



InterNational Committee for Information Technology Standards (INCITS)

Secretariat: Information Technology Industry Council (ITI)

1101 K Street NW, Suite 610, Washington, DC 20005

www.INCITS.org



eb-2016-00369

Document Date: 06/24/16

To: INCITS Members

Reply To: [Deborah J. Spittle](#)

Subject: Public Review and Comments Register for the Approval of:

INCITS 504-3:201x, Information Technology - Generic Identity Command Set Part 3 - GICS
Platform Testing Requirements

Due Date: **The public review is from July 1, 2016 to August 30, 2016.**

Action: The InterNational Committee for Information Technology Standards ([INCITS](#)) announces that the subject-referenced document(s) is being circulated for a 60-day public review and comment period. Comments received during this period will be considered and answered. Commenters who have objections/suggestions to this document should so indicate and include their reasons.

All comments should be forwarded not later than the date noted above to the following address:

INCITS Secretariat/ITI

1101 K Street NW - Suite 610

Washington DC 20005-3922

Email: comments@standards.incits.org (preferred)

This public review also serves as a call for patents and any other pertinent issues (copyrights, trademarks). Correspondence regarding intellectual property rights may be emailed to the INCITS Secretariat at patents@itic.org.

INCITS B10.12 Task Group

- Authorized by INCITS
Procedures -- Distributed by INCITS - **B10.12 IC Cards with Contacts**
Task Group: _____

Title: Information Technology – Generic Identity Command Set Card Application Command Set Part 3 – Card Command Set Testing		Date:	May 18, 2016
		Source:	-
		Editor:	Ellick Chan
		Email:	echan@exponent.com
Project #:	IN 2094	Contact #:	+1 650 688-7152
Version:	0.15		

Project Editor Revision #	Date	B10.12 Doc.#	Description / Comments
	6/17/2010	2010-00063	Presentation of Scope for Part 3
0.1	7/26/2010	2010-00077	Draft GICS Part 3 – Initial Version; Comments due by 8/1/2010
0.2	10/4/2010		Updated earlier draft for GICS Part 3 IAW changes made to GICS v85 Part 1 and GICS v19 Part2
0.3	12/31/2010		Updated v0.20 of GICS Part 3 IAW changes made to GICS v0.86 Part 1 and v0.20 Part 2.
0.4	3/25/2011		Revised v0.30 to better reflect the requirements of testing GICS v0.87 Part 1 and v0.20 Part 2. Several test cases that were based on the informal use of “shall” in Part 1 were eliminated. Other test cases were added to make Part 3 more comprehensive.
0.5	8/12/2011		Added comments and performed an initial and partial revision of Part 3 to reflect latest changes in new versions of Part 1 (v88) and Part 2 (v21).
0.6	8/2/2012	2012-00079	New version issued to confirm to the revised guiding principles that originated from the Part 3 Ad Hoc group and were established during the May 2012 B10.12 meeting.
0.7	9/13/2012		Changed Editor Name and Information; Revised Document to reflect most recent versions of Parts 1 and 2 as well as committee discussions at Minneapolis meeting.
0.8	11/29/2012		Revised document to reflect comments discussed during Oct 29-30 telecon.

Project Editor Revision #	Date	B10.12 Doc.#	Description / Comments
0.9	1/18/2013		Revised document to reflect comment resolution from Jan 2013 B10.12 meeting. Created informative annex to capture assertions impacted by potential Part 1 and 2 Amendments.
0.10	2/28/2013		Revised document to reflect comment resolution from Feb 26 2013 B10.12 telecon.
0.11	4/8/2014		Revised document to reflect comment resolution on Parts 1 & 2 as of March 22, 2014.
0.12	4/21/2015		Changed Editor Name and Information; Revised Document to reflect most recent versions of Parts 1 amendment 1 and 2 amendment 1.
0.13	8/11/2015		Updated to harmonize with updates from Parts 1 and 2 amendment 1.
0.14	12/1/2015		Updated to address the comments from the Nov 18 Ad hoc meeting.
0.15	5/18/2016		Updated to include corrections as a result of ANSI queries. Updated document number and date.

INCITS Standard

INCITS 504-3 :201x

B10.12 INPUT for INCITS PROJECT #2094

Revision 0.15
May 18, 2016

**INCITS Standard:
Information Technology – Generic Identity Command
Set**

Part 3: GICS Platform Testing Requirements

DRAFT

This is draft standard of B10, a Technical Committee of Accredited Standards Committee INCITS. As such, this is not a completed standard and has not been approved. The contents may be modified by the B10 Technical Committee. This standard is made available for review and comment only.

Permission is granted to members of INCITS, its technical committees, and their associated task groups to reproduce this document for the purposes of INCITS standardization activities without further permission, provided this notice is included. All other rights are reserved. Any commercial or for-profit replication or republication is prohibited.

B10.12 Technical Editor
Ellick Chan

Telephone: +1 650 688 7152
E-Mail: echan@exponent.com



47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66

ANSI®
INCITS: 504-3-201X

American National Standard
for Information Technology –

Generic Identity Command Set

Part 3: GICS Platform Testing Requirements

DRAFT

Secretariat
Information Technology Industry Council

American National Standard

Approval of an American National Standard requires review by ANSI that the requirements for due process, consensus, and other criteria for approval have been met by the standards developer. Consensus is established when, in the judgment of the ANSI Board of Standards Review, substantial agreement has been reached by directly and materially affected interests. Substantial agreement means much more than a simple majority, but not necessarily unanimity. Consensus requires that all views and objections be considered, and that a concerted effort be made towards their resolution.

