication Certificate Profile
DTR-07.03.01.05	The keyUsage extension shall assert only the digitalSignature bit. No other bits shall be asserted.	• [PROF], Worksheet titled - Derived PIV Authentication Certificate Profile
DTR-07.03.01.06	The policyIdentifier field in the	• [PROF], Worksheet

DTR No:	DTR Description	Spec. Reference
	certificatePolicies must assert id-fpki-common-derived-pivAuth (OID = 2.16.840.1.101.3.2.1.3.40) or id-fpki-common-derived-pivAuth-hardware (OID = 2.16.840.1.101.3.2.1.3.41).	titled - Derived PIV Authentication Certificate Profile
DTR-07.03.01.07	The subjectAltName extension shall include a UUID encoded as a URN, as specified in Section 3 of [RFC4122], *A Universally Unique IDentifier (UUID) URN Namespace*.	• [PROF], Worksheet titled - Derived PIV Authentication Certificate Profile
DTR-07.03.01.08	The piv-interim extension (OID = 2.16.840.1.101.3.6.9.1) shall be present and contain an interim_indicator field, which is populated with a Boolean value. This extension is not critical.	• [PROF], Worksheet titled - Derived PIV Authentication Certificate Profile
DTR-07.03.01.09	The authorityInfoAccess field shall contain an id-ad-ocsp accessMethod. The access location uses the Uniform Resource Identifier (URI) name form to specify the location of a Hypertext Transfer Protocol (HTTP) accessible Online Certificate Status Protocol (OCSP) server distributing status information for this certificate.	• [PROF], Worksheet titled - Derived PIV Authentication Certificate Profile
DTR-07.03.01.10	The cRLDistributionPoints extension is required and must contain an HTTP URI. The URI must point to a file that has an extension of ".crl" that contains the DER encoded CRL that provides status information about the certificate. (see [RFC2585], *Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP*)	• [PROF], Worksheet titled - Derived PIV Authentication Certificate Profile
DTR-07.03.01.11	The authorityInfoAccess field shall contain an id-ad-caIssuers (1.3.6.1.5.5.7.48.2) accessMethod. The access location shall specify the location to an HTTP accessible Web server where certificates issued to the issuer of this certificate may be found. The URI must point to a file that has an extension of ".p7c" containing a certs-only CMS message (see [RFC5751], *Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification*).	• [PROF], Worksheet titled - Derived PIV Authentication Certificate Profile
DTR-07.03.01.12	The size of the public key for the Derived PIV Authentication certificate shall be in accordance with Table 3-1 of [SP800-78].	• [SP800-78], Section 3.1 - PIV Cryptographic Keys
DTR-07.03.01.13	The public key present in the Derived PIV	• [SP800-157],

DTR No:	DTR Description	Spec. Reference
	Authentication certificate shall correspond to the Derived PIV Authentication private key.	Appendix B.1.2 - Derived PIV Application Data Model Elements
DTR-07.03.01.14	If the public key algorithm is RSA, the exponent shall be equal to 65 537.	• [SP800-78], Section 3.1, PIV Cryptographic Keys

554

555 ### 7.3.2 X.509 Certificate for Digital Signature

556 [SP800-157] doesn't specify any requirements on the digital signature key and certificate. The
557 requirements listed herein follow those specified in [FIPS201] for digital signature certificates
558 that are not issued by legacy PKIs,[7] and thus do not actually apply to the X.509 Certificate for
559 Digital Signature stored within a Derived PIV Application, with the exception that certificates
560 that assert the id-fpki-common-policy, id-fpki-common-hardware, or id-fpki-common-High
561 certificate policy OID are required by the corresponding certificate policy to conform to [PROF].

DTR No:	DTR Description	Spec. Reference
DTR-07.03.02.01	The signature field in the certificate shall specify an algorithm from Table 3-3 of [SP800-78] in the AlgorithmIdentifier.	• [SP800-78], Section 3.2.1 - Specification of Digital Signatures on Authentication Information
DTR-07.03.02.02	If RSA with PSS padding is used, the parameters field of the AlgorithmIdentifier type shall assert SHA-256 (OID = 2.16.840.1.101.3.4.2.1). For RSA with PKCS #1 v1.5 padding, the parameters field is populated with NULL. For ECDSA, the parameters field is absent.	• [PROF], Worksheet titled - End Entity Signature Certificate Profile
DTR-07.03.02.03	The subjectPublicKeyInfo field shall assert an algorithm in the AlgorithmIdentifier in accordance with Table 3-4 of [SP800-78].	• [SP800-78], Section 3.2.2 - Specification of Public Keys In X.509 Certificates
DTR-07.03.02.04	If the public key algorithm is elliptic curve, then the parameters field contains the namedCurve choice populated an appropriate OID from [SP800-78].	• [PROF], Worksheet titled - End Entity Signature Certificate Profile
DTR-07.03.02.05	The keyUsage extension shall assert both the digitalSignature and nonRepudiation bits. No	• [PROF], Worksheet titled - End Entity

[7] Legacy PKIs are the PKIs of departments and agencies that have cross-certified with the Federal Bridge CA (FBCA) at the Medium Hardware or High Assurance Level.

DTR No:	DTR Description	Spec. Reference
	other bits shall be asserted.	Signature Certificate Profile
DTR-07.03.02.06	The policyIdentifier field in the certificatePolicies must assert one of the following: id-fpki-common-policy (OID = 2.16.840.1.101.3.2.1.3.6), id-fpki-common-hardware (OID = 2.16.840.1.101.3.2.1.3.7) or id-fpki-common-High (OID = 2.16.840.1.101.3.2.1.3.16).	• [PROF], Worksheet titled - End Entity Signature Certificate Profile
DTR-07.03.02.07	The authorityInfoAccess field shall contain an id-ad-caIssuers (1.3.6.1.5.5.7.48.2) accessMethod. The access location shall to specify the location of an LDAP accessible directory server or HTTP accessible Web server where certificates issued to the issuer of this certificate may be found. If LDAP is used, the URI must include the DN of the entry containing the relevant certificates and specify the directory attribute in which the certificates are located. If the directory in which the certificates are stored expects the "binary" option to be specified, then the attribute type must be followed by ";binary" in the URI. If HTTP is used, the URI must point to a file that has an extension of ".p7c" containing a certs-only CMS message (see RFC 5751, *Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification* [RFC5751]).	• [PROF], Worksheet titled - End Entity Signature Certificate Profile
DTR-07.03.02.08	The cRLDistributionPoints extension is required and must contain at least one URI, either LDAP or HTTP. If LDAP is used, the URI must include the DN of the entry containing the CRL and specify the directory attribute in which the CRL is located (certificateRevocationList). If HTTP is used, the URI must point to a file that has an extension of ".crl" that contains the DER encoded CRL. (see [RFC2585], *Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP*)	• [PROF], Worksheet titled - End Entity Signature Certificate Profile
DTR-07.03.02.09	The size of the public key for the digital signature certificate shall be in accordance with Table 3-1 of [SP800-78].	• [SP800-78], Section 3.1 - PIV Cryptographic Keys

DTR No:	DTR Description	Spec. Reference
DTR-07.03.02.10	The public key present in the digital signature certificate shall correspond to the digital signature private key.	• [SP800-157], Appendix B.1.2 - Derived PIV Application Data Model Elements
DTR-07.03.02.11	If the public key algorithm is RSA, the exponent shall be equal to 65 537.	• [SP800-78], Section 3.1, PIV Cryptographic Keys

562

563 ### 7.3.3 X.509 Certificate for Key Management

564 [SP800-157] doesn't specify requirements on the key management key and certificate. The
565 requirements listed herein follow those from [FIPS201] for key management certificates that are
566 not issued by legacy PKIs, and thus do not actually apply to the X.509 Certificate for Key
567 Management stored within a Derived PIV Application, with the exception that certificates that
568 assert the id-fpki-common-policy, id-fpki-common-hardware, or id-fpki-common-High
569 certificate policy OID are required by the corresponding certificate policy to conform to [PROF].

DTR No:	DTR Description	Spec. Reference
DTR-07.03.03.01	The signature field in the certificate shall specify an algorithm from Table 3-3 of [SP800-78] in the AlgorithmIdentifier.	• [SP800-78], Section 3.2.1 - Specification of Digital Signatures on Authentication Information
DTR-07.03.03.02	If RSA with PSS padding is used, the parameters field of the AlgorithmIdentifier type shall assert Secure Hash Algorithm (SHA) 256 (OID = 2.16.840.1.101.3.4.2.1). For the other RSA algorithms, the parameters field is populated with NULL. For ECDSA, the parameters field is absent.	• [PROF], Worksheet titled - Key Management Certificate Profile
DTR-07.03.03.03	The subjectPublicKeyInfo field shall assert an algorithm in the AlgorithmIdentifier in accordance with Table 3-4 of [SP800-78].	• [SP800-78], Section 3.2.2 - Specification of Public Keys In X.509 Certificates
DTR-07.03.03.04	If the public key algorithm is elliptic curve, then the parameters field contains the namedCurve choice populated with an appropriate OID from [SP800-78].	• [PROF], Worksheet titled - Key Management Certificate Profile
DTR-07.03.03.05	If the public key algorithm is RSA, then the keyUsage extension shall only assert the keyEncipherment bit. If the public key algorithm is elliptic curve, then the keyUsage	• [PROF], Worksheet titled - Key Management

DTR No:	DTR Description	Spec. Reference
	extension shall only assert the keyAgreement bit.	Certificate Profile
DTR-07.03.03.06	The policyIdentifier field in the certificatePolicies must assert one of the following: id-fpki-common-policy (OID = 2.16.840.1.101.3.2.1.3.6), id-fpki-common-hardware (OID = 2.16.840.1.101.3.2.1.3.7) or id-fpki-common-High (OID = 2.16.840.1.101.3.2.1.3.16).	• [PROF], Worksheet titled - Key Management Certificate Profile
DTR-07.03.03.07	The authorityInfoAccess field shall contain an id-ad-caIssuers (1.3.6.1.5.5.7.48.2) accessMethod. The access location shall to specify the location of an LDAP accessible directory server or HTTP accessible Web server where certificates issued to the issuer of this certificate may be found. If LDAP is used, the URI must include the DN of the entry containing the relevant certificates and specify the directory attribute in which the certificates are located. If the directory in which the certificates are stored expects the "binary" option to be specified, then the attribute type must be followed by ";binary" in the URI. If HTTP is used, the URI must point to a file that has an extension of ".p7c" containing a certs-only CMS message (see [RFC5751], *Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification*).	• [PROF], Worksheet titled - Key Management Certificate Profile
DTR-07.03.03.08	The cRLDistributionPoints extension is required and must contain at least one URI, either LDAP or HTTP. If LDAP is used, the URI must include the DN of the entry containing the CRL and specify the directory attribute in which the CRL is located (certificateRevocationList). If HTTP is used, the URI must point to a file that has an extension of ".crl" that contains the DER encoded CRL. (see [RFC2585], *Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP*)	• [PROF], Worksheet titled - Key Management Certificate Profile
DTR-07.03.03.09	The size of the public key for the key management certificate shall be in accordance with Table 3-1 of [SP800-78].	• [SP800-78], Section 3.1 - PIV Cryptographic Keys
DTR-07.03.03.10	The public key present in the key management	• [SP800-157],

DTR No:	DTR Description	Spec. Reference
	certificate shall correspond to the key management private key.	Appendix B.1.2 - Derived PIV Application Data Model Elements
DTR-07.03.03.11	If the public key algorithm is RSA, the exponent shall be equal to 65 537.	• [SP800-78], Section 3.1, PIV Cryptographic Keys

570

571 ### 7.3.4 X.509 Certificate for the Derived PIV Credential Issuer (Content Signing)[8]

DTR No:	DTR Description	Spec. Reference
DTR-07.03.04.01	The signature field in the certificate shall specify one of the following algorithm OIDs: 1.2.840.113549.1.10 (id-RSASSA-PSS), 1.2.840.113549.1.11 (Sha256WithRSAEncryption), 1.2.840.10045.4.3.2 (edsa-with-Sha256), or 1.2.840.10045.4.3.3 (edsa-with-Sha384).	• [PROF], Worksheet titled - Common PIV Content Signing Certificate Profile
DTR-07.03.04.02	If RSA with PSS padding is used, the parameters field of the AlgorithmIdentifier type shall assert SHA-256 (OID = 2.16.840.1.101.3.4.2.1). For RSA with PKCS #1 v1.5 padding, the parameters field is populated with NULL. For ECDSA, the parameters field is absent.	• [PROF], Worksheet titled - Common PIV Content Signing Certificate Profile
DTR-07.03.04.03	The subjectPublicKeyInfo field shall assert one of the following algorithm OIDs: 1.2.840.113549.1.1.1 (RSA Encryption) or 1.2.840.10045.2.1 (Elliptic curve key).	• [PROF], Worksheet titled - Common PIV Content Signing Certificate Profile
DTR-07.03.04.04	If the public key algorithm is elliptic curve, then the parameters field contains the namedCurve choice populated with one of the following OIDs: 1.2.840.10045.3.1.7 (Curve P-256) or 1.3.132.0.34 (Curve P-384).	• [PROF], Worksheet titled - Common PIV Content Signing Certificate Profile
DTR-07.03.04.05	The keyUsage extension shall assert the digitalSignature bit. No other bits shall be asserted.	• [PROF], Worksheet titled - Common PIV Content Signing Certificate Profile

[8] Located in the Security Object's Cryptographic Message Syntax (CMS) signature field (tag 0xBB).

DTR No:	DTR Description	Spec. Reference
DTR-07.03.04.06	The policyIdentifier field in the certificatePolicies must assert the following: id-fpki-common-contentSigning (2.16.840.1.101.3.2.1.3.39).	• [SP800-157], Appendix B.1.2 - Derived PIV Application Data Model Elements • [FIPS201], Section 4.2.1, Cardholder Unique Identifier (CHUID)
DTR-07.03.04.07	The extended key usage (extKeyUsage) extension shall assert the id-PIV-content-signing (OID = 2.16.840.1.101.3.6.7).	• [SP800-157], Appendix B.1.2 - Derived PIV Application Data Model Elements • [FIPS201], Section 4.2.1, Cardholder Unique Identifier (CHUID)
DTR-07.03.04.08	Certificates must include an authorityInfoAccess extension with at least one instance of the caIssuers access method (1.3.6.1.5.5.7.48.2) that specifies an HTTP URI that points to a location where certificates issued to the issuer of this certificate may be found. The HTTP URI must point to a file that has an extension of ".p7c" containing a certs-only CMS message (see RFC 5751, *Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification* [RFC5751]).	• [PROF], Worksheet titled - Common PIV Content Signing Certificate Profile
DTR-07.03.04.09	The cRLDistributionPoints extension is required and must contain at least URI, either LDAP or HTTP. If LDAP is used, the URI must include the DN of the entry containing the CRL and specify the directory attribute in which the CRL is located certificateRevocationList). If HTTP is used, the URI must point to a file that has an extension of ".crl" that contains the DER encoded CRL. (see [RFC2585], *Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP*)	• [PROF], Worksheet titled - Common PIV Content Signing Certificate Profile

DTR No:	DTR Description	Spec. Reference
DTR-07.03.04.10	The size of the subject public key in the Derived PIV Credential Issuer's (content signing) certificate shall conform to Table 3-2 in [SP800-78].	• [SP800-78], Section 3.2.1 – Specification of Digital Signatures on Authentication Information

572

8. Test Assertions for the Derived PIV Application

This section lists the test assertions used to determine conformity to the derived test requirements (DTR) listed in Section 6. The Implementation Under Test (IUT), in this case a Derived PIV Application submitted by a vendor, must meet the stated objective(s) of the assertion by way of a test or submission of documents/artifacts in order to be deemed conformant to the associated DTR(s).

8.1 Transport Layer Conformance

8.1.1 UICC

8.1.1.1 GlobalPlatform Support for UICC Tokens

Test Assertion	TA-08.01.01.01
Purpose	Confirms that for Universal Integrated Circuit Card (UICC) implementations used to host a Derived PIV Application, the UICC implements the GlobalPlatform Card Secure Element Configuration v1.0 [GPSE].
DTR(s)	• DTR-06.01.01.01
Vendor Documentation	The vendor to provide evidence in its documentation that the UICC that hosts the Derived PIV Application implements the GlobalPlatform Card Secure Element Configuration v1.0 [GPSE].

8.1.2 USB

8.1.2.1 ICCD Specification Support for USB Tokens

Test Assertion	TA-08.01.02.01
Purpose	Confirms that for USB Integrated Circuit(s) Card Devices (ICCD) implementations used to host a Derived PIV Application, the ICCD uses the Bulk-in/Bulk-Out command pipe for APDU transport and implements the Universal Serial Bus Device Class - Smart Card ICCD Specification for USB Integrated Circuit(s) Card Devices [ICCDSPEC].
DTR(s)	• DTR-06.01.02.01 • DTR-06.01.02.03
Vendor Documentation	The vendor to provide evidence in its documentation that the ICCD that hosts the Derived PIV Application implements the Universal Serial Bus Device Class - Smart Card ICCD Specification for USB Integrated Circuit(s) Card Devices [ICCDSPEC]. The vendor confirms that the APDUs are received from the secure element using the Bulk-In command pipe.

8.1.2.2 SP 800-96 Support for USB Tokens

Test Assertion	TA-08.01.02.02
Purpose	For a USB token that hosts a Derived PIV Application, confirm that the token is compliant with the specifications in [SP800-96] for APDU support for contact card readers.
DTR(s)	• DTR-06.01.02.02
Vendor Documentation	The vendor to provide evidence in its documentation that the USB token is compliant with the specifications in [SP800-96] for APDU support for contact card readers.

8.2 Derived PIV Application Data Object Access/Storage Conformance

8.2.1 General

8.2.1.1 Support for Contact Interface

Test Assertion	TA-08.02.01.01
Purpose	Confirms that the Derived PIV Application only supports a contact interface.
DTR(s)	• DTR-06.02.01.01
Vendor Documentation	The vendor to provide evidence in its documentation that the Derived PIV Application only supports a contact interface.

8.2.1.2 One Derived PIV Application

Test Assertion	TA-08.02.01.02
Purpose	Confirms that there is only one Derived PIV Application on any hardware cryptographic token.
DTR(s)	• DTR-06.02.01.02
Vendor Documentation	The vendor to provide information in its documentation validating the compliance with this requirement.

8.2.2 Derived PIV Application Data Objects and Representation

8.2.2.1 Derived PIV Application Data Objects

Test Assertion	TA-08.02.02.01
Purpose	Confirms the data objects (along with their access conditions) are implemented by the vendor of the Derived PIV Application per the specification.