The use of American National Standards is completely voluntary; their existence does not in any respect preclude anyone, whether he has approved the standards or not, from manufacturing, marketing, purchasing, or using products, processes, or procedures not conforming to the standards. The American National Standards Institute does not develop standards and will in no circumstances give an interpretation of any American National Standard. Moreover, no person shall have the right or authority to issue an interpretation of an American National Standard in the name of the American National Standards Institute. Requests for interpretations should be addressed to the secretariat or sponsor whose name appears on the title page of this standard.

CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time. The procedures of the American National Standards Institute require that action be taken periodically to reaffirm, revise, or withdraw this standard. Purchasers of American National Standards may receive current information on all standards by calling or writing the American National Standards Institute.

CAUTION NOTICE: The developers of this standard have requested that holders of patents that may be required for the implementation of the standard disclose such patents to the publisher. However, neither the developers nor the publisher have undertaken a patent search in order to identify which, if any, patents may apply to this standard. As of the date of publication of this standard and following calls for the identification of patents that may be required for the implementation of the standard, no such claims have been made. No further patent search is conducted by the developer or publisher in respect to any standard it processes. No representation is made or implied that licenses are not required to avoid infringement in the use of this standard.

Published by
INCITS/Information Technology Industry Council
1101 K Street NW, Suite 610, Washington DC 20005
Copyright 2009 by INCITS/Information Technology Industry Council
All rights reserved.

Table of Contents

108		
109		
110	1. Overview.....	9
111	1.1 Purpose and Scope	9
112	1.2 Normative References	10
113	2. Definitions, abbreviations and conventions.....	13
114	2.1 Terms and Definitions.....	13
115	2.2 Acronyms, Abbreviations and Symbols	14
116	3. Requirement Definition Method.....	18
117	4. GICS Test Requirements - Card Application Command Set	19
118	4.1 Test of Data Structures for GICS-Applications	19
119	4.1.1 Global Objects	19
120	4.1.2 Files	20
121	4.1.3 Data Objects	23
122	4.2 Security Architecture.....	25
123	4.3 Assigned Values	27
124	4.4 Generic Identity Command Set – Application.....	34
125	4.4.1 SELECT	34
126	4.4.2 SELECT DATA	36
127	4.4.3 GET DATA.....	37
128	4.4.4 PUT DATA	40
129	4.4.5 VERIFY	43
130	4.4.6 CHANGE REFERENCE DATA	44
131	4.4.7 RESET RETRY COUNTER.....	46
132	4.4.8 MANAGE SECURITY ENVIRONMENT (Set)	47
133	4.4.9 GENERAL AUTHENTICATE.....	49
134	4.4.10 PERFORM SECURITY OPERATION	50
135	4.4.11 GET RESPONSE (For Transmission Handling).....	51
136	4.5 Operation	52
137	4.5.1 Model of Computation.....	52
138	4.5.2 Interindustry Data Objects	52
139	4.6 Signature and Key Establishment Protocols	52
140	4.6.2 Signature Protocols	53
141	4.6.3 Key Establishment Protocols.....	54
142	4.6.4 Session Key Establishment	54
143	4.7 Secure Messaging	55
144	4.7.2 AES Secure Messaging.....	55
145	4.8 Card Manager Application (INCITS 504 Part 2 Test Requirements)	56
146	4.8.1 Overview	56
147	4.8.2 Initial –GICS State	57
148	4.8.3 Updates.....	58
149	4.8.4 Commands	59
150	4.8.5 Data Structure.....	59
151	4.8.6 Card Identification Scheme	61
152	4.8.7 Card Management Scheme.....	62
153	4.9 Application Management	62
154	4.9.1 Application Life Cycle	62
155	4.9.2 Security Attributes.....	62
156	4.10 File Management.....	63
157	4.10.1 File Life Cycle	63
158	4.10.2 Data Structures for File Management.....	63
159	4.11 Key Management.....	63

DRAFT Generic Identity Command Set – Part 3: GICS Platform Testing Requirements

160	4.11.1	Key Life Cycle.....	63
161	4.12	Authentication Objects Management.....	63
162		Authentication Objects Life Cycle	63
163	4.13	Administrative Command Set	64
164	4.13.1	APPLICATION MANAGEMENT REQUEST.....	64
165	4.13.2	REMOVE APPLICATION	64
166	4.13.3	CREATE DO	65
167	4.13.4	DELETE DO	66
168	4.13.5	CREATE FILE	66
169	4.13.6	DELETE FILE	67
170	4.13.7	ACTIVATE FILE.....	67
171	4.13.8	DEACTIVATE FILE.....	67
172	4.13.9	GENERATE ASYMMETRIC KEY PAIR	68
173	4.13.10	PUT DATA (Key)	68
174			

Foreword (This forward is not part of INCITS 504-3-201X.)

This American National Standard describes the test requirements for the Generic Identity Command Set.

Requests for interpretation, suggestions for improvement or addenda, or defect reports are welcome. They should be sent to the International Committee for Information Technology Standards, 1250 Eye Street, NW, Suite 200, Washington, DC 20005.

American National Standard for Information Technology --

Generic Identity Command Set

Part 3: GICS Platform Testing Requirements DRAFT

1. Overview

Generic Identity Command Set (GICS) is multi-part U.S. National Standard:

- Part 1: Card Application Command Set
- Part 2: Card Administrative Command Set
- Part 3: GICS Platform Testing Requirements
- Part 4: Card Application Profile Template

GICS provides for Personal Identity Verification (PIV), PIV-I (PIV-Interoperable) and Common Access Card (CAC) card-applications (but not limited to these applications) to be built from a single platform. GICS defines an open platform (it is not a card application) where card applications can be instantiated and deployed according to card application profiles defined through the Part 4 template. GICS is operating system (OS) agnostic and can coexist with other platforms and/or non GICS-based applications.

Fully compliant GICS platforms are interoperable with any GICS-compliant card management and card provisioning system. For example, an application instantiated on a GICS platform, will be compatible and interoperable with the infrastructures relevant to that application. GICS is the common name for INCITS 504 standards and the two terms are used interchangeably.

GICS specifications follow these principles:

- Part 1 and Part 2 provide detailed and comprehensive specifications of all the application and administrative commands for the GICS platform.
- The 'GICS command set' defines data types, authentication protocols, access control definitions, and secure messaging.
- Part 4 provides a template for creating GICS application profiles which are strictly based on Part 1 and Part 2 specifications.
- Application profiles specify usage data models and security configurations.
- A GICS platform conformant to the GICS specifications fully implements Part 1 and Part 2.
- Part 3 provides conformance testing requirements for Parts 1 and 2.

1.1 Purpose and Scope

This part of the multi-part standard defined by INCITS 504 addresses the testing of assertions made in parts 1 and 2 of the standard. Part 3 of this multi-part standard will define conformity assessment to include the use of relevant existing conformity assessments.

DRAFT Generic Identity Command Set – Part 3: GICS Platform Testing Requirements

- Identity credential storage (Namespace standardization)
- Authentication protocols
- Biometric verification¹
- Confidentiality protocols
- Digital signatures
- Card management
- Application management
- Key management
- Related administrative management functions
- Card lifecycle model
- Card enablement

Test requirement definition for GICS Part 1 – Command Application Command Set and Part 2 – Card Administrative Command Set is defined with sufficient detail to satisfy GICS requirements. Testing of card application profile specifications for GICS application (Part 4) is out of scope for Part 3.

The scope for Part 3 Test is limited to definition for what testing is required and does not provide technical guidelines on the methodology to be used during the testing and validation of applicable components. Part 3 focuses on platform conformance testing of Part 1 and Part 2, and focuses on what needs to be tested to enforce full functionality and interoperability. In particular, instances of brute force, exhaustive, or open-ended negative testing are not specified in the requirements here-in. There are no test requirements for negative testing to determine abnormal behavior with the exception of interrogating access control rules and elicitation of error codes where possible and appropriate. It is expected that test methods, procedures and environments will be developed by commercial and/or government entities to be available for developers producing GICS compliant products.

FIPS 140-2 validation is out of scope for the GICS platform conformance testing. Product developers could use existing validation program to get their GICS Platform FIPS 140-2 validated.

1.2 Normative References

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

The following standards contain provisions that, through reference in the text, constitute provisions of this standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent editions of the standards listed below.

Copies of the following documents can be obtained from ANSI: 1) approved ANSI standards, 2) approved and draft international and regional standards (ISO, IEC, CEN/CENELEC, ITUT), and 3) approved and draft foreign standards (including BSI, JIS, and DIN). For further information, contact ANSI Customer Service Department at 212-642-4900 (phone), 212-302-1286 (fax), or via the World Wide Web at <http://www.ansi.org>.

- INCITS 504-1-2013, Generic Identity Command Set – Part 1: Card Application Command Set

¹ Note that the document does not completely specify biometric verification but only includes hooks for biometric data for future use.

DRAFT Generic Identity Command Set – Part 3: GICS Platform Testing Requirements

- 274 • INCITS 504-1-2013 Amendment 1, Generic Identity Command Set – Part 1: Card Application
275 Command Set
276
- 277 • INCITS 504-2-2013, Generic Identity Command Set – Part 2: Card Administration Command Set
278
- 279 • INCITS 504-2-2013 Amendment 1, Generic Identity Command Set – Part 2: Card Administration
280 Command Set
281
- 282 • ISO/IEC 8825-1:2008 – Information technology -- ASN.1 encoding rules: Specification of Basic
283 Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules
284 (DER).
285
- 286 • ISO/IEC 24727-1:2007 – Identification cards – Integrated circuit card programming interfaces – Part
287 1: Architecture
288
- 289 • ISO/IEC 24727-2:2008 – Identification cards – Integrated circuit card programming interfaces – Part
290 2: Generic card interface
291
- 292 • ISO/IEC 24727-3:2008 – Identification cards – Integrated circuit card programming interfaces – Part
293 3: Programming interface
294
- 295 • ISO/IEC 24727-4:2008– Identification cards – Integrated circuit card programming interfaces – Part
296 4: API administration
297
- 298 • ISO/IEC 24727-5:2011 – Identification cards – Integrated circuit card programming interfaces – Part
299 5: Test methods
300
- 301 • ISO/IEC 24727-6:201– Identification cards – Integrated circuit card programming interfaces – Part
302 6: Registration authority procedures for the authentication protocols for interoperability
303
- 304 • ISO/IEC 7816-4:2013, Identification cards — Integrated circuit cards — Part 4: Organization,
305 security and commands for interchange
306
- 307 • ISO/IEC 7816-5:2005, Identification cards — Integrated circuit cards — Part 5: Numbering System
308 and Registration Procedure for Application Identifiers (AID)
309
- 310 • ISO/IEC 7816-6:2004, Identification cards — Integrated circuit cards — Part 6: Interindustry data
311 elements
312
- 313 • ISO/IEC 7816-8:2004, Identification cards — Integrated circuit cards — Part 8: Commands for
314 security operation
315
- 316 • ISO/IEC 7816-9:2004, Identification cards — Integrated circuit cards — Part 9: Commands for card
317 management
318
- 319 • ISO/IEC 7816-11:2004, Identification cards — Integrated circuit cards — Part 11: Personal
320 verification through biometric methods
321
- 322 • ISO/IEC 7816-13:2007, Identification cards — Integrated circuit cards — Part 13: Commands for
323 application management in multi-application environment
324