DTR(s)	• DTR-06.02.02.01
Vendor Documentation	The vendor to provide documentation identifying all the data objects (mandatory and optional) implemented within the Derived PIV Application.

597

598 #### 8.2.2.2 Derived PIV Data Objects Container Capacity

Test Assertion	TA-08.02.02.02
Purpose	Confirms the container capacity for all Derived PIV data objects implemented on the Derived PIV Application.
DTR(s)	• DTR-06.02.02.02 • DTR-06.02.02.03 • DTR-06.02.02.04 • DTR-06.02.02.05 • DTR-06.02.02.06 • DTR-06.02.02.07 • DTR-06.02.02.08
Vendor Documentation	The vendor to provide in its documentation the implemented data objects with their minimum container sizes on the Derived PIV Application.

599

600 #### 8.2.2.3 Status Words

Test Assertion	TA-08.02.02.03
Purpose	Confirms that all return codes are implemented by the Derived PIV Application.
DTR(s)	• DTR-06.02.02.09
Vendor Documentation	The vendor to provide all the status codes returned by the Derived PIV Application for the various token interface commands in its documentation. The status codes are consistent with those specified in Section 5.6 of [SP800-73], Part 1.

601

602 #### 8.2.2.4 BER-TLV for the Derived PIV Data Objects

Test Assertion	TA-08.02.02.04
Purpose	Confirms the BER-TLV tags for the data objects implemented within the Derived PIV Application.
DTR(s)	• DTR-06.02.02.10
Vendor Documentation	The vendor to provide in its documentation the list of all the data objects implemented in the Derived PIV Application with the BER-TLV tags associated with each of them.

603

8.2.2.5 Key Reference Values

Test Assertion	TA-08.02.02.05
Purpose	Confirms that all the key references used on the Derived PIV Application interfaces are in accordance with Table 6-1 of [SP800-78] and Table 4a of [SP800-73], Part 1, with the mappings defined in Table B-2 of [SP800-157].
DTR(s)	• DTR-06.02.02.11
Vendor Documentation	The vendor to provide in its documentation the key references implemented by the Derived PIV Application.

8.2.2.6 Algorithm Identifiers

Test Assertion	TA-08.02.02.06
Purpose	Confirms that the required cryptographic algorithms and their identifiers are implemented by the Derived PIV Application.
DTR(s)	• DTR-06.02.02.12
Vendor Documentation	The vendor to provide in its documentation the cryptographic algorithms and their identifiers supported by the Derived PIV Application.

8.3 Derived PIV Application Command Interface Conformance

8.3.1 SELECT Command

8.3.1.1 Select using the Full and Truncated AID

Test Assertion	TA-08.03.01.01
Purpose	Verifies that the Derived PIV Application executes the SELECT token command for the following conditions: (i) long AID and (ii) right-truncated short AID. The application property template as specified by the vendor is returned.
DTR(s)	• DTR-06.02.01.03 • DTR-06.02.02.09 • DTR-06.03.02.01 • DTR-06.03.02.03 • DTR-06.03.02.04 • DTR-06.03.02.05
Vendor Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader.

	• Suitable drivers have been loaded between the test system and an instance of the reader.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the SELECT command without the version number • AID == 'A0 00 00 03 08 00 00 20 00'
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00' at the end. Check that the application property template conforms to Table 3 of [SP800-73], Part 2, with the exception that the returned AID is the AID listed in Section B.1.1 of [SP800-157]. 2. From Step 2, the command returns the application property template with the status word '90 00' at the end. Check that the application property template conforms to Table 3 of [SP800-73], Part 2, with the exception that the returned AID is the AID listed in Section B.1.1 of [SP800-157].
Postcondition(s)	The Derived PIV Application is now the currently selected application. The application security status of the Derived PIV Application is established.

8.3.1.2 Default Selected Application

Test Assertion	TA-08.03.01.02
Purpose	Confirms that a default selected application exists on the hardware token.
DTR(s)	• DTR-06.02.02.09 • DTR-06.03.02.02
Vendor Documentation	The vendor to provide information in its documentation stating which is the application selected by default within its implementation.

8.3.1.3 Select when Derived PIV Application is Currently Selected

Test Assertion	TA-08.03.01.03
Purpose	Verifies that the Derived PIV Application is not deselected while the currently selected application is the Derived PIV Application and the SELECT command is sent with an AID of the Derived PIV Application. The security status remains unchanged in this case.
DTR(s)	• DTR-06.02.02.09 • DTR-06.03.01.01 • DTR-06.03.01.02 • DTR-06.03.02.06
Vendor Documentation	None.

Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • The Derived PIV Application Password's retry counter is not 0.

Test Scenario	1. Send the SELECT command with
	  • AID == 'A0 00 00 03 08 00 00 20 00 01 00'
	2. Send the VERIFY command with
	  • P2, key reference value, is set to '80'
	  • Data field of the command will contain the correct Derived PIV Application Password, padded with 'FF' (if necessary) to complete the total length of the value to 8 bytes
	3. Repeat Step 1
	4. Send the GENERAL AUTHENTICATE command
	  • CLA is set to:
	  1. '00' if command chaining is not needed or '10' if command chaining is used. (The last chain of the command sets CLA to '00')
	  • P1, algorithm reference, is set to '07' or '11' P2, key reference, is set to '9A' indicating the Derived PIV Authentication key
	  • Data field in the command is to include '81' specifying a challenge, followed by a randomly generated challenge, and '82 00' in order to request a response

Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns status word '90 00'. 3. From Step 3, the command returns the application property template with the status word '90 00'. 4. From Step 4, the command returns the signed challenge with status word '90 00'.
Postcondition(s)	The Derived PIV Application is the currently selected application and the security status of the Derived PIV Application Password is TRUE.

615

616 **8.3.1.4 Select with an Invalid AID when Derived PIV Application is Currently Selected**

Test Assertion	TA-08.03.01.04
Purpose	Verifies that the Derived PIV Application is not deselected while the currently selected application is the Derived PIV Application and the SELECT command is sent with an AID that is not supported.
DTR(s)	• DTR-06.02.02.09 • DTR-06.03.01.02 • DTR-06.03.02.07
Vendor Documentation	None.

Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • The Derived PIV Application Password's retry counter is not 0.

Test Scenario	1. Send the SELECT command with
	  • AID == 'A0 00 00 03 08 00 00 20 00 01 00'
	2. Send the VERIFY command with
	  • P2, key reference value, is set to '80'
	  • Data field of the command will contain the correct Derived PIV Application Password, padded with 'FF' (if necessary) to complete the total length of the value to 8 bytes
	3. Repeat Step 1 with
	  • AID == 'A0 00 00 03 08 00 00 00 00' (invalid AID)
	4. Send the GENERAL AUTHENTICATE command
	  • CLA is set to:
	  1. '00' if command chaining is not needed or '10' if command chaining is used. (The last chain of the command sets CLA to '00')
	  • P1, algorithm reference, is set to '07' or '11'. P2, key reference, is set to '9A' indicating the Derived PIV Authentication Key
	  • Data field in the command is to include '81' specifying a challenge, followed by a randomly generated challenge, and '82 00' in order to request a response

Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns status word '90 00'. 3. From Step 3, the command returns '6A 82' (application not found). 4. From Step 4, the command returns the signed challenge with the status word '90 00'.
Postcondition(s)	The Derived PIV Application continues to be the currently selected application and the application security status of the Derived PIV Application Password is TRUE.

8.3.1.5 Select with Another Valid AID when Derived PIV Application is Currently Selected

Test Assertion	TA-08.03.01.05
Purpose	Confirms that the Derived PIV Application is deselected when the currently selected application is the Derived PIV Application and the SELECT command is sent with another valid AID that is supported.
DTR(s)	• DTR-06.03.02.08
Vendor Documentation	The vendor to provide information in its documentation validating compliance with this requirement.

620

621 ### 8.3.2 GET DATA Command

622 #### 8.3.2.1 Get Data for the Various Derived PIV Data Objects

Test Assertion	TA-08.03.02.01
Purpose	Verifies that the Derived PIV Application accepts the GET DATA command with the access rule of each container as specified in Table 2 of [SP800-73], Part 1 as mapped to [SP800-157]. This test is applicable to the mandatory and the optional data objects specified in [SP800-157].
DTR(s)	• DTR-06.02.02.09 • DTR-06.03.01.01 • DTR-06.03.03.01 • DTR-06.03.03.02 • DTR-06.03.03.03
Vendor Documentation	The vendor to provide information in its documentation stating all the optional data objects supported.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • The mandatory and optional data objects supported by the Derived PIV Application are loaded.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the GET DATA command with • Data field of the command containing the tag ('5FC105') of the X.509 Certificate for Derived PIV Authentication data object 3. If the X.509 Certificate for Digital Signature is supported, send the GET DATA command with • Data field of the command containing the tag ('5FC10A') of the X.509 Certificate for Digital Signature data object 4. If the X.509 Certificate for Key Management is supported, send the GET DATA command with • Data field of the command containing the tag ('5FC10B') of the X.509 Certificate for Key Management data object 5. If the Key History Object and the Retired X.509 Certificates for Key Management are supported, send the GET DATA command with A. Data field of the command containing the tag ('5FC10C') of the Key History Object B. Data field of the command containing the tag ('5FC10D' to '5FC120') of a Retired X.509 Certificate for Key Management (send a separate command for each supported Retired X.509 Certificate for Key Management)

	6. If the Discovery Object is supported, send the GET DATA command with • Data field of the command containing the tag ('7E') of the Discovery Object 7. If the Security Object is supported, send the GET DATA command with • Data field of the command containing the tag ('5FC106') of the Security Object 8. Send the GET DATA command with • Data field of the command containing a tag that does not identify any of the data objects within the Derived PIV Application.
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. For Steps 2, 3, 4, 5A, 5B, 6 and 7, each command returns the requested data object along with the status word '90 00'. 3. For Step 8, the command returns status word '6A 82' (data object not found).
Postcondition(s)	N/A

8.3.3 GENERAL AUTHENTICATE Command

8.3.3.1 Internal Authenticate with the Derived PIV Authentication Key

Test Assertion	TA-08.03.03.01
Purpose	Verifies that the Derived PIV Application responds to the GENERAL AUTHENTICATE command appropriately when authenticating to the test toolkit application.
DTR(s)	• DTR-06.02.02.09 • DTR-06.03.01.01 • DTR-06.03.01.02 • DTR-06.03.04.01 • DTR-06.03.04.05
Vendor Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • The Derived PIV Application Password is recorded. • The Derived PIV Application Password's retry counter is not 0.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the GENERAL AUTHENTICATE command • CLA is set to: 1. '00' if command chaining is not needed or 2. '10' if command chaining is used. (The last

	chain of the command sets CLA to '00') • P1, algorithm reference, is set to '07' or '11' • P2, key reference, is set to '9A' (the Derived PIV Authentication key) • Data field in the command is to include '81' specifying a challenge, followed by a randomly generated challenge, and '82 00' in order to request a response 3. Send the VERIFY command with • P2, key reference value, is set to '80' • Data field of the command will contain the correct Derived PIV Application Password, padded with 'FF' (if necessary) to complete the total length of the value to 8 bytes 4. Repeat Step 2
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns status word '69 82' (security status not satisfied). 3. From Step 3, the command returns status word '90 00'. 4. From Step 4, the command returns the signed challenge with status word '90 00'. Verify the signed challenge.
Postcondition(s)	N/A

8.3.3.2 Internal Authenticate with the Derived PIV Authentication Key (with an Invalid Algorithm Reference and Data Length)

Test Assertion	TA-08.03.03.02
Purpose	Verifies that the Derived PIV Application responds to the GENERAL AUTHENTICATE command appropriately when authenticating to the test toolkit application using an invalid algorithm reference or data length.
DTR(s)	• DTR-06.02.02.09 • DTR-06.03.01.01 • DTR-06.03.01.02 • DTR-06.03.04.01 • DTR-06.03.04.05
Vendor Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • The Derived PIV Application Password is recorded. • The Derived PIV Application Password's retry counter is not 0.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00'

	2. Send the VERIFY command with • P2, key reference value, is set to '80' • Data field of the command will contain the correct Derived PIV Application Password, padded with 'FF' (if necessary) to complete the total length of the value to 8 bytes 3. Send the GENERAL AUTHENTICATE command • CLA is set to: 1. '00' if command chaining is not needed or 2. '10' if command chaining is used. (The last chain of the command sets CLA to '00') • P1, algorithm reference, is set to something other than '07' or '11' (indicating an invalid algorithm reference) • P2, key reference, is set to '9A' (the Derived PIV Authentication key) • Data field in the command is to include '81' specifying a challenge, followed by a randomly generated challenge, and '82 00' in order to request a response 4. Send the GENERAL AUTHENTICATE command • CLA is set to: 1. '00' if command chaining is not needed or 2. '10' if command chaining is used. (The last chain of the command sets CLA to '00') • P1, algorithm reference, is set to '07' or '11' • P2, key reference, is set to '9A' (the Derived PIV Authentication key) • Data field in the command is to include '81' specifying a challenge, followed by a randomly generated challenge (which is of incorrect length based on the chosen algorithm [e.g., challenge is greater than they key size]), and '82 00' in order to request a response
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns status word '90 00'. 3. From Step 3, the command returns status word '6A 86' (incorrect parameter in P1 or P2). 4. From Step 4, the command returns status word '6A 80' (incorrect parameter in command data field).
Postcondition(s)	N/A

8.3.3.3 Mutual Authenticate with Derived PIV Token Management Key

Test Assertion	TA-08.03.03.03
Purpose	Verifies that the Derived PIV Application responds to the GENERAL AUTHENTICATE command appropriately when mutually authenticating to the test toolkit application using the Derived PIV Token Management Key (if supported).

DTR(s)	• DTR-06.02.02.09 • DTR-06.03.01.01 • DTR-06.03.04.01 • DTR-06.03.04.05
Vendor Documentation	The vendor to provide in its documentation whether the Derived PIV Token Management Key is supported, and if yes, the value of the key.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the GENERAL AUTHENTICATE command • CLA is set to '00' • P1, algorithm reference, is set to '00', '03', '08', '0A', or '0C' • P2, key reference, is set to '9B' • Data field in the command is to include '80' requesting a witness from the Derived PIV Application 3. Send the GENERAL AUTHENTICATE command • CLA is set to '00' • P1, algorithm reference is set to the same value as specified in Step 2. • P2, key reference is set to '9B' Data field in the command is to include '80' followed by decryption of the witness sent by the Derived PIV Application and '81' followed by a challenge and then '82 00'
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns with the witness followed by status word '90 00'. 3. From Step 3, the Derived PIV Application verifies the decrypted witness and then responds with encryption of the challenge sent by Test Toolkit Application followed by status word '90 00'. Decrypt the encrypted challenge and compare it to the one sent to the token.
Postcondition(s)	N/A

8.3.3.4 External Authenticate with Derived PIV Token Management Key

Test Assertion	TA-08.03.03.04
Purpose	Verifies that the Derived PIV Application responds to the GENERAL AUTHENTICATE command appropriately when externally authenticating to the test toolkit application using the Derived PIV Token Management Key (if supported).
DTR(s)	• DTR-06.02.02.09

	• DTR-06.03.01.01 • DTR-06.03.04.01 • DTR-06.03.04.05
Vendor Documentation	The vendor to provide in its documentation whether the Derived PIV Token Management Key is supported and if yes, the value of the key.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the GENERAL AUTHENTICATE command • CLA is set to '00' • P1, algorithm reference, is set to '00', '03', '08', '0A', or '0C' • P2, key reference, is set to '9B' • Data field in the command is to include '81' followed by '00' indicating it is a request for challenge 3. Send the GENERAL AUTHENTICATE command • CLA is set to '00' • P1, algorithm reference, is set to the same value as in Step 2 • P2, key reference, is set to '9B' • Data field in the command is to include '82' followed by an encrypted challenge
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns a challenge followed by status word '90 00'. 3. From Step 3, the Test Toolkit Application responds with encryption of the challenge sent by Derived PIV Application. The token returns status word '90 00'.
Postcondition(s)	N/A

633

634 **8.3.3.5 General Authenticate with the Digital Signature Key**

Test Assertion	TA-08.03.03.05
Purpose	Verifies that the Derived PIV Application responds to the GENERAL AUTHENTICATE command appropriately when signing using the digital signature key.
DTR(s)	• DTR-06.02.02.09 • DTR-06.03.01.01DTR-06.03.01.02 • DTR-06.03.04.02 • DTR-06.03.04.05
Vendor	None.

Documentation	
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • The Derived PIV Application Password is recorded. • The Derived PIV Application Password's retry counter is not 0.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the GENERAL AUTHENTICATE command • CLA is set to: 1. '00' if command chaining is not needed or 2. '10' if command chaining is used. (The last chain of the command sets CLA to '00') • P1, algorithm reference, is set to '07', '11' or '14' • P2, key reference, is set to '9C' indicating the digital signature key • Data field in the command is to include '81' specifying a challenge, followed by a randomly generated challenge, and '82 00' in order to request a response 3. Send the VERIFY command with • P2, key reference value, is set to '80' • Data field of the command will contain the correct Derived PIV Application Password, padded with 'FF' (if necessary) to complete the total length of the value to 8 bytes 4. Repeat Step 2 5. Repeat Step 2
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns status word '69 82' (security status not satisfied). 3. From Step 3, the command returns status word '90 00'. 4. From Step 4, the command returns the signed challenge with status word '90 00'. Verify the signature using the public key from the digital signature certificate and the challenge sent to the token. 5. From Step 5, the command returns status word '69 82' (security status not satisfied), since the digital signature key has a "PIN Always" security condition.
Postcondition(s)	N/A

8.3.3.6 Internal Authenticate with the Digital Signature Key (with Invalid Algorithm Reference and Data Length)

Test Assertion	TA-08.03.03.06

Purpose	Verifies that the Derived PIV Application responds to the GENERAL AUTHENTICATE command appropriately when signing using the digital signature key with an invalid algorithm reference or data length.
DTR(s)	• DTR-06.02.02.09 • DTR-06.03.01.01 • DTR-06.03.01.02 • DTR-06.03.04.02 • DTR-06.03.04.05
Vendor Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • The Derived PIV Application Password is recorded. • The Derived PIV Application Password's retry counter is not 0.