DRAFT Generic Identity Command Set – Part 3: GICS Platform Testing Requirements

- 325 • NIST SP 800-73-4 Interfaces for Personal Identity Verification, Part 2 - End-Point PIV Card
326 Application Interface, May 2015
327
- 328 • NIST SP 800-78-2 Cryptographic Algorithms and Key Sizes for Personal Identity Verification,
329 February 2010
330

2. Definitions, abbreviations and conventions

2.1 Terms and Definitions

For the purposes of this document, the following terms and definitions shall apply:

Access Rule: Data element containing an access mode referring to an action and security conditions to fulfill before acting [ISO/IEC 7816-4].

Application: See GICS-Application.

Application Dedicated File: Structure hosting an application in a card [ISO/IEC 7816-4]. Note that embedded card-applications within a card-application are not supported by this standard.

Application Identifier: Data element (from five to sixteen bytes) that identifies a card-application [ISO/IEC 7816-4].

Application Profile: An application specific data model which will be defined by application developer based on the INCITS 504 Part 4 Application Profile Template.

Application Session: Span of time between the selection of a card-application and the selection of a different card-application or card reset whichever occurs first.

Card-Application: Uniquely addressable set of functionalities on an ICC that provide data storage and computational services to a client-application [ISO/IEC 24727-1].

Card-manager-application: GICS-application capable of managing a set of GICS-applications [GICS part 2].

Card Verifiable Certificate: Certificate that can be verified within the context of a card-application.

Client-Application: Processing software needing access to one or more card-application(s) [ISO/IEC 24727-1].

Command-Response Pair: Set of two messages at the interface: a command APDU followed by a response APDU in the opposite direction [ISO/IEC 7816-4].

Credential: Synonym for identity credential.

Currently Selected Application: Application dedicated file at the root of the file hierarchy.

Dedicated File: Structure containing file control information and, optionally, memory available for allocation [ISO/IEC 7816-4].

Data Element: Item of information seen at the interface for which are defined a name, a description of logical content, a format and a coding [ISO/IEC 7816-4 & ISO/IEC 7816-6].

Data Object: Information seen at the interface consisting of the concatenation of a mandatory tag field, a mandatory length field and a conditional value field [ISO/IEC 7816-4].

Elementary File: Set of data objects sharing the same file identifier and the same security attribute(s) [ISO/IEC 7816-4].

File Identifier: Two-byte data element used to address a file [ISO/IEC 7816-4].

GICS-Application: Card-application supporting an identity claim encoded as a collection of data objects and accessed with the Generic Identity Command Set.

GICS Platform: ICC or related embodiment hosting a card-manager-application and zero or more card-applications in compliance with this standard.

Identity Credential: Evidence attesting to one's right to credit or authority; in this standard, it is the GICS Card-Application data elements that are associated with an individual which authoritatively binds an identity (and, optionally, additional attributes) to that individual.

Integrated Circuit Card: Electronic component designed to perform processing and/or memory functions.

Platform: Specification of a computer system's hardware and operating system software that defines the environment in which other software operates.

Reference Data Qualifier: The reference data qualifier is a reference to a security object such as key or a PIN that is targeted by the APDU command.

Secure Messaging: Set of means for cryptographic protection of (parts of) command-response pairs [ISO/IEC 7816-4].

Security Attribute: Condition of use of objects in the card including stored data and data processing functions, expressed as a data element containing one or more access rules [ISO/IEC 7816-4].

Security Condition: Boolean expression in security states.

Security Environment: Set of components required by a card-application in the card for secure messaging or for security operations [ISO/IEC 7816-4].

Security State: Boolean variable indicating whether (TRUE) or not (FALSE) a particular security procedure such as an authentication protocol has been successfully executed since the last time this variable was set to FALSE.

Security Status: Collection of security states.

Template: Set of BER-TLV data objects forming the value field of a constructed BER-TLV data object [ISO/IEC 7816-4].

2.2 Acronyms, Abbreviations and Symbols

For the purposes of this document, the following acronyms, abbreviations and symbols shall apply.