Test Scenario	1. Send the SELECT command with
	  • AID == 'A0 00 00 03 08 00 00 20 00 01 00'
	2. Send the VERIFY command with
	  • P2, key reference value, is set to '80'
	  • Data field of the command will contain the correct Derived PIV Application Password, padded with 'FF' (if necessary) to complete the total length of the value to 8 bytes
	3. Send the GENERAL AUTHENTICATE command
	  • CLA is set to:
	  1. '00' if command chaining is not needed or
	  2. '10' if command chaining is used. (The last chain of the command sets CLA to '00')
	  • P1, algorithm reference, is set to something other than '07', '11' or '14' (indicating an invalid algorithm reference)
	  • P2, key reference, is set to '9C' indicating the digital signature key
	  • Data field in the command is to include '81' specifying a challenge, followed by a randomly generated challenge, and '82 00' in order to request a response
	4. Send the VERIFY command with
	  • P2, key reference value, is set to '80'
	  • Data field of the command will contain the correct Derived PIV Application Password, padded with 'FF' (if necessary) to complete the total length of the value to 8 bytes
	5. Send the GENERAL AUTHENTICATE command
	  • CLA is set to:
	  1. '00' if command chaining is not needed or
	  2. '10' if command chaining is used. (The last chain of the command sets CLA to '00')
	  • P1, algorithm reference, is set to '07', '11' or

	'14' • P2, key reference, is set to '9C' indicating the digital signature key • Data field in the command is to include '81' specifying a challenge, followed by a randomly generated challenge (with an incorrect length based on the chosen algorithm [e.g., challenge is greater than they key size]), and '82 00' in order to request a response
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns status word '90 00'. 3. From Step 3, the command returns status word '6A 86' (incorrect parameter in P1 or P2). 4. From Step 4, the command returns status word '90 00'. 5. From Step 5, the command returns status word '6A 80' (incorrect parameter in command data field).
Postcondition(s)	N/A

638

639 **8.3.3.7 General Authenticate with the Key Management Key**

Test Assertion	TA-08.03.03.07
Purpose	Verifies that the Derived PIV Application responds to the GENERAL AUTHENTICATE command appropriately when using the key management key.
DTR(s)	• DTR-06.02.02.09 • DTR-06.03.01.01 • DTR-06.03.01.02 • DTR-06.03.04.03 • DTR-06.03.04.05
Vendor Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • The Derived PIV Application Password is recorded. • The Derived PIV Application Password's retry counter is not 0.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the GENERAL AUTHENTICATE command • CLA is set to: 1. '00' if command chaining is not needed or 2. '10' if command chaining is used. (The last chain of the command sets CLA to '00') • P1, algorithm reference, is set to '07', '11' or '14'

	• P2, key reference, is set to '9D' indicating the key management key • Data field in the command is to include one of the following: 1. If P1 = '07', the template '81' contains an encrypted key 2. If P1 = '11' or '14', the template '85' contain the other party's public key.[9] 3. Send the VERIFY command with • P2, key reference value, is set to '80' • Data field of the command will contain the correct Derived PIV Application Password value, padded with 'FF' (if necessary) to complete the total length of the value to 8 bytes 4. Repeat Step 2 5. Send the GENERAL AUTHENTICATE command • CLA is set to: 1. '00' if command chaining is not needed or 2. '10' if command chaining is used. (The last chain of the command sets CLA to '00') • P1, algorithm reference, is set to something other than '07', '11' or '14' (indicating incorrect algorithm) • P2, key reference, is set to '9D' indicating the key management key • Data field in the command is to include a template appropriate for the '9D' key. 6. Send the GENERAL AUTHENTICATE command • CLA is set to: 1. '00' if command chaining is not needed or 2. '10' if command chaining is used. (The last chain of the command sets CLA to '00') • P1, algorithm reference, is set to '07', '11' or '14' • P2, key reference, is set to '9D' indicating the key management key • Data field in the command is to include a malformed template.
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns status word '69 82' (security status not satisfied). 3. From Step 3, the command returns status word '90 00'. 4. From Step 4, for algorithm reference '07' as P1 value, the command returns the transported key with status word '90 00'. Compare the test toolkit application's copy of the plaintext key to the one received in the response from the token. For algorithm reference '11' or '14' as P1 value, the command returns the shared secret Z[10] with

[9] Template '85' contains the other party's public key, a point on Curve P-256 or P-384, encoded as '04' || X || Y, without the use of point compression, as described in Section 2.3.3 of [SEC1].
[10] Z is the X coordinate of point P as defined in [SP800-56A], Section 5.7.1.2

	status word '90 00'. Compare the shared secret computed by the token with the shared secret computed off token. 5. From Step 5, the command returns status word '6A 86' (incorrect parameter in P1 or P2). 6. From Step 6, the command returns status word '6A 80' (incorrect parameter in command data field).
Postcondition(s)	N/A

640

641 **8.3.3.8 General Authenticate with the Retired Key Management Keys**

Test Assertion	TA-08.03.03.08
Purpose	Verifies that the Derived PIV Application responds to the GENERAL AUTHENTICATE command appropriately when using the retired key management keys.
DTR(s)	• DTR-06.02.02.03 • DTR-06.03.01.01 • DTR-06.03.04.03 • DTR-06.03.04.05
Vendor Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • The Derived PIV Application Password is recorded. • The Derived PIV Application Password's retry counter is not 0.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the VERIFY command with • P2, key reference value, is set to '80' • Data field of the command will contain the correct Derived PIV Application Password value, padded with 'FF' (if necessary) to complete the total length of the value to 8 bytes 3. Send the GET DATA command with • Data field of the command containing the tag of the Key History Object data object ('5FC10C'). Retrieve the key history's data elements: • If keysWithOnCardCerts = 0 and keysWithOffCardCerts > 0 o Read the certificate(s) and key references (pairs) from the vendor provided URL file. For each key reference value in the range (0x95 – keysWithOffCardCerts + 1) through 0x95, verify that the provided URL file includes that key reference, issue a

	challenge for that key reference (follow Step 2 from TA-08.03.03.07), and verify the response using the public key from the corresponding certificate from the provided URL file • If keysWithOnCardCerts > 0 and keyWithOffCardCerts = 0 o For each key reference value in the range 0x82 through (0x82 + keysWithOnCardCerts – 1), read the certificates from the token and issue a challenge for each retired private key[11] (follow Step 2 from TA-08.03.03.07), and verify the response using the public key from the corresponding certificate. • If keysWithOnCardCerts > 0 and keyWithOffCardCerts > 0 For each key reference value in the range 0x82 through (0x82 + keysWithOnCardCerts – 1) and in the range (0x95 – keysWithOffCardCerts + 1) through 0x95, verify that the provided URL file includes that key reference, issue a challenge for that key reference (follow Step 2 from TA-08.03.03.07), and verify the response using the public key from the corresponding certificate from the provided URL file.
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns status word '90 00'. 3. From Step 3, the GET DATA commands return the requested data along with status word '90 00'. Each GENERAL AUTHENTICATE command: a. For key transport (as indicated by algorithm reference '07' as P1 value), the command returns the transported key with status word '90 00' at the end. Compare the test toolkit application's copy of the plaintext key to the one received in the response from the token. b. For ECDH, (as indicated by algorithm reference '11' or '14' as P1 value), the command returns the shared secret Z with status word '90 00'. Compare the shared secret computed by the token with the shared secret computed off token.
Postcondition(s)	N/A

8.3.3.9 Internal Authenticate with an Invalid Key Reference

Test Assertion	TA-08.03.03.09

[11] See Table 7 of [SP800-73], Part 1 for the association of certificate BER-TLV tags to corresponding key reference values.

Purpose	Verifies that the Derived PIV Application responds to the GENERAL AUTHENTICATE command appropriately when authenticating to the test toolkit application using an invalid key reference.
DTR(s)	• DTR-06.02.02.09 • DTR-06.03.01.01 • DTR-06.03.01.02 • DTR-06.03.04.01 • DTR-06.03.04.02 • DTR-06.03.04.03 • DTR-06.03.04.04 • DTR-06.03.04.05
Vendor Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • The Derived PIV Application Password is recorded. • The Derived PIV Application Password's retry counter is not 0.

Test Scenario	1. Send the SELECT command with
	  • AID == 'A0 00 00 03 08 00 00 20 00 01 00'
	2. Send the VERIFY command with
	  • P2, key reference value, is set to '80'
	  • Data field of the command will contain the correct Derived PIV Application Password, padded with 'FF' (if necessary) to complete the total length of the value to 8 bytes
	3. Send the GENERAL AUTHENTICATE command
	  • CLA is set to:
	  1. '00' if command chaining is not needed or
	  2. '10' if command chaining is used. (The last chain of the command sets CLA to '00')
	  • P1, algorithm reference, is set to '07' or '11'
	  • P2, key reference, is set to an incorrect key reference (one that is not supported)
	  • Data field in the command is to include '81' specifying a challenge, followed by a randomly generated challenge, and '82 00' in order to request a response

Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns status word '90 00'. 3. From Step 3, the command returns status word '6A 86' (incorrect parameter in P1 or P2).
Postcondition(s)	N/A

644

8.3.3.10 Support for Command Chaining

Test Assertion	TA-08.03.03.10
Purpose	Confirms that the Derived PIV Application responds to the GENERAL AUTHENTICATE command and supports command chaining to permit the uninterrupted transmission of long command data fields to the Derived PIV Application.
DTR(s)	• DTR-06.03.04.04 • DTR-06.03.04.05
Vendor Documentation	The vendor to provide information in its documentation demonstrating compliance to this requirement. The GET RESPONSE command is used to return the complete result of the cryptographic operation. In addition, if a token command other than the GENERAL AUTHENTICATE command is received by the Derived PIV Application before the termination of a GENERAL AUTHENTICATE chain, the Derived PIV Application rolls back to the state it was in immediately prior to the reception of the first command in the interrupted chain.

8.3.4 VERIFY Command

8.3.4.1 Verify with a Valid Key Reference and the Correct Password

Test Assertion	TA-08.03.04.01
Purpose	Verifies that the Derived PIV Application responds to the VERIFY command with a valid key reference and sets the security status appropriately when the correct password is provided.
DTR(s)	• DTR-06.02.02.09 • DTR-06.02.02.13 • DTR-06.03.01.01 • DTR-06.03.01.02 • DTR-06.03.05.01
Vendor Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • The Derived PIV Application Password is recorded. • The Derived PIV Application Password's retry counter is not 0.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the VERIFY command with • P2, key reference value, is set to '80' • Data field of the command will contain the correct Derived PIV Application Password,

	padded with 'FF' (if necessary) to complete the total length of the value to 8 bytes 3. Send the GENERAL AUTHENTICATE command • CLA is set to: 1. '00' if command chaining is not needed or 2. '10' if command chaining is used. (The last chain of the command sets CLA to '00') • P1, algorithm reference, is set to '07' or '11'. P2, key reference, is set to '9A' indicating the Derived PIV Authentication key • Data field in the command is to include '81' specifying a challenge, followed by a randomly generated challenge, and '82 00' in order to request a response
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns status word '90 00'. 3. From Step 3, the command returns the signed challenge with status word '90 00'.
Postcondition(s)	N/A

649

650 **8.3.4.2 Verify and Reset Security Status**

Test Assertion	TA-08.03.04.03
Purpose	Verifies that the Derived PIV Application responds to the VERIFY command for resetting the security status with the correct key reference.
DTR(s)	• DTR-06.02.02.09 • DTR-06.03.01.01 • DTR-06.03.01.02 • DTR-06.03.05.01 • DTR-06.03.05.05
Vendor Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • The Derived PIV Application Password is recorded. • The Derived PIV Application Password's retry counter is not 0.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the VERIFY command with • P2, key reference value, is set to '80' • Data field of the command will contain the correct Derived PIV Application Password,

	padded with 'FF' (if necessary) to complete the total length of the value to 8 bytes 3. Reset the security status of the '80' key reference by sending the VERIFY command with • P2, key reference value, is set to '80' • P1 parameter is 'FF' and both L_c and the data field are absent 4. Send the GENERAL AUTHENTICATE command • CLA is set to: 1. '00' if command chaining is not needed or 2. '10' if command chaining is used. (The last chain of the command sets CLA to '00') • P1, algorithm reference, is set to '07' or '11'. P2, key reference, is set to '9A' indicating the Derived PIV Authentication key • Data field in the command is to include '81' specifying a challenge, followed by a randomly generated challenge, and '82 00' in order to request a response
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns status word '90 00'. 3. From Step 3, the command returns status word '90 00'. 4. From Step 4, the command returns status word '69 82' (security status not satisfied).
Postcondition(s)	N/A

651

652 **8.3.4.3 Verify with an Incorrect Length and Padding for the Current Password**

Test Assertion	TA-08.03.04.04
Purpose	Verifies that the Derived PIV Application responds correctly to the VERIFY command when the password length and padding requirements are not met.
DTR(s)	• DTR-06.02.02.09 • DTR-06.02.02.14 • DTR-06.03.01.01
Vendor Documentation	The vendor to provide in its documentation the status word returned by the Derived PIV Application when the password length or padding requirements are not met.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • The Derived PIV Application Password is recorded. The password shall be 6 bytes in length. • The Derived PIV Application Password's retry counter is greater

	than 1.[12]
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the VERIFY command with • P2, key reference value, is set to '80' • Data field of the command will contain the correct Derived PIV Application Password, NOT padded with 'FF', so that the total length of the value is less than 8 bytes 3. Send the VERIFY command with • P2, key reference value, is set to '80' • Data field of the command will contain the correct Derived PIV Application Password, padded with 'FF' to complete the total length of the value to 10 bytes 4. Send the VERIFY command with • P2, key reference value, is set to '80' • Data field of the command will contain the correct Derived PIV Application Password, padded to 8 bytes with 'FF' in byte 7 and 'AA' in byte 8 5. Send the VERIFY command with • P2, key reference value, is set to '80' • Data field of the command will contain an arbitrary Derived PIV Application Password which is only 5 bytes in length padded with 'FF' to complete the total length of the value to 8 bytes
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns status word '6A 80' (incorrect parameter in command data field) or '63 CX' (verification failed, with X indicating the number of further allowed retries) (verify the error code supplied matches what is described in vendor documentation). 3. From Step 3, the command returns status word '6A 80' (incorrect parameter command data field) or '63 CX' (verification failed, with X indicating the number of further allowed retries (verify the error code supplied matches what is described in vendor documentation). 4. From Step 4, the command returns status word '6A 80' (incorrect parameter in command data field) or '63 CX' (verification failed, with X indicating the number of further allowed retries) (verify the error code supplied matches what is described in vendor documentation). 5. From Step 5, the command returns status word '6A 80' (incorrect parameter in command data field) or '63 CX' (verification failed,

[12] It may be necessary to perform a successful VERIFY command while performing the test scenario in order to keep the Derived PIV Application Password's retry counter from dropping to 0.

	with X indicating the number of further allowed retries) (verify the error code supplied matches what is described in vendor documentation).
Postcondition(s)	N/A

653

654 **8.3.4.4 Verify with an Incorrect Format for the Current Password**

Test Assertion	TA-08.03.04.05
Purpose	Verifies that the Derived PIV Application responds appropriately to the VERIFY command when an incorrectly formatted password is passed.
DTR(s)	• DTR-06.02.02.09 • DTR-06.02.02.13 • DTR-06.02.02.14 • DTR-06.02.02.15 • DTR-06.03.01.01
Vendor Documentation	The vendor to provide in its documentation the status word returned by the Derived PIV Application when the password format requirements are not met.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • The Derived PIV Application Password is recorded. • The Derived PIV Application Password's retry counter is greater than 1.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the VERIFY command with • P2, key reference value, is set to '80' • Data field of the command will contain an arbitrary Derived PIV Application Password where the first byte is 0x5B and all other non-padded bytes contain values limited to either 0x30–0x39 or 0x41–0x5A or 0x61–0x7A, padded with 'FF' to complete the total length of the value to 8 bytes 3. Repeat Step 2 five times with byte positions 2, 3, 4, 5, and 6 containing the 0x5B byte, respectively. Note: It may be necessary to send the VERIFY command with a correct Derived PIV Application Password in order to prevent the retry counter from decrementing to zero.
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns status word '6A 80' (incorrect

	parameter in command data field) or '63 CX' (verification failed, with X indicating the number of further allowed retries). Verify the error code supplied matches what is described in the vendor's documentation. 3. From Step 3, all commands return status word '6A 80' (incorrect parameter command data field) or '63 CX' (verification failed, with X indicating the number of further allowed retries). Verify the error code supplied matches what is described in the vendor's documentation.
Postcondition(s)	N/A

8.3.4.5 Verify with an Incorrect Password/Blocking the Derived PIV Application

Test Assertion	TA-08.03.04.06
Purpose	Verifies that the Derived PIV Application is blocked based on the retry counter when a correctly formatted, but incorrect password is sent repeatedly using the VERIFY command.
DTR(s)	• DTR-06.02.02.09 • DTR-06.03.01.01 • DTR-06.03.05.02 • DTR-06.03.05.03 • DTR-06.03.05.04
Vendor Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • The Derived PIV Application Password is recorded. • The Derived PIV Application Password's retry counter is not 0.

Test Scenario	1. Send the SELECT command with
	  • AID == 'A0 00 00 03 08 00 00 20 00 01 00'
	2. Send the VERIFY command repeatedly, until after the issuer specified maximum number of password tries is exceeded with
	  • P2, key reference value, is set to '80'
	  • Data field of the command will contain an arbitrary, but correctly formatted, password value other than what is obtained from the vendor, padded with 'FF' (if necessary) to complete the total length of the value to 8 bytes
	3. Send the VERIFY command after the issuer specified maximum number of password tries is exceeded with
	  • P2, key reference value, is set to '80'
	  • Data field of the command will contain the correct password value, padded with 'FF' (if necessary) to complete the total length of the

	value to 8 bytes
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns status word '63 CX' until the maximum number of password tries is reached (X indicates the number of further allowed retries). The command returns status word '69 83' (authentication method blocked) when the maximum number of password tries is exceeded. 3. From Step 3, the command returns status word '69 83' (authentication method blocked).
Postcondition(s)	The Derived PIV Application Password's retry counter is 0.