ACD: Application Capability Description

ADF: Application Dedicated File

431 AES: Advanced Encryption Standard
432
433 AID: Application ID
434
435 AMB: Access Mode Byte
436
437 ANSI: American National Standards Institute
438
439 APDU: Application Programming Data Unit
440
441 ASCII: American Standard Code for Information Interchange
442
443 ASN.1: Abstract Syntax Notation One
444
445 AS: ASsertion
446
447 AT: Authentication Template
448
449 ATR: Answer-to-reset
450
451 BER: Basic Encoding Rules
452
453 CAC: Common Access Card
454
455 CCD: Card Capability Description
456
457 CER: Canonical Encoding Rules
458
459 CHV: Card Holder Verification
460
461 CLA: CLAss byte, the first byte in a command header
462
463 CP: Control Parameters
464
465 CRT: Control Reference Template
466
467 CT: Confidentiality Template
468
469 CVC: Card Verifiable Certificate
470
471 DER: Distinguished Encoding Rules
472
473 DES: Data Encryption Standard
474
475 DF: Dedicated File
476
477 DO: Data Object
478
479 DST: Digital Signature Template
480
481 DTR: Derived Test Requirement
482
483 ECC: Elliptic Curve Cryptography

DRAFT Generic Identity Command Set – Part 3: GICS Platform Testing Requirements

484 ECCCDH: Elliptic Curve Cryptography Cofactor Diffie-Hellman
485
486 ECDSA: Elliptic Curve Digital Signature Algorithm
487
488 EF: Elementary File
489
490 ENC: Encryption
491
492 FDB: File Descriptor Byte
493
494 FID: File Identifier
495
496 FIPS: Federal Information Processing Standard
497
498 FMD: File Management Data
499
500 FS: Forward Secrecy
501
502 GICS: Generic Identity Command Set
503
504 GUID: Global Unique Identifier
505
506 HT: Hash Template
507
508 ICC: Integrated Circuit Card (with or without contacts)
509
510 ID: Identifier
511
512 IEC: International Electrotechnical Commission
513
514 INCITS: InterNational Committee for Information Technology Standards
515
516 INS: INStruction byte, the second byte in a command header
517
518 ISO: International Organization for Standardization
519
520 IV: Initial Vector
521
522 KAT: Key Agreement Template
523
524 KDF: Key Derivation Function
525
526 KEK: Key Encryption Key
527
528 L_c: Length field for coding the number N_c
529
530 LCS: Life cycle status byte
531
532 L_e: Length field for coding the number N_e
533
534 M/O: Mandatory / Optional
535
536 MAC: Message Authentication Code

537 MF: Master File
538
539 MGF: Mask Generation Function
540
541 MOC: Match-On-Card
542
543 MSE: Manage Security Environment
544
545 N_c: Number of bytes in the command data field
546
547 N_e: Maximum number of bytes in the response data field
548
549 N_r: Number of bytes in the response data field
550
551 NIST: National Institute of Standards and Technology
552
553 OAEP: Optimal asymmetric encryption padding
554
555 P1: Parameter 1, the third byte in a command header
556
557 P2: Parameter 2, the fourth byte in a command header
558
559 PIN: Personal Identification Number
560
561 PIV: Personal Identity Verification
562
563 PIV-I: Personal Identity Verification – Interoperable
564
565 PKCS: Public-key cryptography standards
566
567 PRF: Pseudo-random Function
568
569 PSO: Perform Security Operation
570
571 PSS: Probabilistic Signature Scheme
572
573 RFU: Reserved for Future Use
574
575 RSA: Rivest Shamir Adleman
576
577 RSASSA: RSA Signature Scheme with Appendix
578
579 SAM: Secure Access Module
580
581 SCB: Security Condition Byte
582
583 SCP: Secure Channel Protocol
584
585 SEID: Security Environment ID
586
587 SHA: Secure Hashing Algorithm
588
589 SM: Secure Messaging

SP: Special Publication
SPT: Security Parameter Template
TBD: To Be Determined
TE: TEst Requirement
TLV: Tag Length Value
VE: Required VEndor Information
ZKM: Zero Key Management

3. Requirement Definition Method

All the characteristics of a GICS platform which are described in Part 1 or Part 2 and are central to the concept of an interoperable GICS platform are addressed in Part 3 with conformance test requirements. Specifically, each 'must', 'only' and 'shall' statements in Part 1 and Part 2 are addressed by the inclusion in Part 3 with a corresponding test requirement. There are no requirements provided for testing of a particular application that is loaded onto the platform.

Two types of test requirements are presented in this document. *Explicit Test Requirements* are extracted directly from normative assertive statements from Part 1 or Part 2 with minimal phrase alteration. *Derived Test Requirements* are used when additional clarification or modification to a condition statement is needed to leave no question as the meaning or intent of testing. Derived test requirements are also used to ensure correct and interoperable behavior intended in Parts 1 and 2.

Both types of test requirements consist of the following content:

Actual condition statements taken/derived from Part 1 and 2 — these include conditions for successful command execution for each command as well as exception behaviors explicitly specified by statements using the words "shall," "must," and other normative delimiters in the standard. The condition statements are identified by codes starting with 'AS' followed by a running sequence.

Required Vendor Information — these include information that the vendors (could also be agencies or integrators) are mandated to provide in their documentation. The Required Vendor Information is identified by codes starting with 'VE' followed by a running sequence. For brevity, the required vendor information content portion will be listed only when applicable to the test requirement. Note that VE is not currently used in this document.

Required Test Activities — these are actions that the tester has to perform in order to satisfy the requirements stated in actual condition statements. Required Test Activities are identified by codes starting with 'TE' followed by a description of what needs to be tested.