8.3.5 CHANGE REFERENCE DATA Command

8.3.5.1 Change Reference Data with the Correct Derived PIV Application Password and with the Correct PUK

Test Assertion	TA-08.03.05.01
Purpose	Verifies that the Derived PIV Application can change the current password with CHANGE REFERENCE DATA command.
DTR(s)	• DTR-06.02.02.09 • DTR-06.03.01.01 • DTR-06.03.05.06 • DTR-06.03.06.01 • DTR-06.03.06.03
Vendor Documentation	The vendor to provide in its documentation the reset retry value of the Derived PIV Application Password
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • The Derived PIV Application Password and PUK are recorded. • The Derived PIV Application Password's retry counter and the PUK's retry counter are not 0.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the CHANGE REFERENCE DATA command with • P2, key reference value, is set to '80' • Data field of the command will contain the correct password value (password 1), concatenated without delimitation with an arbitrary new valid password value (password 2). Both passwords should be padded (if needed) with 'FF' to complete the total length of each value to 8 bytes 3. Send the VERIFY command with • P1, is set to 'FF'

	• P2, key reference value, is set to '80' • L_C and the command data field are absent 4. Send the VERIFY command with • P1, is set to '00' • P2, key reference value, is set to '80' • L_C and the command data field are absent 5. Send the VERIFY command with • P2, key reference value, is set to '80' • Data field of the command will contain the new password value (password 2 from Step 2), padded with 'FF' (if necessary) to complete the total length of the value to 8 bytes Perform Step 6 only if the Derived PIV Application supports changing the PUK with the CHANGE REFERENCE DATA command. 6. Send the CHANGE REFERENCE DATA command with • P2, key reference value, is set to '81' • Data field of the command will contain the correct PUK value, concatenated without delimitation with an arbitrary new PUK value.
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns status word '90 00'. The password has now been changed. 3. From Step 3, the command returns status word '90 00' and the security status of the PIN is reset. 4. From Step 4, the command returns status word '63 CX' where X is equal to the reset retry value of the Derived PIV Application Password. 5. Form Step 5, the command returns status word '90 00' 6. From Step 6, the command returns status word '90 00' and the PUK value has been changed.
Postcondition(s)	The Derived PIV Application Password and PUK (if supported) are changed.

8.3.5.2 Change Reference Data with an Invalid Key Reference

Test Assertion	TA-08.03.05.02
Purpose	Verifies that the Derived PIV Application does not change the password with the CHANGE REFERENCE DATA command with an invalid key reference.
DTR(s)	• DTR-06.02.02.09 • DTR-06.03.01.01 • DTR-06.03.06.02
Vendor Documentation	None.

Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • The Derived PIV Application Password is recorded. • The Derived PIV Application Password's retry counter is not 0.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the CHANGE REFERENCE DATA command with • P2, key reference value, is set to something that is not '80' or '81' • Data field of the command will contain the correct password value (password 1), concatenated without delimitation with an arbitrary new valid password value (password 2). Both passwords are padded with 'FF' (if necessary) to complete the total length of each value to 8 bytes 3. Send the VERIFY command with • P2, key reference value, is set to '80' • Data field of the command will contain the password value (password 1), padded with 'FF' (if necessary) to complete the total length of the value to 8 bytes
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns an error status word. 3. From Step 3, the command returns status word '90 00'.
Postcondition(s)	The original password ('80') is still in effect.

8.3.5.3 Change Reference Data with an Incorrect Length and Padding for the New Password or with an Incorrect Length of New PUK

Test Assertion	TA-08.03.05.03
Purpose	Verifies that the Derived PIV Application responds appropriately to the CHANGE REFERENCE DATA command when the length and padding requirements of the new password are not met or when the length of the new PUK is incorrect.
DTR(s)	• DTR-06.02.02.09 • DTR-06.02.02.14 • DTR-06.03.01.01 • DTR-06.03.06.05 • DTR-06.03.06.06 • DTR-06.03.06.08
Vendor Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an

	appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • The Derived PIV Application Password and PUK are recorded. • The Derived PIV Application Password's retry counter and the PUK's retry counter are not 0.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the CHANGE REFERENCE DATA command with • P2, key reference value, is set to '80' • Data field of the command will contain the correct password value (password 1) padded to 8 bytes with 'FF' (if necessary) concatenated without delimitation with an arbitrary new password value (password 2) that is padded to less than 8 bytes 3. Send the CHANGE REFERENCE DATA command with • P2, key reference value, is set to '80' • Data field of the command will contain the correct password value (password 1) padded to 8 bytes with 'FF' (if necessary) concatenated without delimitation with an arbitrary new password value (password 2) that is 6 bytes but padded to 8 bytes with 'FF' in byte 7 and 'AA' in byte 8 4. Send the CHANGE REFERENCE DATA command with • P2, key reference value, is set to '80' • Data field of the command will contain the correct password (password 1) padded to 8 bytes with 'FF' (if needed) concatenated without delimitation with an arbitrary new password (password 2) that is less than 6 bytes but padded to 8 bytes with 'FF' 5. Send the CHANGE REFERENCE DATA command with • P2, key reference value, is set to '80' • Data field of the command will contain the correct password (password 1) padded to 8 bytes with 'FF'(if necessary) concatenated without delimitation with an arbitrary new password (password 2) that is greater than 8 bytes in length Perform Steps 6 and 7 only if the Derived PIV Application supports changing the PUK with the CHANGE REFERENCE DATA command. 6. Send the CHANGE REFERENCE DATA command with • P2, key reference value, is set to '81' • Data field of the command will contain the correct PUK value (PUK 1) concatenated without delimitation with an arbitrary new PUK value (PUK 2) that is less than 8 bytes in length 7. Send the CHANGE REFERENCE DATA command with • P2, key reference value, is set to '81' • Data field of the command will contain the

	correct PUK (PUK 1) concatenated without delimitation with an arbitrary new PUK (PUK 3) that is greater than 8 bytes in length
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns status word '6A 80' (incorrect parameter in command data field). 3. From Step 3, the command returns status word '6A 80' (incorrect parameter in command data field). 4. From Step 4, the command returns status word '6A 80' (incorrect parameter in command data field). 5. From Step 5, the command returns status word '6A 80' (incorrect parameter in command data field). 6. From Step 6, the command returns status word '6A 80' (incorrect parameter in the command data field). 7. From Step 7, the command returns status word '6A 80' (incorrect parameter in the command data field).
Postcondition(s)	Neither the password nor the PUK value has changed.

8.3.5.4 Change Reference Data with an Incorrect Format for the New Password

Test Assertion	TA-08.03.05.04
Purpose	Verifies that the Derived PIV Application responds appropriately to the CHANGE REFERENCE DATA command when the new password does not satisfy the format requirements.
DTR(s)	• DTR-06.02.02.09 • DTR-06.02.02.14 • DTR-06.03.01.01 • DTR-06.03.06.05 • DTR-06.03.06.06 • DTR-06.03.06.08
Vendor Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • The Derived PIV Application Password is recorded. • The Derived PIV Application Password's retry counter is not 0.

Test Scenario	1. Send the SELECT command with
	  • AID == 'A0 00 00 03 08 00 00 20 00 01 00'
	2. Send the CHANGE REFERENCE DATA command with
	  • P2, key reference value, is set to '80'
	  • Data field of the command will contain the correct password (password 1) padded to 8 bytes

	with 'FF' (if needed) concatenated without delimitation with an arbitrary new password value that contains 0x5B in the first byte position, all other non-padded bytes contain values limited to either 0x30–0x39 or 0x41–0x5A or 0x61–0x7A (password 2). Both passwords should be padded with 'FF'(as needed) to complete the total length of each value to 8 bytes (repeat test five times with byte positions 2, 3, 4, 5, and 6 containing the 0x5B byte, respectively)
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, each time the command returns status word '6A 80' (incorrect parameter in command data field).
Postcondition(s)	Current password is unchanged.

668

669 **8.3.5.5 Change Reference Data with an Incorrect Format for the Current Password**

Test Assertion	TA-08.03.05.05
Purpose	Verifies that the Derived PIV Application responds appropriately to the CHANGE REFERENCE DATA command when the current password format requirements are not met.
DTR(s)	• DTR-06.02.02.09 • DTR-06.02.02.14 • DTR-06.03.01.01 • DTR-06.03.06.05 • DTR-06.03.06.08
Vendor Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • The Derived PIV Application Password is recorded. • The Derived PIV Application Password's retry counter is not 0.

Test Scenario	1. Send the SELECT command with
	  • AID == 'A0 00 00 03 08 00 00 20 00 01 00'
	2. Send the CHANGE REFERENCE DATA command with
	  • P2, key reference value, is set to '80'
	  • Data field of the command will contain an arbitrary password value that contains 0x5B in the first byte position, all other non-padded bytes contain values limited to either 0x30–0x39 or 0x41–0x5A or 0x61–0x7A concatenated without delimitation with a properly formatted new password value where all non-padded bytes contain values limited to either 0x30–0x39 or 0x41–0x5A or 0x61–0x7A. Both passwords should be padded

	with 'FF'(as needed) to complete the total length of each value to 8 bytes. (repeat test five times with byte positions 2, 3, 4, 5, and 6 containing the 0x5B byte, respectively) Note: In Step 2 it may be necessary to send the VERIFY command with a correct Derived PIV Application Password in order to prevent the retry counter from decrementing to zero.
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns either status word: 1) '6A 80' (incorrect parameter in command data field) or 2) '63 CX' and the retry counter is decremented by 1 (where 'X' is the number of tries remaining).
Postcondition(s)	Current password is unchanged.

8.3.5.6 Change Reference Data with a Correctly Formatted but Incorrect Current Password or with a Correctly Formatted but Incorrect PUK

Test Assertion	TA-08.03.05.06
Purpose	Verifies that the Derived PIV Application responds appropriately when the CHANGE REFERENCE DATA command is sent repeatedly with a correctly formatted, but incorrect, Derived PIV Application Password or with a correctly formatted, but incorrect, PUK value.
DTR(s)	• DTR-06.02.02.09 • DTR-06.03.01.01 • DTR-06.03.06.04 • DTR-06.03.06.05 • DTR-06.03.06.07 • DTR-06.03.06.09
Vendor Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • The Derived PIV Application Password and the PUK are recorded. • The reset retry values for the Derived PIV Application Password and PUK are recorded. • The Derived PIV Application Password's retry counter and the PUK's retry counter are not 0.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the CHANGE REFERENCE DATA command repeatedly until after the issuer specified maximum number of password

	tries is exceeded with • P2, key reference value, is set to '80' • Data field of the command will contain an incorrect, but correctly formatted, password value, concatenated without delimitation with a valid new password value. Both passwords should be padded with 'FF' (if necessary) to complete the total length of each value to 8 bytes 3. Send the CHANGE REFERENCE DATA command with • P2, key reference value, is set to '80' • Data field of the command will contain the correct password value, concatenated without delimitation with a valid new password value. Both passwords should be padded with 'FF' (if necessary) to complete the total length of each value to 8 bytes Perform Steps 4 and 5 only if the Derived PIV Application supports changing the PUK with the CHANGE REFERENCE DATA command. 4. Send the CHANGE REFERENCE DATA command repeatedly until after the issuer specified maximum number of PUK tries is exceeded with • P2, key reference value, is set to '81' • Data field of the command will contain an incorrect, but correctly formatted, PUK value, concatenated without delimitation with a valid new PUK value 5. Send the CHANGE REFERENCE DATA command with • P2, key reference value, is set to '81' • Data field of the command will contain the correct PUK value, concatenated without delimitation with a valid new PUK value
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, each time the command returns status word '63 CX' (where 'X' indicates the number of further allowed retries) and the retry counter is decremented. The command returns status word '69 83' (reference data change operation blocked) when the maximum number of tries is exceeded. 3. From Step 3, the command returns status word '69 83' (reference data change operation blocked). 4. From Step 4, each time the command returns status word '63 CX' (where 'X' indicates the number of further allowed retries) and the retry counter is decremented. The command returns status word '69 83' (reference data change operation blocked) when the maximum number of tries is exceeded. 5. From Step 5, the command returns status word '69 83' (reference data change operation blocked).
Postcondition(s)	The Derived PIV Application Password's retry counter and the PUK's retry counter are 0.

673

8.3.6 RESET RETRY COUNTER Command

8.3.6.1 Reset Retry Counter for the Derived PIV Application Password

Test Assertion	TA-08.03.06.01
Purpose	Verifies that the Derived PIV Application changes the password with the RESET RETRY COUNTER command when the PUK and command format are correct.
DTR(s)	• DTR-06.02.02.09 • DTR-06.03.01.01 • DTR-06.03.07.01 • DTR-06.03.07.08
Vendor Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • The PUK is recorded. • The reset retry value for the Derived PIV Application Password is recorded. • The Derived PIV Application Password's retry counter and the PUK's retry counter are not 0.

Test Scenario	1. Send the SELECT command with
	  • AID == 'A0 00 00 03 08 00 00 20 00 01 00'
	2. Send the VERIFY command with
	  • P2, key reference value, is set to '80'
	  • Data field of the command contains an arbitrary, but correctly formatted password other than what is obtained from the vendor, padded with 'FF' (as necessary) to complete the total length of the value to 8 bytes
	3. Send the RESET RETRY COUNTER command with
	  • P2, key reference value, is set to '80'
	  • Data field of the command contains the PUK value for key reference '80' concatenated without delimitation with a new password padded with 'FF' (if necessary) to complete the total length of the value to 8 bytes.
	4. Obtain number of remaining retries of the '80' key reference by sending the VERIFY command with
	  • P2, key reference value, is set to '80'
	  • P1 parameter is '00' and both L_c and the data field are absent
	5. Send the VERIFY command with
	  • P2, key reference value, is set to '80'
	  • Data field of the command contains the new password value, padded with 'FF' (if necessary)

	to complete the total length of the value to 8 bytes
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns status word '63 CX' (where 'X' is the number of retries remaining). The retry counter is decremented by 1. 3. From Step 3, the command returns status word '90 00'. 4. From Step 4, the command returns status word '63 CX' (where 'X' is the number of retries remaining). Verify that 'X' from this step is greater than 'X' from Step 2 and is equal to the reset retry value. 5. From Step 5, the command returns status word '90 00'.
Postcondition(s)	The Derived PIV Application Password has been changed.

676

677 **8.3.6.2 Reset Retry Counter with an Invalid Key Reference**

Test Assertion	TA-08.03.06.02
Purpose	Verifies that the Derived PIV Application responds appropriately to the RESET RETRY COUNTER command for an invalid key reference.
DTR(s)	• DTR-06.02.02.09 • DTR-06.03.01.01 • DTR-06.03.07.01
Vendor Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • The PUK is recorded.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the RESET RETRY COUNTER command with • P2, key reference value, is set to a value other than '80' • Data field of the command contains the PUK value for key reference '80', concatenated without delimitation with a valid new password padded with 'FF' (if necessary) to complete the total length of the value to 8 bytes
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns an error status word and the PUK's retry counter remains unchanged.
Postcondition(s)	Current password is unchanged.

678

8.3.6.3 Reset Retry Counter with an Incorrect Length and Padding for the New Password

Test Assertion	TA-08.03.06.03
Purpose	Verifies that the Derived PIV Application does not set a new password with the RESET RETRY COUNTER command when the password length and padding requirements are not met.
DTR(s)	• DTR-06.02.02.09 • DTR-06.03.01.01 • DTR-06.03.07.04
Vendor Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • The Derived PIV Application Password and the PUK are recorded. • The Derived PIV Application Password's retry counter and the PUK's retry counter are not 0.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the RESET RETRY COUNTER command with • P2, key reference value, is set to '80' • Data field of the command contains the PUK value for key reference '80' concatenated with a new password value that is less than 8 bytes in length and is not padded with 'FF' 3. Send the RESET RETRY COUNTER command with • P2, key reference value, is set to '80' • Data field of the command contains the PUK value for key reference '80' concatenated with a new password value that is padded with 'FF' to complete 10 bytes 4. Send the RESET RETRY COUNTER command with • P2, key reference value, is set to '80' • Data field of the command contains the PUK value for key reference '80' concatenated with a new password value that is 6 bytes but padded to 8 bytes with 'FF' in byte 7 and 'AA' in byte 8 5. Send the RESET RETRY COUNTER command with • P2, key reference value, is set to '80' • Data field of the command contains the PUK value for key reference '80' concatenated with a new password value that is less than 6 bytes padded with 'FF' to complete 8 bytes 6. Send the VERIFY command with • P2, key reference value, is set to '80' • Data field of the command will contain the correct Derived PIV Application Password, padded with 'FF' (if necessary) to complete the total

	length of the value to 8 bytes
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns status word '6A 80' (incorrect parameter in command data field). 3. From Step 3, the command returns status word '6A 80' (incorrect parameter in command data field). 4. From Step 4, the command returns status word '6A 80' (incorrect parameter in command data field). 5. From Step 5, the command returns status word '6A 80' (incorrect parameter in command data field). 6. From Step 6, the command returns status word '90 00'.
Postcondition(s)	Current password is unchanged.

680

681 **8.3.6.4 Reset Retry Counter with an Incorrect Format for the New Password**

Test Assertion	TA-08.03.06.04
Purpose	Verifies that the Derived PIV Application does not set a new password with the RESET RETRY COUNTER command when the format requirements of the new password are not met.
DTR(s)	• DTR-06.02.02.09 • DTR-06.03.01.01 • DTR-06.03.07.04 • DTR-06.03.07.05 • DTR-06.03.07.06 • DTR-06.03.07.07
Vendor Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • The Derived PIV Application Password and the PUK are recorded. • The Derived PIV Application Password's retry counter and the PUK's retry counter are not 0.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the RESET RETRY COUNTER with • P2, key reference value, is set to '80' • Data field of the command contains the correct PUK value for key reference '80' concatenated without delimitation with an arbitrary new password value that contains 0x5B in the first byte position, all other non-padded bytes contain values limited to either 0x30–0x39 or 0x41–0x5A

	or 0x61-0x7A. The new password should be padded with 'FF' (if necessary) to complete the total length of the value to 8 bytes 3. Repeat Step 2 five times with byte positions 2, 3, 4, 5, and 6 of the password containing the 0x5B byte, respectively. 4. Send the VERIFY command with • P2, key reference value, is set to '80' • Data field of the command will contain the correct Derived PIV Application Password, padded with 'FF' (if necessary) to complete the total length of the value to 8 bytes
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns status word '6A 80' (incorrect parameter in command data field). 3. From Step 3, each time the command returns status word '6A 80' (incorrect parameter in command data field). 4. From Step 4, the command returns status word '90 00'.
Postcondition(s)	Current password is unchanged.

682

683 **8.3.6.5 Reset Retry Counter with an incorrect length for the PUK**

Test Assertion	TA-08.03.06.05
Purpose	Verifies that the Derived PIV Application does not set a new password with the RESET RETRY COUNTER command when the PUK length is incorrect.
DTR(s)	• DTR-06.02.02.09 • DTR-06.03.01.01 • DTR-06.03.07.04 • DTR-06.03.07.05 • DTR-06.03.07.06 • DTR-06.03.07.07
Vendor Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • The Derived PIV Application Password and the PUK are recorded. • The Derived PIV Application Password's retry counter is not 0 and the PUK's retry counter is greater than 1.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the RESET RETRY COUNTER with

	• P2, key reference value, is set to '80' • Data field of the command contains an arbitrary PUK value that is less than 8 bytes in length concatenated without delimitation with an arbitrary new valid password value. The new password should be padded with 'FF' (if necessary) to complete the total length of the value to 8 bytes 3. Send the RESET RETRY COUNTER with • P2, key reference value, is set to '80' • Data field of the command contains an arbitrary PUK value that is greater than 8 bytes in length concatenated without delimitation with an arbitrary new valid password value. The new password should be padded with 'FF' (if necessary) to complete the total length of the value to 8 bytes 4. Send the VERIFY command with • P2, key reference value, is set to '80' • Data field of the command will contain the correct Derived PIV Application Password, padded with 'FF' (if necessary) to complete the total length of the value to 8 bytes
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns either status word: 1) '6A 80' (incorrect parameter in command data field) or 2) '63 CX' and the PUK's retry counter is decremented by 1 (where 'X' is the number of tries remaining). 3. From Step 3, the command returns either status word: 1) '6A 80' (incorrect parameter in command data field) or 2) '63 CX' and the PUK's retry counter is decremented by 1 (where 'X' is the number of tries remaining). 4. From Step 4, the command returns status word '90 00'.
Postcondition(s)	Current password is unchanged.

684

685 **8.3.6.6 Reset Retry Counter using an Incorrect PUK**

Test Assertion	TA-08.03.06.06
Purpose	Verifies that the Derived PIV Application does not change the value of the Derived PIV Application Password when an incorrect PUK is provided.
DTR(s)	• DTR-06.02.02.09 • DTR-06.03.01.01 • DTR-06.03.07.02 • DTR-06.03.07.03 • DTR-06.03.07.05 • DTR-06.03.07.06

	• DTR-06.03.07.07
Vendor Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • The Derived PIV Application Password and the PUK are recorded. • The Derived PIV Application Password's retry counter is not 0 and the PUK's retry counter greater than 1.

Test Scenario	1. Send the SELECT command with
	  • AID == 'A0 00 00 03 08 00 00 20 00 01 00'
	2. Send the VERIFY command with
	  • P2, key reference value, is set to '80'
	  • Data field of the command contains an arbitrary, but correctly formatted, Derived PIV Application Password, padded with 'FF' (as necessary) to complete the total length of the value to 8 bytes
	3. Send the RESET RETRY COUNTER with
	  • P2, key reference value, is set to '80'
	  • Data field of the command contains an incorrect PUK value concatenated without delimitation with a new valid password value padded with 'FF' to complete the total length of the value to 8 bytes.
	4. Obtain number of remaining retries of the '80' key reference by sending the VERIFY command with
	  • P2, key reference value, is set to '80'
	  • P1 parameter is '00' and both L_c and the data field are absent
	5. Send the RESET RETRY COUNTER with
	  • P2, key reference value, is set to '80'
	  • Data field of the command containing an incorrect PUK value concatenated without delimitation with a new password padded with 'FF' (if necessary) to complete the total length of the value to 8 bytes. This operation is repeated until the number of resets allowed is exceeded
	6. Send the RESET RETRY COUNTER with
	  • P2, key reference value, is set to '80'
	  • Data field of the command contains the correct PUK value concatenated without delimitation with a new correctly-formatted password value padded to 8 bytes with 'FF' (if necessary)

Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns status word '63 CX' (X == number of retries left for the Derived PIV Application Password) 3. From Step 3, the command returns status word '63 CX' (where 'X' indicates the number of further allowed retries for the PUK)

	4. From Step 4, the command returns status word '63 CX' (where 'X' is the number of retries remaining for the Derived PIV Application Password. Verify that 'X' from this step is the same as 'X' from Step 2. 5. From Step 5, the command returns status word '63 CX' (where 'X' indicates the number of further allowed retries for the PUK) and the PUK's retry counter is decremented each time. The command returns status word '69 83' (reset operation blocked) when the command is invoked after the value of 'X' becomes 0. 6. From Step 6, the command returns status word '69 83' (reset operation blocked).
Postcondition(s)	The Reset Retry Counter command is blocked.

686

687 ### 8.3.7 PUT DATA Command

688 #### 8.3.7.1 Put Data for various Data Objects of the Derived PV Application

Test Assertion	TA-08.03.07.01
Purpose	Verifies that the Derived PIV Application responds appropriately to the PUT DATA command.
DTR(s)	• DTR-06.02.02.02 • DTR-06.02.02.03 • DTR-06.02.02.04 • DTR-06.02.02.05 • DTR-06.02.02.06 • DTR-06.02.02.07 • DTR-06.02.02.08 • DTR-06.02.02.09 • DTR-06.03.01.01 • DTR-06.03.08.01
Vendor Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • The Derived PIV Application Token Management Key is recorded. • The mutual authentication of the Derived PIV Application and the Test Toolkit Application has not been performed. • Data objects to be loaded are equal to the minimum container sizes specified for that object.[13]

[13] Data objects for the containers do not have to be properly formatted for this test.

Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the PUT DATA command with • CLA is set to: 1. '00' if command chaining is not needed or 2. '10' if command chaining is used. (The last chain of the command sets CLA to '00') • Data field in the command is to include the tag of the X.509 Certificate for PIV Authentication data object ('5FC105') • Data field in the command is to include data object that will be placed in the X.509 Certificate for PIV Authentication container 3. If the X.509 Certificate for Digital Signature is supported, repeat Step 2 with • Data field in the command is to include the tag of the X.509 Certificate for Digital Signature data object ('5FC10A') • Data field in the command is to include the data content that will be placed in the X.509 Certificate for Digital Signature container 4. If the X.509 Certificate for Key Management is supported, repeat Step 2 with • Data field in the command is to include the tag of the X.509 Certificate for Key Management data object ('5FC10B') • Data field in the command is to include the data object that will placed in the X.509 Certificate for Key Management container 5. If the token supports the Discovery Object, repeat Step 2 with • Data field in the command is to include the tag of the Discovery Object ('7E') • Data field in the command is to include the data object that will placed in the Discovery Object container 6. If the Security Object is supported, repeat Step 2 with • Data field in the command is to include the tag of the Security Object ('5FC106') • Data field in the command is to include the data object that will be placed the Security Object container 7. If the Key History Object is supported, repeat Step 2 with • Data field in the command is to include the tag of the Key History object ('5FC10C') • Data field in the command is to include the data object that will placed in the Key History Object container 8. If the Key History Object is supported, repeat Step 2 for each implemented retired X.509 Certificate for Key Management with • Data field in the command is to include the tag of one of the 20 retired X.509 Certificates for

	Key Management ('5FC10D'-'5FC120') • Data field in the command is to include the data object that will be placed the retired X.509 Certificate for Key Management container NOTE: The following tests are to be performed only if the Derived PIV Application supports the use of the '9B' key (Derived PIV Token Management Key) 9. Perform mutual authentication of Derived PIV Application and the Test Toolkit Application using Test Assertion TA-08.03.03.03 (GENERAL AUTHENTICATE). 10. Repeat Steps 2-8. Following the PUT DATA commands, perform the GET DATA commands (see TA-08.03.03.02.01) to verify that the same data that was personalized with the PUT DATA commands are returned by the GET DATA commands.
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2 through Step 8, the commands return status word '69 82' (security status not satisfied). 3. From Step 9, the test results are consistent with those expected as part of TA-08.03.03.03: a. From Step 1 of TA-08.03.03.03, the command returns the application property template with the status word '90 00'. b. From Step 2 of TA-08.03.03.03, the command returns with the witness followed by status word '90 00'. c. From Step 3 of TA-08.03.03.03, the Derived PIV Application verifies the decrypted witness and then responds with encryption of the challenge sent by Test Toolkit Application followed by status word '90 00'. Decrypt the encrypted challenge and compare it to the one sent to the token. 4. From Step 10, all commands return status word '90 00', and input and output data match.
Postcondition(s)	N/A

8.3.8 GENERATE ASYMMETRIC KEY PAIR Command

8.3.8.1 Generate Asymmetric Key Pair for the Various Keys

Test Assertion	TA-08.03.08.01
Purpose	Verifies that the Derived PIV Application responds appropriately to the GENERATE ASYMMETRIC KEY PAIR command.
DTR(s)	• DTR-06.02.02.09 • DTR-06.03.01.01 • DTR-06.03.04.05 • DTR-06.03.09.01

	• DTR-06.03.09.02
Vendor Documentation	The vendor to provide documentation specifying the cryptographic mechanism identifiers (from Table 5 of [SP800-73], Part 1) that have been implemented.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • The Derived PIV Application Token Management Key is recorded. • The mutual authentication of the Derived PIV Application and the Test Toolkit Application has not been performed. • The Derived PIV Application Password is recorded. • The Derived PIV Application Password's retry counter is not 0.

Test Scenario	1. Send the SELECT command with
	  • AID == 'A0 00 00 03 08 00 00 20 00 01 00'
	2. Send the GENERATE ASYMMETRIC KEY PAIR command with
	  • P2 is set to value '9A'
	  • Data field in the command is to include either '07' or '11' as the cryptographic mechanism identifier
	3. If the X.509 Certificate for Digital Signature is supported, send the GENERATE ASYMMETRIC KEY PAIR command with
	  • P2 is set to value '9C'
	  • Data field in the command is to include either '07', '11', '14' as the cryptographic mechanism identifier
	4. If the X.509 Certificate for Key Management and the on-token generation of the key management key is supported, send the GENERATE ASYMMETRIC KEY PAIR command with
	  • P2 is set to value '9D'
	  • Data field in the command is to include either '07', '11', '14' as the cryptographic mechanism identifier
	
	NOTE: The following tests are to be performed only if the Derived PIV Application supports the use of the '9B' key (Derived PIV Token Management Key)
	
	5. Perform mutual authentication of Derived PIV Application and the Test Toolkit Application using Test Assertion TA-08.03.03.03 (GENERAL AUTHENTICATE)
	6. Repeat Steps 2, 3, and 4.
	7. Repeat Step 2 with the cryptographic mechanism identifier value in the data field set to a value that is not supported by the Derived PIV Application.
	8. Repeat Step 2 with P2 set to a key reference value that is not supported by the Derived PIV Application.
	9. Send the VERIFY command with
	  • P2, key reference value, is set to '80'

	• Data field of the command will contain the correct Derived PIV Application Password, padded with 'FF' (if necessary) to complete the total length of the value to 8 bytes 10. Send the GENERAL AUTHENTICATE command • CLA is set to: 1. '00' if command chaining is not needed or 2. '10' if command chaining is used. (The last chain of the command sets CLA to '00') • P1, algorithm reference, is set to '07' or '11' • P2, key reference, is set to '9A' • Data field in the command is to include '81' specifying a challenge, followed by a randomly generated challenge, and '82 00' in order to request a response 11. If the X.509 Certificate for Digital Signature is supported, send the GENERAL AUTHENTICATE command • CLA is set to: 1. '00' if command chaining is not needed or 2. '10' if command chaining is used. (The last chain of the command sets CLA to '00') • P1, algorithm reference, is set to '07', '11' or '14' • P2, key reference, is set to '9C' • Data field in the command is to include '81' specifying a challenge, followed by a randomly generated challenge, and '82 00' in order to request a response 12. If the X.509 Certificate for Key Management and the on-token generation of the key management key is supported, send the GENERAL AUTHENTICATE command • CLA is set to: 1. '00' if command chaining is not needed or 2. '10' if command chaining is used. (The last chain of the command sets CLA to '00') • P1, algorithm reference, is set to '07', '11' or '14' • P2, key reference, is set to '9D' indicating the key management key • Data field in the command is to include one of the following: 1. If P1 = '07', the template '81' contains a key encrypted using the key management public key returned in Step 6. 2. If P1 = '11' or '14', the template '85' contain the other party's public key.[14]
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, 3, and 4, the command returns status word '69 82' (security status not satisfied).

[14] Template '85' contains the other party's public key, a point on Curve P-256 or P-384, encoded as '04' || X || Y, without the use of point compression, as described in Section 2.3.3 of [SEC1].

	3. From Step 5, the test results are consistent with those expected as part of TA-08.03.03.03: a. From Step 1 of TA-08.03.03.03, the command returns the application property template with the status word '90 00'. b. From Step 2 of TA-08.03.03.03, the command returns with the witness followed by status word '90 00'. c. From Step 3 of TA-08.03.03.03, the Derived PIV Application verifies the decrypted witness and then responds with encryption of the challenge sent by Test Toolkit Application followed by status word '90 00'. Decrypt the encrypted challenge and compare it to the one sent to the token. 4. From Step 6, the commands return status word '90 00' and the data field contains the '7F49' template with the generated public key, which consists of either a modulus and public exponent (RSA) or a point (elliptic curve cryptography). 5. From Step 7, the command returns status word '6A 80' (incorrect parameter command data field). 6. From Step 8, the command returns status word '6A 86' (incorrect parameter P2). 7. From Step 9, the command returns status word '90 00'. 8. From Step 10, the command returns the signed challenge with status word '90 00'. Verify the signed challenge using the Derived PIV Authentication public key that was returned in Step 6. 9. From Step 11, the command returns the signed challenge with status word '90 00'. Verify the signed challenge using the digital signature public key that was returned in Step 6. 10. From Step 12, for algorithm reference '07' as P1 value, the command returns the transported key with status word '90 00'. Compare the test toolkit application's copy of the plaintext key to the one received in the response from the token. For algorithm reference '11' or '14' as P1 value, the command returns the shared secret Z [15] with status word '90 00'. Compare the shared secret computed by the token with the shared secret computed off token (using the key management public key that was returned in Step 6).
Postcondition(s)	The token has newly generated private key(s).

[15] Z is the X coordinate of point P as defined in [SP800-56A], Section 5.7.1.2

9. Test Assertions for the Derived PIV Application Data Model

This section lists the test assertions used to determine conformity to the derived test requirements (DTR) listed in Section 7. The Implementation Under Test (IUT), the Derived PIV Data Objects loaded on a Derived PIV Application by an issuer, must meet the stated objective(s) of the assertion by way of a test or submission of artifacts in order to be deemed conformant to the associated DTR(s).

9.1 BER-TLV Conformance

The following assumptions apply to the test assertions within this section.

1	When the length of the value field is between 0 and 127 bytes, the length field should consist of a single byte where bit 8 is set to 0 and bits 7 to 1 encode the number of bytes in the value field. When the length of the value field is greater than 127 bytes, the length field consists of two or more bytes.[16] The first byte is '81', '82', '83' or '84' where the low order nibble of each of these possible first-byte values (1, 2, 3, or 4 respectively) encodes the number of subsequent bytes in the length field. These subsequent bytes are taken together in order to be a big-endian integer encoding the number of bytes in the value field. Table 1 shows the encoding of the length field.
2	Except for the Discovery Object tag, each BER-TLV tag is encoded as three bytes.
3	Each data object returned is appended with a 2 byte status word.
4	All variable length value fields can have zero lengths, which will result in a tag length field being immediately followed by the next tag, if applicable.
5	The final byte of the command string can be set to 0x00 to retrieve an entire data object regardless of the size of that object.

Number of bytes in the length field	First byte	Subsequent bytes	Length of the value field
1 byte	'00' to '7F'	None	0 to 127
2 byte	'81'	'00' to 'FF'	0 to 255
3 byte	'82'	'0000' to 'FFFF'	0 to 65 535
4 byte	'83'	'000000' to 'FFFFFF'	0 to 16 777 215
5 byte	'84'	'00000000' to 'FFFFFFFF'	0 to 4 294 967 295

Table 1 - Encoding of Length Field

[16] Use of the shortest encoding format is preferred.

9.1.1 X.509 Certificate for Derived PIV Authentication

9.1.1.1 BER-TLV of X.509 Certificate for Derived PIV Authentication

Test Assertion	TA-09.01.01.01
Purpose	Verifies that the X.509 Certificate for Derived PIV Authentication conforms to the Derived PIV data model requirements.
DTR(s)	• DTR-07.01.02.01
Issuer Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the GET DATA command with • Data field of the command containing the tag ('5FC105') of the X.509 Certificate for Derived PIV Authentication data object 3. Read and parse the byte array in accordance with BER-TLV format.
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns status word '90 00' along with the X.509 Certificate for Derived PIV Authentication data object. 3. From Step 3, all mandatory tags for the X.509 Certificate for Derived PIV Authentication data object are present in the order indicated in Table 10 of [SP800-73], Part 1.

9.1.2 X.509 Certificate for Digital Signature

9.1.2.1 BER-TLV of X.509 Certificate for Digital Signature

Test Assertion	TA-09.01.02.01
Purpose	Verifies that the X.509 Certificate for Digital Signature (if present) conforms to the Derived PIV data model requirements.
DTR(s)	• DTR-07.01.01.01 • DTR-07.01.03.01
Issuer Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader.

Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the GET DATA command with • Data field of the command containing the tag ('5FC10A') of the X.509 Certificate for Digital Signature data object 3. If the X.509 Certificate for Digital Signature data object was retrieved in Step 2, read and parse the byte array in accordance with BER-TLV format.
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns one of the following: • An X.509 Certificate for Digital Signature data object followed by status word '90 00'; • A zero-length data object followed by status word '90 00' – which indicates that a container for the X.509 certificate exists, but it has not been personalized; or • Status word '6A 82' (data object not found) – which indicates the container for the X.509 certificate does not exist 3. From Step 3, all mandatory tags for the X.509 Certificate for Digital Signature data object are present in the order indicated in Table 15 of [SP800-73], Part 1.

9.1.3 X.509 Certificate for Key Management

9.1.3.1 BER-TLV of X.509 Certificate for Key Management

Test Assertion	TA-09.01.03.01
Purpose	Verifies that the X.509 Certificate for Key Management (if present) conforms to the Derived PIV data model requirements.
DTR(s)	• DTR-07.01.01.01 • DTR-07.01.04.01
Issuer Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the GET DATA command with • Data field of the command containing the tag ('5FC10B') of the X.509 Certificate for Key Management data object 3. If the X.509 Certificate for Key Management data object was retrieved in Step 2, read and parse the byte array in accordance with BER-TLV format.

Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns one of the following: • An X.509 Certificate for Key Management followed by status word '90 00'; • A zero-length data object followed by status word '90 00' – which indicates that a container for the X.509 certificate exists, but it has not been personalized; or • Status word '6A 82' (data object not found) – which indicates the container for the X.509 certificate does not exist 3. From Step 3, all mandatory tags for the X.509 Certificate for Key Management are present in the order indicated in Table 16 of [SP800-73], Part 1.