Validation of some DTRs are not covered by the test assertions provided in this document. These DTRs require compliance of a component with an external specification or standard such as the specifications for cryptographic algorithms. No required test procedures are provided for these DTRs, and a note is added to indicate that "this assertion is externally tested." The tester is required to check the vendor documentation for claimed compliance with such requirements or confirm the presence of an external test/compliance certificate obtained from the test organization, when applicable.

4. GICS Test Requirements - Card Application Command Set

4.1 Test of Data Structures for GICS-Applications

4.1.1 Global Objects

AS1.1 The following files and data structures are always accessible through GICS interface without changing the context. These files and structures shall always be accessible from the card manager application and other GICS applications.

- EF.ATR/INFO
- EF.DIR
- Card capability description (CCD)

The foregoing data are always freely retrievable from any Application Dedicated File (ADF) by using GET DATA. These files shall be type '39' files containing only BER-TLV data objects.

TE1.1.1 The tester shall validate that the indicated data structures are always accessible from the card-manager application and any other GICS application loaded on the platform using the GET DATA command with P1-P2 = File ID and a command data field of '5C 00'.

TE1.1.2 The tester shall verify that the indicated data structures are located in type '39' files as BER-TLV objects.

TE1.1.3 The tester shall verify that retrieval of the global objects does not deselect the currently selected EF and/or ADF.

TE1.1.4 The tester shall verify that retrieval of the global objects does not alter the current context.

AS1.2 No other EF within a GICS application shall have a File ID of '2F 01'.

TE1.2.1 The tester shall verify that the platform rejects the creation of a file having FID='2F 01'.

AS1.3 The response data to the command '00CB 2F01 02 5C00 00' (GET DATA of EF.ATR/INFO) is the concatenation of all Data Objects (DO) which are present in EF.ATR/INFO.

TE1.3.1 The tester shall verify that the response from GET DATA using the EF.ATR/INFO FID returns all data objects present in EF.ATR/INFO

AS1.4 The content of EF.DIR is constructed automatically by GICS and updated whenever a new GICS based card-application is created. The removal of a card-application deletes the AID in the EF.DIR.

TE1.4.1 The tester shall verify that creating and removing a GICS-based card-application triggers the required automatic updates of EF.DIR.

AS1.5 No other EFs within a GICS application shall have a File ID of '2F 00'

TE1.5.1 The tester shall verify that the platform rejects the creation of a file having FID='2F 00'.

AS1.6 The EF.DIR is freely retrievable global data and the response data field to the command '00CB 2F00 02 5C00 00' is the concatenation of all card-application templates, regardless of the currently selected EF or ADF.

DRAFT Generic Identity Command Set – Part 3: GICS Platform Testing Requirements

TE1.6.1 The tester shall verify that the content of EF.DIR is freely retrievable and that the response to the command '00CB 2F00 02 5C00 00' is the concatenation of all card-application templates, regardless of the currently selected EF or ADF.

AS1.7 A CCD DO (tag '7F 62') is always retrievable from all card-applications.

TE1.7.1 The tester shall verify that a CCD DO (tag '7F 62') is always retrievable from all card-applications.

TE1.7.2 The tester shall verify that tag '7F 62' is reserved for CCD DO.

AS1.8 No other EF within a GICS application shall use the File ID '3F FF' or '7F 62'.

TE1.8.1 The tester shall verify that platform rejects the creation of a file having FID='3F FF' or '7F 62'.

AS1.9 The CCD can be retrieved at any time and from any GICS ADF by using a GET DATA command with P1- P2 = '3F FF' and a command data field that contains '5C 02 7F 62'

TE1.9.1 The tester shall verify that the CCD can be retrieved at any time and from any GICS ADF by using a GET DATA command with P1-P2 = '3F FF' and a command data field that contains '5C 02 7F 62.'

4.1.2 Files

AS1.10 The GICS standard shall support the card-application file types described in the sub clauses of Part 1, Section 3.2.

TE1.10.1 None applicable. The files types are verified as part of more specific test requirements.

AS1.11 The following file identifier values are reserved by ISO/IEC 7816-4 and shall not be used to identify GICS data objects or files.

- '00 00' – Current file
- '00 4D' – Extended header data list
- '2F 00' – EF.DIR
- '2F 01' – EF.ATR/INFO
- '3F 00' – Master file
- '3F FF' – File from the current context
- 'FF FF' – Current template

TE1.11.1 The tester shall verify that the platform rejects the use of any reserved FIDs.

AS1.12 An ADF shall be defined as a structure with a name that contains control parameters, BER-TLV objects, security objects, and elementary files.

TE1.12.1 The tester shall verify that the platform supports creation of an ADF with control parameters, BER-TLV objects, security objects and elementary files.

AS1.13 Each ADF shall be associated with and uniquely named by an ISO/IEC 7816-4 application identifier. GICS applications can be selected only by application identifier (which can be discovered by using EF.DIR).

TE1.13.1 The tester shall verify that each ADF is uniquely named by an ISO-IEC 7816-4 application identifier.