712

713 ### 9.1.4 Discovery Object

714 #### 9.1.4.1 BER-TLV of Discovery Object and Presence of Security Object

Test Assertion	TA-09.01.04.01
Purpose	Verifies that the Discovery Object (if present) conforms to the Derived PIV data model requirements.
DTR(s)	• DTR-07.01.01.01 • DTR-07.01.05.01 • DTR-07.01.05.02 • DTR-07.01.08.02
Issuer Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader.
Test Scenario	1. Send the SELECT token command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the GET DATA command with • Data field of the command containing the tag ('7E') of the Discovery Object. 3. If the Discovery Object was retrieved in Step 2, read and parse the byte array in accordance with BER-TLV format. 4. If the Discovery Object was retrieved in Step 2, verify that the Security Object is present within the Derived PIV Application by sending a GET DATA command to read the data object.
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns one of the following:

	• A Discovery Object followed by status word '90 00'; • A zero-length data object followed by status word '90 00' – which indicates that a container for the Discovery Object exists, but it has not been personalized; or • Status word '6A 82' (data object not found) – which indicates the container for the Discovery Object does not exist) 3. From Step 3, all mandatory tags for the Discovery Object are present and are in the order indicated in Table 18 of [SP800-73], Part 1. The first byte of the PIN Usage Policy is set to 0x40 and the second byte is set to 0x00. In addition, the PIV Card Application AID in tag 0x4F is set to 'A0 00 00 03 08 00 00 20 00 01 00' 4. From Step 4, the command returns status word '90 00' along with the Security Object.

715

716 ### 9.1.5 Key History Object

717 #### 9.1.5.1 BER-TLV of Key History Object and Presence of Security Object

Test Assertion	TA-09.01.05.01
Purpose	Verifies that the Key History Object (if present) conforms to the Derived PIV data model requirements.
DTR(s)	• DTR-07.01.01.01 • DTR-07.01.06.01 • DTR-07.01.08.02
Issuer Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the GET DATA command with • Data field of the command containing the tag ('5FC10C') of the Key History Object. 3. If the Key History Object was retrieved in Step 2, read and parse the byte array in accordance with BER-TLV format. 4. If the Key History Object was retrieved in Step 2, verify that the Security Object is present within the Derived PIV Application by sending a GET DATA command to read this data object.
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns one of the following:

	• A Key History Object followed by status word '90 00'; • A zero-length data object followed by status word '90 00' - which indicates that a container for the Key History Object exists, but it has not been personalized; or • Status word '6A 82' (data object not found) - which indicates the container for the Key History Object does not exist 3. From Step 3, all mandatory tags for the Key History Object are present in the order indicated in Table 19 of [SP800-73], Part 1. 4. From Step 4, the command returns status word '90 00' along with the Security Object.

718

719 ### 9.1.6 Retired X.509 Certificates for Key Management

720 #### 9.1.6.1 BER-TLV of Retired X.509 Certificates for Key Management

Test Assertion	TA-09.01.06.01
Purpose	Verifies that the Retired X.509 Certificates for Key Management (if present) conform to the Derived PIV data model requirements.
DTR(s)	• DTR-07.01.01.01 • DTR-07.01.07.01
Issuer Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send 20 GET DATA commands with • Data field of each command containing the tag ('5FC10D' to '5FC120') for one of the 20 Retired X.509 Certificates for Key Management 3. For each Retired X.509 Certificate for Key Management retrieved in Step 2, read and parse the byte array for each in accordance with BER-TLV format.
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, each command returns one of the following: • A Retired X.509 Certificate for Key Management followed by status word '90 00'; • A zero-length data object followed by status word '90 00' – which indicates that a container for the retired X.509 certificate exists, but it has not been personalized; or • Status word '6A 82' (data object not found) – which

	indicates the container for the retired X.509 certificate does not exist) 3. From Step 3, all mandatory tags in each of the available Retired X.509 Certificates for Key Management are present in the order indicated in Table 20 to Table 39 of [SP800-73], Part 1.

721

722 ### 9.1.7 Security Object

723 #### 9.1.7.1 BER-TLV of Security Object and Presence of Unsigned Data Objects

Test Assertion	TA-09.01.07.01
Purpose	Verifies that the Security Object conforms to the Derived PIV data model requirements and unsigned data objects are included within the Security Object on the Derived PIV Application.
DTR(s)	• DTR-07.01.01.01 • DTR-07.01.08.01 • DTR-07.01.08.03
Issuer Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • A Security Object is present within the Derived PIV Application.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the GET DATA command with • Data field of the command containing the tag ('5FC106') for the Security Object 3. Read and parse the byte array in accordance with BER-TLV format. 4. Parse the tag 0xBA to extract the Data Groups to Container ID mapping instances. 5. Verify that all unsigned data objects (the Discovery and/or Key History object) are included in the Security Object. 6. Verify that the unsigned data objects exist within the Derived PIV Application by reading the data object from each container.
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns the Security Object followed by status word '90 00'. 3. From Step 3, all mandatory tags for the Security Object are present in the order indicated in Table 12 of [SP800-73], Part 1. 4. From Step 5, all unsigned data objects are included in the

	Security Object. 5. From Step 6, all data objects found in the mapping are actually present on the Derived PIV Application as evidenced by the GET DATA commands returning the data objects along with status word '90 00'.

724

725 ## 9.2 Signed Data Object Conformance

726 ### 9.2.1 Security Object

727 #### 9.2.1.1 Data Object Hash Integrity Check

Test Assertion	TA-09.02.01.01
Purpose	Verifies the integrity of the hashes of the data objects referenced in the Security Object (if present).
DTR(s)	• DTR-07.02.01.01 • DTR-07.01.05.02 • DTR-07.01.08.02
Issuer Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • A Security Object is present within the Derived PIV Application.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the GET DATA command with • Data field of the command containing the tag ('5FC106') of the Security Object 3. Identify the various data elements that are part of the security object by parsing the Mapping of Data Group (DG) to ContainerID (i.e. TAG 0xBA). 4. Extract the ldsSecurityObject from the eContent field of the Security Object Asymmetric Signature (i.e. TAG 0xBB). 5. Get all the data objects that are present in the mapping obtained from Step 3 (i.e., the Discovery Object and/or the Key History Object). 6. Compute the hash for each data object and verify that it matches the hash value present in the ldsSecurityObject.
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns the Security Object and the status word '90 00'. 3. From Step 5, the command returns the Discovery Object and/or

	Key History Object. 4. From Step 6, the actual hashes of the data objects extracted in Step 5 are identical to their corresponding hash values present in the Security Object.

728

729 **9.2.1.2 Presence of CMS SignedData**

Test Assertion	TA-09.02.01.02
Purpose	Verifies that the Security Object contains an asymmetric digital signature, implemented as a SignedData type in accordance with [RFC5652].
DTR(s)	• DTR-07.02.01.02 • DTR-07.02.01.03
Issuer Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • A Security Object is present within the Derived PIV Application.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the GET DATA command with • Data field of the command containing the tag ('5FC106') of the Security Object 3. Parse the obtained Security Object and extract the contents from the asymmetric digital signature field (i.e., tag 0xBB) 4. Process the contents of the digital signature
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns the requested data object along with the status word '90 00'. 3. From Step 4, the content of the digital signature is an object that is a SignedData type which is in accordance with [RFC5652].

730

731 **9.2.1.3 SignedData Version**

Test Assertion	TA-09.02.01.03
Purpose	Verifies that the version of the SignedData content type is v3.
DTR(s)	• DTR-07.02.01.04
Issuer Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and

	an instance of the reader. • A Security Object is present within the Derived PIV Application.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the GET DATA command with • Data field of the command containing the tag ('5FC106') of the Security Object 3. Extract the version field contents from the asymmetric signature of the Security Object (i.e., tag 0xBB)
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns the requested data object along with the status word '90 00'. 3. From Step 3, the value of the version field of the SignedData is v3.

732

733 **9.2.1.4 SignedData digestAlgorithms**

Test Assertion	TA-09.02.01.04
Purpose	Verifies that the digestAlgorithms field of the SignedData content type is in accordance with Table 3-2 of [SP800-78].
DTR(s)	• DTR-07.02.01.05
Issuer Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • A Security Object is present within the Derived PIV Application.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the GET DATA command with • Data field of the command containing the tag ('5FC106') of the Security Object 3. Extract the digestAlgorithms and certificates fields contents from the Security Object. 4. From the certificate obtained, extract the subjectPublicKeyInfo->subjectPublicKey and determine the type and size of the signer's public key. 5. Determine the digest algorithm specified in the digestAlgorithms field obtained in Step 3 using Table 3-6 of [SP800-78]. 6. Match the digest algorithm obtained from Step 5 to an entry of Table 3-2 of [SP800-78] based on the public key algorithm and size (Step 4).
Expected Result(s)	1. From Step 1, the command returns the application property

	template with the status word '90 00'. 2. From Step 2, the command returns the requested data object along with the status word '90 00'. 3. From Step 6, the digestAlgorithms field value of the SignedData is in accordance with Table 3-2 of [SP800-78].

734

735 **9.2.1.5 encapContentInfo Contents**

Test Assertion	TA-09.02.01.05
Purpose	Verifies that the eContentType of the encapContentInfo is id-icao-ldsSecurityObject and the eContent field of the encapContentInfo contains the contents of the ldsSecurity object.
DTR(s)	• DTR-07.02.01.06 • DTR-07.02.01.07
Issuer Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • A Security Object is present within the Derived PIV Application.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the GET DATA command with • Data field of the command containing the tag ('5FC106') of the Security Object 3. Extract and parse the encapContentInfo field contents from the Security Object.
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns the requested data object along with the status word '90 00'. 3. From Step 3, the eContent field contains a correctly formatted ldsSecurityobject and the eContentType asserts id-icao-ldsSecurityObject in encapContentInfo.

736

737 **9.2.1.6 Derived PIV Credential Issuer's (Content Signing) Certificate Inclusion**

Test Assertion	TA-09.02.01.06
Purpose	Verifies that the Security Object includes the certificate of the Derived PIV Credential Issuer (i.e., the issuer's content signing certificate).
DTR(s)	• DTR-07.02.01.08
Issuer Documentation	None.

Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • A Security Object is present within the Derived PIV Application.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the GET DATA command with • Data field of the command containing the tag ('5FC106') of the Security Object 3. Extract and parse the certificates field contents from the Security Object.
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns status word '90 00' along with the Security Object. 3. From Step 3, the certificates field contains an X.509 certificate which is the Derived PIV Credential Issuer's (content signing) certificate.

9.2.1.7 SignerInfo digestAlgorithm

Test Assertion	TA-09.02.01.07
Purpose	Verifies that the digestAlgorithm field of the SignerInfo field is in accordance with Table 3-2 of [SP800-78].
DTR(s)	• DTR-07.02.01.09
Issuer Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • A Security Object is present within the Derived PIV Application.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the GET DATA command with • Data field of the command containing the tag ('5FC106') of the Security Object 3. Extract the SignerInfo->digestAlgorithm field from the Security Object. 4. Extract the certificates field contents from the Security Object. 5. From the certificate obtained, extract the subjectPublicKeyInfo->subjectPublicKey. 6. Compute the type and size of the signer's public key. 7. Determine the digest algorithm specified in the

	digestAlgorithm field obtained in Step 3 using Table 3-6 of [SP800-78]. 8. Match the digest algorithm obtained from Step 7 to an entry of Table 3-2 of [SP800-78] based on the public key algorithm and size (Step 6).
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command the requested data object along with the returns status word '90 00'. 3. From Step 8, the digestAlgorithm field value of the SignerInfo is in accordance with Tables 3-6 and 3-2 of [SP800-78] and it matches the value present in the digestAlgorithms field of the SignedData.

740

741 **9.2.1.8 SignerInfo signatureAlgorithm**

Test Assertion	TA-09.02.01.08
Purpose	Verifies that for RSA with PKCS #1 v1.5 padding, the signatureAlgorithm field specifies the rsaEncryption OID (as per Section 3.2 of [RFC3370]) and for ECDSA and RSA with PSS padding, the signatureAlgorithm is in accordance with Table 3-3 of [SP800-78].
DTR(s)	• DTR-07.02.01.10
Issuer Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • A Security Object is present within the Derived PIV Application.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the GET DATA command with • Data field of the command containing the tag ('5FC106') of the Security Object 3. From the signature block (tag 0xBB) match the SignerInfo->signatureAlgorithm field contents to an entry in Table 3-3 of [SP800-78].
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns the requested data object along with the status word '90 00'. 3. From Step 3, the signatureAlgorithm field specified in the SignerInfo field for RSA with PKCS #1 v1.5 padding specifies the rsaEncryption OID (as per Section 3.2 of [RFC3370]) and for ECDSA and RSA with PSS padding, the signatureAlgorithm is in accordance with Table 3-3 of [SP800-

	78].

742

743 #### 9.2.1.9 Digital Signature

Test Assertion	TA-09.02.01.09
Purpose	Verifies that the signature in the SignerInfo corresponds to the Security Object and that it is signed with the Derived PIV Credential Issuer's (content signing) certificate.
DTR(s)	• DTR-07.02.01.11
Issuer Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • A Security Object is present within the Derived PIV Application.

Test Scenario	1. Send the SELECT command with
	  • AID == 'A0 00 00 03 08 00 00 20 00 01 00'
	2. Send the GET DATA command with
	  • Data field of the command containing the tag ('5FC106') of the Security Object
	3. Extract the contents of the Security Object asymmetric signature (TAG 0xBB).
	4. Extract and parse the certificates field contents from the Security Object.
	5. Using the certificate extracted from the asymmetric signature block, verify the signature of the Security Object.

Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns the requested data object along with the status word '90 00'. 3. From Step 5, the certificates field of the SignedData contains the Derived PIV Credential Issuer's (content signing) certificate, which is used to verify the digital signature on the Security Object.

744

745 ## 9.3 PKI Conformance

746 ### 9.3.1 X.509 Certificate for Derived PIV Authentication[17]

747 #### 9.3.1.1 Signature Algorithm

Test Assertion	TA-09.03.01.01

[17] The Derived PIV Authentication key and certificate may be tested outside of the Derived PIV Application. Specific test assertions can be developed by test entities to test this key and certificate based on the environment (e.g., web browser) in which the key pair is being used. See Appendix A for examples of testing approaches.

Purpose	Verifies that the proper signature algorithm has been used to sign the Derived PIV Authentication certificate as specified in Table 3-3 of [SP800-78].
DTR(s)	• DTR-07.03.01.01 • DTR-07.03.01.02
Issuer Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • A Derived PIV Authentication certificate is present within the Derived PIV Application.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the GET DATA command with • Data field of the command containing the tag ('5FC105') of the X.509 Certificate for Derived PIV Authentication data object 3. Extract signature->algorithm field value from the certificate.
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns the requested data object along with the status word '90 00' 3. From Step 3, the algorithm value is in accordance with Table 3-3 of [SP800-78]. If the algorithm value is id-RSASSA-PSS, then the hashAlgorithm field in signature->parameters is populated with SHA-256 (OID = 2.16.840.1.101.3.4.2.1). For RSA with PKCS #1 v1.5 padding, the parameters field is populated with NULL. For ECDSA, the parameters field is absent.

9.3.1.2 Subject Public Key Algorithm

Test Assertion	TA-09.03.01.02
Purpose	Verifies that the public key algorithm used for generating the keys is as specified in Table 3-4 of [SP800-78].
DTR(s)	• DTR-07.03.01.03 • DTR-07.03.01.04
Issuer Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • A Derived PIV Authentication certificate is present within the

	Derived PIV Application.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the GET DATA command with • Data field of the command containing the tag ('5FC105') of the X.509 Certificate for Derived PIV Authentication data object 3. Extract subjectPublicKeyInfo->algorithm->algorithm field value 4. Match the algorithm value to the Table 3-4 of [SP800-78]. 5. If the algorithm is elliptic curve, ensure that the OID for Curve P-256 from Table 3-5 of [SP800-78] is populated in the subjectPublicKeyInfo->algorithm->parameters->namedCurve field. Note: If the RSA algorithm is used, the subjectPublicKeyInfo->algorithm->parameters field will be NULL.
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns the requested data object along with the status word '90 00'. 3. From Steps 4 and 5, it is determined that the Derived PIV Authentication key is generated using an allowed asymmetric key algorithm.

9.3.1.3 Public Key Size

Test Assertion	TA-09.03.01.03
Purpose	Verifies that the key size requirements are in accordance with Table 3-1 of [SP800-78].
DTR(s)	• DTR-07.03.01.12
Issuer Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • A Derived PIV Authentication certificate is present within the Derived PIV Application.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send GET DATA command with • Data field of the command containing the tag ('5FC105') of the X.509 Certificate for Derived PIV Authentication data object 3. Extract subjectPublicKeyInfo->algorithm->algorithm field value. 4. Extract the subjectPublicKeyInfo->subjectPublicKey

	from the certificate 5. Match the key size to Table 3-1 of [SP800-78].
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns the requested data object along with the status word '90 00'. 3. From Step 5, the key size is in accordance with Table 3-1 of [SP800-78].

752

753 **9.3.1.4 Key Usage Extension**

Test Assertion	TA-09.03.01.04
Purpose	Verifies that the Derived PIV Authentication certificate asserts the appropriate purpose for the key.
DTR(s)	• DTR-07.03.01.05
Issuer Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • A Derived PIV Authentication certificate is present within the Derived PIV Application.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the GET DATA command with • Data field of the command containing the tag ('5FC105') of the X.509 Certificate for Derived PIV Authentication data object 3. Extract the value of the keyUsage extension from the certificate
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns the requested data object along with the status word '90 00'. 3. From Step 3, the digitalSignature bit has been set. No other bits have been set.

754

755 **9.3.1.5 Certificate Policy**

Test Assertion	TA-09.03.01.05
Purpose	Verifies that the Derived PIV Authentication certificate asserts the appropriate certificate policy OID.
DTR(s)	• DTR-07.03.01.06
Issuer Documentation	None.
Precondition(s)	• A token with the Derived PIV Application token is inserted into an appropriate token reader.

	• Suitable drivers have been loaded between the test system and an instance of the reader. • A Derived PIV Authentication certificate is present within the Derived PIV Application.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the GET DATA command with • Data field of the command containing the tag ('5FC105') of the X.509 Certificate for Derived PIV Authentication data object. 3. Extract the value of the certificatePolicies extension from the certificate.
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns the requested data object along with the status word '90 00'. 3. From Step 3, the certificatePolicies extension asserts either the id-fpki-common-derived-pivAuth or id-fpki-common-derived-pivAuth-hardware OID.

9.3.1.6 Authority Information Access Extension

Test Assertion	TA-09.03.01.06
Purpose	Verifies that the authority information access extension in the Derived PIV Authentication certificate is populated with: (i) the location to the OCSP server that provides status information for this certificate and (ii) the location to an HTTP accessible Web server where certificates issued to the issuer of this certificate may be found.
DTR(s)	• DTR-07.03.01.09 • DTR-07.03.01.11
Issuer Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • A Derived PIV Authentication certificate is present within the Derived PIV Application.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the GET DATA command with • Data field of the command containing the tag ('5FC105') of the X.509 Certificate for Derived PIV Authentication data object 3. Extract the the value of the authorityInfoAccess extension from the certificate.

Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command the requested data object along with the returns status word '90 00'. 3. From Step 3, an accessMethod containing id-ad-ocsp (1.3.6.1.5.5.7.48.1) is present that contains an accessLocation of type uniformResourceIdentifier where the scheme is "http" (not "https"). An id-ad-caIssuers (1.3.6.1.5.5.7.48.2) accessMethod is also present where the accessLocation is of type uniformResourceIdentifier and the scheme is "http."

758

759 **9.3.1.7 Asymmetric Key Pair**

Test Assertion	TA-09.03.01.07
Purpose	Verifies that the public key that exists in the Derived PIV Authentication certificate corresponds to the private key located in the Derived PIV Application.
DTR(s)	• DTR-07.03.01.13
Issuer Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • A Derived PIV Authentication certificate is present within the Derived PIV Application. • The Derived PIV Application Password is recorded. • The Derived PIV Application Password's retry counter is not 0.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the GET DATA command with • Data field of the command containing the tag ('5FC105') of the X.509 Certificate for Derived PIV Authentication data object. 3. Send the VERIFY command with • P2, key reference value, is set to '80' • Data field of the command will contain the correct Derived PIV Application Password, padded with 'FF' (if necessary) to complete the total length of the value to 8 bytes 4. Send the GENERAL AUTHENTICATE command • CLA is set to: 1. '00' if command chaining is not needed or '10' if command chaining is used. (The last chain of the command sets CLA to '00') • P1, algorithm reference, is set to '07' or '11'. P2, key reference, is set to '9A' indicating the Derived PIV Authentication Key

	• Data field in the command is to include '81' specifying a challenge, followed by a randomly generated challenge, and '82 00' in order to request a response 5. Verify the signature obtained in Step 4 using the subject public key from the certificate.
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns the requested data object along with status word '90 00'. 3. From Step 3, the command returns the status word '90 00'. 4. From Step 4, the command returns the signed challenge with the status word '90 00'. 5. From Step 5, the private key corresponds to the public key contained in the certificate as the signature verification succeeds.

760

761 **9.3.1.8 UUID in the subjectAltName**

Test Assertion	TA-09.03.01.08
Purpose	Verifies that a UUID is populated in the subjectAltName field of the Derived PIV Authentication certificate.
DTR(s)	• DTR-07.03.01.07
Issuer Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • A Derived PIV Authentication certificate is present within the Derived PIV Application.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the GET DATA command with • Data field of the command containing the tag ('5FC105') of the X.509 Certificate for Derived PIV Authentication data object 3. Extract the value of the subjectAltName extension from the certificate.
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns the requested data object along with the status word '90 00'. 3. From Step 3, a name of type uniformResourceIdentifier containing a UUID is present.

762

9.3.1.9 piv-interim Extension

Test Assertion	TA-09.03.01.09
Purpose	Verifies that the piv-interim extension is present in the Derived PIV Authentication certificate.
DTR(s)	• DTR-07.03.01.08
Issuer Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • A Derived PIV Authentication certificate is present within the Derived PIV Application.

Test Scenario	1. Send the SELECT command with
	  • AID == 'A0 00 00 03 08 00 00 20 00 01 00'
	2. Send the GET DATA command with
	  • Data field of the command containing the tag ('5FC105') of the X.509 Certificate for Derived PIV Authentication data object
	3. Extract the piv-interim extension from the certificate.

Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns the requested data object along with the status word '90 00'. 3. From Step 3, the non-critical piv-interim extension is present and contains the interim_indicator field, which is of type BOOLEAN.

9.3.1.10 cRLDistributionPoints Extension

Test Assertion	TA-09.03.01.10
Purpose	Verifies that the cRLDistributionPoints extension in the Derived PIV Authentication certificate contains an HTTP URI.
DTR(s)	• DTR-07.03.01.10
Issuer Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • A Derived PIV Authentication certificate is present within the Derived PIV Application.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the GET DATA command with

	• Data field of the command containing the tag ('5FC105') of the X.509 Certificate for Derived PIV Authentication data object 3. Extract the cRLDistributionPoints extension from the certificate.
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns the requested data object along with the status word '90 00'. 3. From Step 3, a URI with the "HTTP" scheme that can be used to access CRL information is present.

766

767 **9.3.1.11 RSA Exponent**

Test Assertion	TA-09.03.01.11
Purpose	Verifies that for RSA keys, the exponent of the asymmetric key for Derived PIV Authentication is equal to 65 537.
DTR(s)	• DTR-07.05.01.14
Issuer Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • A Derived PIV Authentication certificate is present within the Derived PIV Application.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the GET DATA command with • Data field of the command containing the tag ('5FC105') of the X.509 Certificate for Derived PIV Authentication data object 3. Extract the subjectPublicKeyInfo->subjectPublicKey from the certificate. 4. Parse the exponent from the extracted public key.
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns the requested data object along with the status word '90 00'. 3. From Step 4, the exponent of the RSA asymmetric key for PIV Authentication is equal to 65 537.

768

9.3.2 X.509 Certificate for Digital Signature[18]

9.3.2.1 Signature Algorithm

Test Assertion	TA-09.03.02.01
Purpose	Verifies that the proper signature algorithm has been used to sign the digital signature certificate as specified in Table 3-3 of [SP800-78].
DTR(s)	• DTR-07.03.02.01 • DTR-07.03.02.02
Issuer Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • A digital signature certificate is present within the Derived PIV Application.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the GET DATA command with • Data field of the command containing the tag ('5FC10A') of the X.509 Certificate for Digital Signature data object 3. Extract signature->algorithm field value from the certificate.
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns the requested data object along with the status word '90 00'. 3. From Step 3, the algorithm value is in accordance with Table 3-3 of [SP800-78]. If the algorithm value is id-RSASSA-PSS, then the hashAlgorithm field in signature->parameters is populated with SHA-256 (OID = 2.16.840.1.101.3.4.2.1). For RSA with PKCS #1 v1.5 padding, the parameters field is populated with NULL. For ECDSA, the parameters field is absent.

9.3.2.2 Subject Public Key Algorithm

Test Assertion	TA-09.03.02.02
Purpose	Verifies that the public key algorithm used for generating the keys is as specified in Table 3-4 of [SP800-78].

[18] The digital signature key and certificate may be tested outside of the Derived PIV Application. Specific test assertions can be developed by test entities to test this key and certificate based on the environment (e.g., email application) in which the key pair is being used. See Appendix A for example testing approaches.

DTR(s)	• DTR-07.03.02.03 • DTR-07.03.02.04
Issuer Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • A digital signature certificate is present within the Derived PIV Application.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the GET DATA command with • Data field of the command containing the tag ('5FC10A') of the X.509 Certificate for Digital Signature data object 3. Extract subjectPublicKeyInfo->algorithm->algorithm field value. 4. Match the algorithm value to the Table 3-4 of [SP800-78]. 5. If the algorithm is elliptic curve, ensure that an OID from Table 3-5 of [SP800-78] is populated in the subjectPublicKeyInfo->algorithm->parameters->namedCurve field. Note: If the RSA algorithm is used, the subjectPublicKeyInfo->algorithm->parameters field will be NULL.
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns the requested data object along with the status word '90 00'. 3. From Steps 4 and 5, the digital signature key is generated using an allowed asymmetric key algorithm.

9.3.2.3 Public Key Size

Test Assertion	TA-09.03.02.03
Purpose	Verifies that the key size requirements are in accordance with Table 3-1 of [SP800-78].
DTR(s)	• DTR-07.03.02.09
Issuer Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • A digital signature certificate is present within the Derived PIV Application.

Test Scenario	1. Send the SELECT token command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the GET DATA command with • Data field of the command containing the tag ('5FC10A') of the X.509 Certificate for Digital Signature data object 3. Extract subjectPublicKeyInfo->algorithm->algorithm field value. 4. Extract the subjectPublicKeyInfo->subjectPublicKey from the certificate 5. Match the key size to Table 3-1 of [SP800-78].
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns the requested data object along with the status word '90 00'. 3. From Step 5, the key size is in accordance with Table 3-1 of [SP800-78].

9.3.2.4 Key Usage Extension

Test Assertion	TA-09.03.02.04
Purpose	Verifies that the digital signature certificate asserts the appropriate purposes for the key.
DTR(s)	• DTR-07.03.02.05
Issuer Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • A digital signature certificate is present within the Derived PIV Application.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the GET DATA command with • Data field of the command containing the tag ('5FC10A') of the X.509 Certificate for Digital Signature data object 3. Extract the value of the keyUsage extension from the certificate.
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns the requested data object along with the status word '90 00'. 3. From Step 3, the digitalSignature and nonRepudiation bits have been set. No other bits have been set.

9.3.2.5 Certificate Policy

Test Assertion	TA-09.03.02.05
Purpose	Verifies that the digital signature certificate asserts the appropriate certificate policy OID.
DTR(s)	• DTR-07.03.02.06
Issuer Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • A digital signature certificate is present within the Derived PIV Application.

Test Scenario	1. Send the SELECT command with
	  • AID == 'A0 00 00 03 08 00 00 20 00 01 00'
	2. Send the GET DATA command with
	  • Data field of the command containing the tag ('5FC10A') of the X.509 Certificate for Digital Signature data object.
	3. Extract the value of the certificatePolicies extension from the certificate.

Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns the requested data object along with the status word '90 00'. 3. From Step 3, the certificatePolicies extension asserts one of the following: id-fpki-common-policy, id-fpki-common-hardware or id-fpki-common-High.

9.3.2.6 Authority Information Access Extension

Test Assertion	TA-09.03.02.06
Purpose	Verifies that the authority information access extension in the digital signature certificate is populated appropriately and contains an id-ad-caIssuers (1.3.6.1.5.5.7.48.2) accessMethod, which points to the location where the certificates issued to the issuer of this certificate can be found.
DTR(s)	• DTR-07.03.02.07
Issuer Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • A digital signature certificate is present within the Derived PIV

	Application.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the GET DATA command with • Data field of the command containing the tag ('5FC10A') of the X.509 Certificate for Digital Signature data object. 3. Extract the value of the authorityInfoAccess extension from the certificate.
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns the requested data object along with the status word '90 00'. 3. From Step 3, the authorityInfoAccess extension contains an id-ad-caIssuers (1.3.6.1.5.5.7.48.2) accessMethod with an accessLocation of type uniformResourceIdentifier where the scheme is “http” or “ldap.”

781

782 **9.3.2.7 Asymmetric Key Pair**

Test Assertion	TA-09.03.02.07
Purpose	Verifies that the public key that exists in the digital signature certificate corresponds to the private key within the Derived PIV Application.
DTR(s)	• DTR-07.03.02.10
Issuer Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • A digital signature certificate is present within the Derived PIV Application. • The Derived PIV Application Password is recorded. • The Derived PIV Application Password’s retry counter is not 0.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the GET DATA command with • Data field of the command containing the tag ('5FC10A') of the X.509 Certificate for Digital Signature data object 3. Send the VERIFY command with • P2, key reference value, is set to '80' • Data field of the command will contain the correct Derived PIV Application Password, padded with 'FF' (if necessary) to complete the total length of the value to 8 bytes 4. Send the GENERAL AUTHENTICATE command • CLA is set to: 1. '00' if command chaining is not needed or

	'10' if command chaining is used. (The last chain of the command sets CLA to '00') • P1, algorithm reference, is set to '07', '11', or '14'. P2, key reference, is set to '9C' indicating the digital signature key • Data field in the command is to include '81' specifying a challenge, followed by a randomly generated challenge, and '82 00' in order to request a response 5. Verify the signature obtained in Step 4 using the subject public key from the certificate obtained in Step 2.
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns the requested data object along with status word '90 00'. 3. From Step 3, the command returns status word '90 00'. 4. From Step 4, the command returns the signed challenge with the status word '90 00' 5. From Step 5, the private key corresponds to the public key contained in the certificate as the signature verification succeeds.

783

784 **9.3.2.8 cRLDistributionPoints Extension**

Test Assertion	TA-09.03.02.08
Purpose	Verifies that the cRLDistributionPoints extension in the digital signature certificate contains at least one URI, either LDAP or HTTP.
DTR(s)	• DTR-07.03.02.08
Issuer Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • A digital signature certificate is present within the Derived PIV Application.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the GET DATA command with • Data field of the command containing the tag ('5FC10A') of the X.509 Certificate for Digital Signature data object 3. Extract the cRLDistributionPoints extension from the certificate.
Expected Result(s)	1. From Step 1, the command returns the application property

	template with the status word '90 00'. 2. From Step 2, the command returns the requested data object along with the status word '90 00'. 3. From Step 3, a URI with either the "LDAP" or "HTTP" scheme that can be used to access CRL information is present.

785

786 #### 9.3.2.9 RSA Exponent

Test Assertion	TA-09.03.02.09
Purpose	Verifies that for RSA keys, the exponent of the asymmetric key for digital signature is equal to 65 537.
DTR(s)	• DTR-07.03.02.11
Issuer Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • A digital signature certificate is present within the Derived PIV Application.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the GET DATA command with • Data field of the command containing the tag ('5FC10A') of the X.509 Certificate for Digital Signature data object 3. Extract the subjectPublicKeyInfo->subjectPublicKey from the certificate. 4. Parse the exponent from the extracted public key.
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns the requested data object along with the status word '90 00'. 3. From Step 4, the exponent of the RSA asymmetric key for digital signature is equal to 65 537.

787

788 ### 9.3.3 X.509 Certificate for Key Management[19]

789 #### 9.3.3.1 Signature Algorithm

Test Assertion	TA-09.09.03.01

[19] The key management key and certificate may be tested outside of the Derived PIV Application. Specific test assertions can be developed by test entities to test this key and certificate based on the environment (e.g., email application) in which the key pair is being used. See Appendix A for example of testing approaches.

Purpose	Verifies that the proper signature algorithm has been used to sign the key management certificate as specified in Table 3-3 of [SP800-78].
DTR(s)	• DTR-07.03.03.01 • DTR-07.03.03.02
Issuer Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • A key management certificate is present within the Derived PIV Application.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the GET DATA command with • Data field of the command containing the tag ('5FC10B') of the X.509 Certificate for Key Management data object 3. Extract signature->algorithm field value from the certificate.
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns the requested data object along with the status word '90 00'. 3. From Step 3, the algorithm value is in accordance with Table 3-3 of [SP800-78]. If the algorithm value is id-RSASSA-PSS, then the hashAlgorithm field in signature->parameters field is populated with SHA-256 (OID = 2.16.840.1.101.3.4.2.1). For RSA with PKCS #1 v1.5 padding, the parameters field is populated with NULL. For ECDSA, the parameters field is absent.

9.3.3.2 Subject Public Key Algorithm

Test Assertion	TA-09.03.03.02
Purpose	Verifies that the public key algorithm used for generating the keys is as specified in Table 3-4 of [SP800-78].
DTR(s)	• DTR-07.03.03.03 • DTR-07.03.03.04
Issuer Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader.

	• A key management certificate is present within the Derived PIV Application.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the GET DATA command with • Data field of the command containing the tag ('5FC10B') of the X.509 Certificate for Key Management data object 3. Extract subjectPublicKeyInfo->algorithm->algorithm field value. 4. Match the algorithm value to the Table 3-4 of [SP800-78]. 5. If the algorithm is elliptic curve, ensure that an OID from Table 3-5 of [SP800-78] is populated in the subjectPublicKeyInfo->algorithm->parameters->namedCurve field. Note: If the RSA algorithm is used, the subjectPublicKeyInfo->algorithm->parameters field will be be NULL.
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns the requested data object along with the status word '90 00'. 3. From Steps 4 and 5, the key management key is generated using an allowed asymmetric key algorithm.

9.3.3.3 Public Key Size

Test Assertion	TA-09.09.03.03
Purpose	Verifies that the key size requirements are in accordance with Table 3-1 of [SP800-78].
DTR(s)	• DTR-07.03.03.09
Issuer Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • A key management certificate is present within the Derived PIV Application.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the GET DATA command with • Data field of the command containing the tag ('5FC10B') of the X.509 Certificate for Key Management data object 3. Extract subjectPublicKeyInfo->algorithm->algorithm field value. 4. Extract the subjectPublicKeyInfo->subjectPublicKey

	from the certificate. 5. Match the key size to Table 3-1 of [SP800-78].
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns the requested data object along with the status word '90 00'. 3. From Step 5, the key size is in accordance with Table 3-1 of [SP800-78].

9.3.3.4 Key Usage Extension

Test Assertion	TA-09.03.03.04
Purpose	Verifies the key management certificate asserts the appropriate purposes for the key.
DTR(s)	• DTR-07.03.03.05
Issuer Documentation	None.
Precondition(s)	• A Token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • A key management certificate is present within the Derived PIV Application.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the GET DATA command with • Data field of the command containing the tag ('5FC10B') of the X.509 Certificate for Key Management data object 4. Extract subjectPublicKeyInfo->algorithm->algorithm field value. 5. Extract the value of the keyUsage extension from the certificate.
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns the requested data object along with the status word '90 00'. 3. From Step 5, if the public key algorithm is RSA, then the keyUsage extension only asserts the keyEncipherment bit. If the public key algorithm is elliptic curve, then the keyUsage extension only asserts the keyAgreement bit.

9.3.3.5 Certificate Policy

Test Assertion	TA-09.03.03.05
Purpose	Verifies the key management certificate asserts the appropriate certificate policy OID.

DTR(s)	• DTR-07.03.03.06
Issuer Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • A key management certificate is present within the Derived PIV Application.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the GET DATA command with • Data field of the command containing the tag ('5FC10B') of the X.509 Certificate for Key Management data object 3. Extract the value of the certificatePolicies extension from the certificate.
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns the requested data object along with the status word '90 00'. 3. From Step 3, the certificatePolicies extension asserts one of the following: id-fpki-common-policy, id-fpki-common-hardware or id-fpki-common-High.

798

799 **9.3.3.6 Authority Information Access Extension**

Test Assertion	TA-09.03.03.06
Purpose	Verifies that the authority information access extension in the key management certificate is populated appropriately and contains an id-ad-caIssuers (1.3.6.1.5.5.7.48.2) accessMethod, which points to the location where the certificates issued to the issuer of this certificate can be found.
DTR(s)	• DTR-07.03.03.07
Issuer Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • A key management certificate is present within the Derived PIV Application.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the GET DATA command with • Data field of the command containing the tag ('5FC10B') of the X.509 Certificate for Key Management data object 3. Extract the value of the authorityInfoAccess

	extension from the certificate.
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns the requested data object along with the status word '90 00'. 3. From Step 3, the authorityInfoAccess extension contains an id-ad-caIssuers (1.3.6.1.5.5.7.48.2) accessMethod with an accessLocation of type uniformResourceIdentifier where the scheme is “http” or “ldap.”