- 740 TE1.13.2 The tester shall verify that an ADF can be selected by the application identifier present in
741 EF.DIR.
742 TE1.13.3 The tester shall verify that it is not possible to create an ADF with an application identifier
743 already present in EF.DIR.
744
- 745 **AS1.14 The files rooted at an ADF shall contain all the data objects encoding the data elements of**
746 **exactly one GICS-application. Application data objects are stored in the ADF or in the EFs**
747 **under the ADF.**
748
- 749 TE1.14.1 The tester shall verify that application data objects can be created both within the ADF and
750 within an EF under the ADF.
751 TE1.14.2 The tester shall verify that a given GICS application has a local name space and cannot employ
752 data objects or files that are not rooted at that ADF.
753
754
- 755 **AS1.15 The file descriptor byte of an ADF shall be '38'.**
756
- 757 TE1.15.1 The tester shall verify that an ADF with file description byte '38' is accepted by the platform.
758
- 759 **AS1.16 The cryptographic mechanisms available for use when an ADF is currently selected shall**
760 **be described in the cryptographic mechanism identifier template (tag 'AC') in the control**
761 **parameters template (tag '62') of the ADF.**
762
- 763 TE1.16.1 The tester shall verify that any algorithm listed in the cryptographic mechanism identifier
764 template of the CPT of the ADF is available for use when the ADF is currently selected.
765 TE1.16.2 The tester shall verify that any algorithm that is not listed in the cryptographic mechanism
766 identifier template of the CPT of the ADF is not available for use when the ADF is currently
767 selected.
768 TE1.16.3 The tester shall verify that if a GICS application uses any of the protocols defined in GICS Part
769 1, Table 23, the control parameters of an ADF for a GICS application uses cryptographic
770 mechanism identifier template (tag 'AC') to indicate which cryptographic mechanisms are used
771 from GICS Part 1, Table 23.
772
- 773 **AS1.17 The ACD DO shall be stored at the ADF level. The ACD of a selected card application can**
774 **be retrieved at any time with a GET DATA command with P1-P2 = '3F FF' and a command**
775 **data field that contains '5C 02 7F 63'. No other EFs within a GICS application shall have a**
776 **file ID of '7F 63'.**
777
- 778 TE1.17.1 The tester shall verify that the ACD of the selected application can be retrieved with GET DATA,
779 regardless of the current security status.
780 TE1.17.2 The tester shall verify that the ACD DO can be retrieved with a GET DATA command with P1-
781 P2 = '3F FF' (retrieval from the currently selected DF) and a command data field that contains
782 '5C 02 7F 63'.
783 TE1.17.3 The tester shall verify that the platform rejects the creation of a file having FID='7F 63'.
784
- 785 **AS1.18 An elementary file with file descriptor byte '39' shall contain only BER-TLV data objects.**
786 **The content of this EF is a concatenation of DOs that share the same access control rules.**
787
- 788 TE1.18.1 The tester shall verify that an EF with file descriptor byte '39' can contain one or more BER-TLV
789 data objects concatenated together.
790 TE1.18.2 The tester shall verify that the card only accepts BER-TLV data objects as data in a type '39' file.
791

AS1.19 An elementary file with file descriptor byte '31' shall contain the value field of exactly one BER-TLV data object. The tag of the data shall be the single BER-TLV tag of the data object to be retrieved from the file.

TE1.19.1 The tester shall verify that an EF with file descriptor byte '31' can contain the value field of exactly one BER-TLV object.

TE1.19.2 The tester shall verify that the tag of the BER-TLV data that was used to place the value field data in the file can be used to retrieve the data by tag.

AS1.20 A GET DATA referencing the data object type '31' file shall return a data object using the inter-industry discretionary data object '53'.

TE1.20.1 The tester shall verify that the response of a GET DATA command referencing the data object type '31' file shall return a data object using the inter-industry discretionary data object '53'.

AS1.21 A PUT DATA referencing the data object to be stored in a type '31' file shall indicate the data object tag but present the value of the data object using the inter-industry discretionary data object '53'.

TE1.21.1 The tester shall verify that the PUT DATA command executes successfully when placing data into a type '31' file when indicating the data object tag and presenting the value of the data object using the inter-industry discretionary data object '53'.

AS1.22 Certificates on GICS applications shall use tags in accordance with Section 3.2.3 of GICS Part 1.

TE1.22.1 Not separately tested.

AS1.23 Specific DO Tags must be used within the EFs to allow the CVC processing within authentication protocols. The specific DO tags for CVC are:

- '7F21': Card Verifiable Certificate
- '7F22': Card Verifiable Certificate, without Subject Identifier Value (Subject Identifier length is set to zero)
- '5F20': Subject Identifier Value

TE1.23.1 The tester shall verify that the listed DO tags for CVC allow CVC processing with the corresponding data within authentication protocols.

AS1.24 The Card Verifiable Certificate Format used by the GICS platform is as specified in Section 3.2.3.2 of GICS Part 1.

TE1.24.1 The tester shall verify that a CVC following the format specified in GICS Part 1, Section 3.2.3 is accepted by the platform for representing CVC as used within the authentication protocols.

AS1.25 Specific DO Tags must be used within the EFs to allow the X.509 certificate processing by the relying systems. The specific DO tags for X.509 certificates are:

- '70': Certificate
- '71': CertInfo
- '72': MSCUID (Optional)
- 'FE': Error Detection Code

TE1.25.1 The tester shall verify that an EF storing an X.509 certificate that includes the optional MSCUID data exposed the data objects listed above.

4.1.3 Data Objects

AS1.26 Data objects that do not have control parameters inherit security properties of EF or ADF in which they belong.