800

801 **9.3.3.7 Asymmetric Key Pair**

Test Assertion	TA-09.03.03.07
Purpose	Verifies that the public key that exists in the key management certificate corresponds to the private key within the Derived PIV Application.
DTR(s)	• DTR-07.03.03.10
Issuer Documentation	None.
Precondition(s)	• A Token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • A key management certificate is present within the Derived PIV Application. • The Derived PIV Application Password is recorded. • The Derived PIV Application Password’s retry counter is not 0.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the GET DATA command with • Data field of the command containing the tag ('5FC10B') of the X.509 Certificate for Key Management data object 3. Send the VERIFY command with • P2, key reference value, is set to '80' • Data field of the command will contain the correct Derived PIV Application Password, padded with 'FF' (if necessary) to complete the total length of the value to 8 bytes 4. Send the GENERAL AUTHENTICATE command • CLA is set to: 1. '00' if command chaining is not needed or '10' if command chaining is used. (The last chain of the command sets CLA to '00') • P1, algorithm reference, is set to '07', '11', or '14'. P2, key reference, is set to '9D' indicating the key management key • Data field in the command is to include one

	of the following: 1. If P1 = '07', the template '81' contains an encrypted key 2. If P1 = '11' or '14', the template '85' contains the other party's public key.[20] 5. Verify the response obtained in Step 4 using the subject public key from the certificate obtained in Step 2.
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns the requested data object along with the status word '90 00'. 3. From Step 3, the command returns status word '90 00' 4. From Step 4, for algorithm reference '07', the command returns the transported key with status word '90 00'. For algorithm reference '11' or '14', the command returns the shared secret Z[21] with status word '90 00'. 5. From Step 5, the private key corresponds to the public key contained in the certificate. For algorithm reference '07', the test tool application's copy of the plaintext key corresponds to the one received in the response to Step 4 from the token. For algorithm reference '11' or '14', the shared secret returned in Step 4 matches the shared secret computed off token.

802

803 **9.3.3.8 cRLDistributionPoints Extension**

Test Assertion	TA-09.03.03.08
Purpose	Verifies that the cRLDistributionPoints extension in the key management certificate contains at least one URIs, either LDAP or HTTP.
DTR(s)	• DTR-07.03.03.08
Issuer Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • A key management certificate is present within the Derived PIV Application.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the GET DATA command with • Data field of the command containing the tag

[20] Template '85' contains the other party's public key, a point on Curve P-256 or P-384, encoded as '04' || X || Y, without the use of point compression, as described in Section 2.3.3 of [SEC1].
[21] Z is the X coordinate of point P as defined in [SP800-56A], Section 5.7.1.2

	('5FC10B') of the X.509 Certificate for Key Management data object 3. Extract the cRLDistributionPoints extension from the certificate.
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns the requested data object along with the status word '90 00'. 3. From Step 3, a URI with either the "LDAP" or "HTTP" scheme that can be used to access CRL information is present.

804

805 **9.3.3.9 RSA Exponent**

Test Assertion	TA-09.09.03.09
Purpose	Verifies that for RSA keys, the exponent of the asymmetric key for key management is equal to 65 537.
DTR(s)	• DTR-07.03.03.11
Issuer Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • A key management certificate is present within the Derived PIV Application.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the GET DATA command with • Data field of the command containing the tag ('5FC10B') of the X.509 Certificate for Key Management data object 3. Extract the subjectPublicKeyInfo->subjectPublicKey from the certificate. 4. Parse the exponent from the extracted public key.
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns the requested data object along with the status word '90 00'. 3. From Step 4, the exponent of the RSA asymmetric key for key management is equal to 65 537.

806

807 **9.3.4 X.509 Certificate of the Derived PIV Credential Issuer (Content Signing)**

808 **9.3.4.1 Signature Algorithm**

Test Assertion	TA-09.03.04.01
Purpose	Verifies that the signature field of the Derived PIV Credential Issuer's (content signing) certificate specifies one of the following

	algorithm OIDs: 1.2.840.113549.1.10 (id-RSASSA-PSS), 1.2.840.113549.1.11 (Sha256WithRSAEncryption), 1.2.840.10045.4.3.2 (edsa-with-Sha256), 1.2.840.10045.4.3.3 (edsa-with-Sha384).
DTR(s)	• DTR-07.03.04.01 • DTR-07.03.04.02
Issuer Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • A Security Object is present within the Derived PIV Application.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the GET DATA command with • Data field of the command containing the tag ('5FC106') of the Security Object 3. Extract and parse the certificates field contents from the Security Object. 4. Extract signature->algorithm field value from the certificate.
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns the requested data object along with the status word '90 00'. 3. From Step 4, the algorithm value is in accordance with Table 3-3 of [SP800-78]. If the algorithm value is id-RSASSA-PSS, then the hashAlgorithm field in signature->parameters is populated with SHA-256 (OID = 2.16.840.1.101.3.4.2.1). For RSA with PKCS #1 v1.5 padding, the parameters field is populated with NULL. For ECDSA, the parameters field is absent.

9.3.4.2 Subject Public Key Algorithm

Test Assertion	TA-09.03.04.02
Purpose	Verifies that the public key algorithm used for generating the keys is one of the following OIDs: 1.2.840.113549.1.1.1 (RSA Encryption) or 1.2.840.10045.2.1 (elliptic curve key).
DTR(s)	• DTR-07.03.04.03 • DTR-07.03.04.04
Issuer Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader.

	• Suitable drivers have been loaded between the test system and an instance of the reader. • A Security Object is present within the Derived PIV Application.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the GET DATA command with • Data field of the command containing the tag ('5FC106') of the Security Object 3. Extract and parse the certificates field contents from the Security Object. 4. Extract subjectPublicKeyInfo->algorithm->algorithm field value from the extracted certificate. 5. Match the algorithm value to the Table 3-4 of [SP800-78]. 6. If the algorithm is elliptic curve, ensure that an OID from Table 3-5 of [SP800-78] is populated in the subjectPublicKeyInfo->algorithm->parameters->namedCurve field. Note: If the RSA algorithm is used, the subjectPublicKeyInfo->algorithm->parameters field will be NULL.
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns the requested data object along with the status word '90 00'. 3. From Step 5, the Derived PIV Credential Issuer's (content signing) key pair is generated using an allowed asymmetric key algorithm. 4. From Step 6, the Derived PIV Credential Issuer's (content signing) key pair is generated using an allowed curve.

9.3.4.3 Public Key Size[22]

Test Assertion	TA-09.03.04.03
Purpose	Verifies that size of the subject public key in the Derived PIV Credential Issuer's (content signing) certificate conforms to Table 3-2 of [SP800-78].
DTR(s)	• DTR-07.03.04.10
Issuer Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader.

[22] Note that the Security Object for a Derived PIV Application is signed using a private key whose corresponding public key is contained in a Derived PIV Credential Issuer's (content signing) certificate.

	• A Security Object is present within the Derived PIV Application.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the GET DATA command with • Data field of the command containing the tag ('5FC106') of the Security Object 3. Extract and parse the certificates field contents from the Security Object. 4. Extract subjectPublicKeyInfo->algorithm->algorithm field value. 5. Extract the subjectPublicKeyInfo->subjectPublicKey from the certificate 6. Match the key size to Table 3-2 of [SP800-78].
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns the requested data object along with the status word '90 00'. 3. From Step 6, the key size is in accordance with Table 3-2 of [SP800-78].

9.3.4.4 Key Usage Extension

Test Assertion	TA-09.03.04.04
Purpose	Verifies the Derived PIV Credential Issuer's (content signing) certificate asserts the appropriate purpose for the key.
DTR(s)	• DTR-07.03.04.05
Issuer Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • A Security Object is present within the Derived PIV Application.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the GET DATA command with • Data field of the command containing the tag ('5FC106') of the Security Object 3. Extract and parse the certificates field contents from the Security Object. 4. Extract the value of the keyUsage extension from the certificate.
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command the requested data object along with the returns status word '90 00'. 3. From Step 4, the digitalSignature bit has been set. No other bits

	have been set.

9.3.4.5 Certificate Policy

Test Assertion	TA-09.03.04.05
Purpose	Verifies the Derived PIV Credential Issuer's (content signing) certificate asserts the appropriate certificate policy OID.
DTR(s)	• DTR-07.03.04.06
Issuer Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • A Security Object is present within the Derived PIV Application.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the GET DATA command with • Data field of the command containing the tag ('5FC106') of the Security Object 3. Extract and parse the certificates field contents from the Security Object. 4. Extract the value of the certificatePolicies extension from the certificate.
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command the requested data object along with the returns status word '90 00'. 3. From Step 4, the certificatePolicies extension asserts the id-fpki-common-piv-contentSigning policy.

9.3.4.6 Extended Key Usage

Test Assertion	TA-09.03.04.06
Purpose	Verifies the Derived PIV Credential Issuer's (content signing) certificate asserts the appropriate OID in the extended key usage extension.
DTR(s)	• DTR-07.03.04.07
Issuer Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • A Security Object is present within the Derived PIV

	Application.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the GET DATA command with • Data field of the command containing the tag ('5FC106') of the Security Object 3. Extract and parse the certificates field contents from the Security Object. 4. Extract the value of the extKeyUsage extension from the certificate.
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns the requested data object along with the status word '90 00'. 3. From Step 4, the extended key usage extension asserts the id-PIV-content-signing OID, indicating that the certificate is authorized to sign PIV data objects.

819

820 **9.3.4.7 Authority Information Access Extension**

Test Assertion	TA-09.03.04.07
Purpose	Verifies the authority information access extension in the Derived PIV Credential Issuer's (content signing) certificate is populated appropriately and contains the id-ad-caIssuers (1.3.6.1.5.5.7.48.2) accessMethod, which points to the location where the certificates issued to the issuer of this certificate can be found.
DTR(s)	• DTR-07.03.04.08
Issuer Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • A Security Object is present within the Derived PIV Application.
Test Scenario	1. Send the SELECT command with • AID == 'A0 00 00 03 08 00 00 20 00 01 00' 2. Send the GET DATA command with • Data field of the command containing the tag ('5FC106') of the Security Object 3. Extract and parse the certificates field contents from the Security Object. 4. Extract the value of the authorityInfoAccess extension from the certificate.
Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns the requested data object along with the status word '90 00'. 3. From Step 4, the authorityInfoAccess extension contains an id-

	ad-caIssuers (1.3.6.1.5.5.7.48.2) accessMethod with an accessLocation of type uniformResourceIdentifier where the scheme is “http.”

821

822 **9.3.4.8 cRLDistributionPoints Extension**

Test Assertion	TA-09.03.04.08
Purpose	Verifies that cRLDistributionPoints extension in the Derived PIV Credential Issuer’s (content signing) certificate contains at least one URI, either LDAP or HTTP.
DTR(s)	• DTR-07.03.04.09
Issuer Documentation	None.
Precondition(s)	• A token with the Derived PIV Application is inserted into an appropriate token reader. • Suitable drivers have been loaded between the test system and an instance of the reader. • A Security Object is present within the Derived PIV Application.

Test Scenario	1. Send the SELECT command with
	  • AID == 'A0 00 00 03 08 00 00 20 00 01 00'
	2. Send the GET DATA command with
	  • Data field of the command containing the tag ('5FC106') of the Security Object
	3. Extract and parse the certificates field contents from the Security Object
	4. Extract the cRLDistributionPoints extension from the certificate.

Expected Result(s)	1. From Step 1, the command returns the application property template with the status word '90 00'. 2. From Step 2, the command returns the requested data object along with the status word '90 00'. 3. From Step 4, a URI with either the “LDAP” or “HTTP” scheme that can be used to access CRL information is present.

823

Appendix A—Testing of Derived PIV Credentials on Embedded Tokens

Embedded hardware tokens are not removable from the mobile device, but may be accessed by software using the underlying cryptographic interface of the mobile device. Since these tokens are built into the mobile device, they do not require an application interface definition to enable communication between the token and the mobile device native environment. Nevertheless, embedded tokens can be tested for the service they provide. Two types of testing are described below:

A.1 Functional Testing

In order to ensure that an embedded Derived PIV Credential follows the specification, test entities may develop test assertions to test these credentials within their operating environment. For example, in order to determine if a Derived PIV Authentication certificate and associated private key on the mobile device can be used for authentication, a test entity may set up an TLS-enabled test website and test whether a mobile device with an embedded Derived PIV Authentication certificate can successfully authenticate to the site. Similarly, for testing digital signature and encryption capabilities, a native email client on a mobile device may be setup to sign or decrypt Secure/Multipurpose Internet Mail Extensions (S/MIME) messages and the results reviewed to determine suitable functionality.

A.2 Data Model Testing

In order to perform data model conformance testing, test entities need to obtain the certificates (i.e., Derived PIV Authentication, digital signature, and key management). Methods for obtaining the certificates include, but are not limited to, (i) performing a functional test and acquiring the certificate by means of that test, (ii) using vendor-specific interface commands to extract the certificates, or (iii) requesting the certificates from the issuer directly.

Once the certificates have been obtain, test entities can follow (as appropriate) the test assertions from Section 9.3 to verify that the certificates conform to the appropriate profiles.

Appendix B—Acronyms

API	Application Programming Interface
BER	Basic Encode Rules
CMS	Cryptographic Message Syntax
CRL	Certificate Revocation List
DTR	Derived Test Requirement
ECDH	Elliptic Curve Diffie–Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
HSPD	Homeland Security Presidential Directive
HTTP	Hypertext Transfer Protocol
ICCD	Integrated Circuit(s) Card Devices
IUT	Implementation Under Test
NIST	National Institute of Standards and Technology
OSCP	Online Certificate Status Protocol
OID	Object Identifier
PC	Personal Computer
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PSS	Probabilistic Signature Scheme
PUK	Password Unblocking Key
RSA	Rivest Shamir Adleman
SD	Secure Digital
SHA	Secure Hash Algorithm
S/MIME	Secure/Multipurpose Internet Mail Extensions
SSP	Shared Service Provider
TA	Test Assertion
TLV	Tag-Length-Value
USB	Universal Serial Bus
UICC	Universal Integrated Circuit Cards
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

Appendix C—Glossary of Terms

Application Protocol Data Unit	A part of the application layer in the Open Systems Interconnection Reference model that is used for communication between two separate device's applications. In the context of smart cards, an APDU is the communication unit between a smart card reader and a smart card. The structure of the APDU is defined by [ISO7816-4].
Derived PIV Application	A standardized application residing on a cryptographic token that hosts a Derived PIV Credential and associated mandatory and optional elements.
Derived PIV Credential	An X.509 Derived PIV Authentication certificate, which is issued in accordance with the requirements specified in [SP800-157], where the PIV Authentication certificate on the Applicant's PIV Card serves as the original credential. The Derived PIV Credential is an additional common identity credential under [HSPD12] and [FIPS201] that is issued by a Federal department or agency and that is used with mobile devices

All other significant technical terms used within this document are defined in other key documents including [FIPS201], [SP800-63], and [SP800-73].

Appendix D—References

[FIPS140] Federal Information Processing Standards (FIPS) 140-2, *Security Requirements for Cryptographic Modules*, May 2001. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

[FIPS201] Federal Information Processing Standards (FIPS) Publication 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, August 2013. http://dx.doi.org/10.6028/NIST.FIPS.201-2

[GPSE] *GlobalPlatform Card Secure Element Configuration v1.0,* October 2012. http://www.globalplatform.org/specificationscard.asp.

[HSPD12] Homeland Security Presidential Directive-12, *Policies for a Common Identification Standard for Federal Employees and Contractors*, August 27, 2004. http://www.dhs.gov/homeland-security-presidential-directive-12

[ICCDSPEC] *Universal Serial Bus Device Class: Smart Card ICCD Specification for USB Integrated Circuit(s) Card Devices*, Revision 1.0, April 2005. http://www.usb.org/developers/devclass_docs/DWG_Smart-Card_USB-ICC_ICCD_rev10.pdf

[ISO7816-4] International Organization for Standardization/International Electrotechnical Commission, *Identification cards — Integrated circuit cards – Part 4: Organization, security and commands for interchange,* ISO/IEC 7816-4:2013, 2013. http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54550

[PROF] *X.509 Certificate and Certificate Revocation List (CRL) Profile for the Shared Service Providers (SSP) Program*, Version 1.7, May 2015. http://idmanagement.gov/documents/certificate-and-crl-extensions-profile-ssp-program.

[RFC2585] *Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP,* May 1999. https://tools.ietf.org/html/rfc2585

[RFC3370] *Cryptographic Message Syntax (CMS) Algorithms,* August 2002. https://tools.ietf.org/html/rfc3370

[RFC4122] *A Universally Unique IDentifier (UUID) URN Namespace,* July 2005. https://tools.ietf.org/rfc/rfc4122

[RFC5652] *Cryptographic Message Syntax,* September 2009. https://tools.ietf.org/html/rfc5652

[RFC5751] *Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2*

Message Specification, January 2010. https://tools.ietf.org/html/rfc5751

[SEC1] Standards for Efficient Cryptography Group (SECG), "SEC 1: Elliptic Curve Cryptography," Version 1.0, September 2000.

[SP800-56A] NIST Special Publication 800-56A Revision 2, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, May 2013. http://dx.doi.org/10.6028/NIST.SP.800-56Ar2

[SP800-63] NIST Special Publication 800-63-2, *Electronic Authentication Guideline*, August 2013. http://dx.doi.org/10.6028/NIST.SP.800-63-2

[SP800-73] NIST Special Publication 800-73-4, *Interfaces for Personal Identity Verification*, May 2015. http://dx.doi.org/10.6028/NIST.SP.800-73-4

[SP800-78] NIST Special Publication 800-78-4, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, May 2015. http://dx.doi.org/10.6028/NIST.SP.800-78-4

[SP800-79] NIST Special Publication 800-79-2, *Guidelines for the Authorization of Personal Identity Verification Card Issuers and Derived PIV Credential Issuers)*, July 2015. http://dx.doi.org/10.6028/NIST.SP.800-79-2

[SP800-96] NIST Special Publication 800-96, *PIV Card to Reader Interoperability Guidelines*, September 2006. http://csrc.nist.gov/publications/nistpubs/800-96/SP800-96-091106.pdf

[SP800-157] NIST Special Publication 800-157, *Guidelines for Derived Personal Identity Verification (PIV) Credentials*, December 2014. http://dx.doi.org/10.6028/NIST.SP.800-157

884