TE1.26.1 The tester shall verify that a data objects that do not have control parameters (normal data objects that are not security objects) inherit security properties of EF or ADF in which they belong.

AS1.27 Security objects such as PINs, passwords, symmetric (secret) keys, and asymmetric (public and private) keys are supported in GICS. Each of these objects shall have a control parameter template (tag '62') that defines its characteristics and use. The security objects defines their own access rules and do not inherit access control rules of an application they may be nested in.

TE1.27.1 The tester shall verify that the platform supports creation of security objects such as PINs, passwords, symmetric (secret) keys, and asymmetric (public and private) keys.

TE1.27.2 The tester shall verify a control parameter template can be defined for each security object.

TE1.27.3 The tester shall verify that the access control rules are taken from the dedicated CPT rather than from the application the SO is nested in.

AS1.28 There shall be exactly one security attribute associated with each security object and this attribute shall be described using the Security Parameter template (tag 'AD') within control parameters. Each security object shall be identified by a unique two byte security object number (tag '82' or '83' within tag 'AD').).

TE1.28.1 The tester shall verify that a security attribute can be associated with a security object that referenced the object using the two byte ID.

TE1.28.2 The tester shall verify that only one security attribute can be associated with a given security object.

TE1.28.3 The tester shall verify that each security object is identified by a unique two byte security object number.

AS1.29 The assigned value of security object shall not conflict with the file identifier values since security objects and files share the same namespace.

TE1.29.1 The tester shall verify that the platform rejects the creation of a security object that has the same identifier as an existing file object.

AS1.30 The first byte of the security object number shall be the cryptographic mechanism reference value as defined in Table 23 for the keys. The first byte of the security object number shall be '00' for PINs or passwords. The second byte of the security object number shall be reference data qualifier as assigned by application developer.

TE1.30.1 The tester shall verify that the first byte of the security object number follows the format described in Table 23.

TE1.30.2 The tester shall verify that the first byte of the security object number is '00' for PINs or passwords.

TE1.30.3 The tester shall verify that the second byte of the security object number is a valid reference data qualifier.

AS1.31 The security object security parameter template does not change when a key value is updated.

TE1.31.1 The tester shall verify that the object security parameter template does not change when a key value is updated.

AS1.32 A key can be updated with different properties by first deleting the existing security object and then creating a replacement object with the correct attributes.

TE1.32.1 The tester shall verify that a key is updated with different properties by deleting the existing security object and then creating a replacement object with different attributes.

AS1.33 Exactly one application template (tag '61') shall be associated with each ADF file. The application template shall contain data objects according to GICS Part 1, Table 15.

TE1.33.1 The tester shall verify that each ADF file has only one application template (tag '61').

TE1.33.2 The tester shall verify that the application template contains data objects according to GICS Part 1, Table 15.

AS1.34 Exactly one control parameter template (tag '62') shall be associated with each file or security object. The control parameter template associated with an ADF shall contain data objects according to GICS Part 1, Table 10.

TE1.34.1 The tester shall verify that each file or security object has only one control parameter template (tag '62').

TE1.34.2 The tester shall verify that the control parameter template associated with an ADF contains data objects according to GICS Part 1, Table 10.

AS1.35 The control parameter template associated with a file shall contain data objects according to GICS Part 1, Table 11.

TE1.35.1 The tester shall verify that the control parameter template associated with each file contains data objects according to GICS Part 1, Table 11.

AS1.36 The control parameter template associated with a security objects shall contain data objects according to GICS Part 1, Table 12.

TE1.36.1 The tester shall verify that the control parameter template associated with each security object contains data objects accordingly to GICS Part 1, Table 12.

AS1.37 The information that is related to a file is always available at the interface by using the response to the SELECT command (CP, FMD, or APT depending on command parameters).

TE1.37.1 The tester shall verify that information related to each file is always available at the interface by using the response to the SELECT command.

4.2 Security Architecture

AS2.1 An access control rule shall consist of an access mode and a security condition.

TE2.1.1 The tester shall verify that each access control rule consists of an access mode and a security condition.

AS2.2 The security status indicator of an authenticable entity shall be TRUE if the entity has been authenticated and FALSE otherwise.

TE2.2.1 The tester shall verify that the security status indicator of each authenticable entity is TRUE if and only if the entity has been authenticated and FALSE otherwise.

AS2.3 A successful execution of an authentication protocol shall set the security status indicator associated with the credential used in the protocol to TRUE.

TE2.3.1 The tester shall verify that a successful execution of an authentication protocol sets the security status indicator associated with the credential used in the protocol to TRUE.

AS2.4 An aborted or failed execution of an authentication protocol shall set the security status indicator associated with the credential used in the protocol to FALSE.

TE2.4.1 The tester shall verify that an aborted or failed execution of an authentication protocol sets the security status indicator associated with the credential used in the protocol to FALSE.

AS2.5 The global security status indicators shall remain unchanged when changing from one card-application to another.

TE2.5.1 The tester shall verify that the global security status indicators shall remain unchanged when changing from one card-application to another.

AS2.6 A security status indicator is said to be a card-application security status indicator if it is set to FALSE when the currently selected card-application changes from one card-application to another.

TE2.6.1 The tester shall verify that when the currently selected card-application changes from one card application to another the original card-application's security status indicator is set to FALSE.

AS2.7 Session keys generated using a global key in a successful execution of secure messaging shall be available to all card-applications. Session keys generated using card-application keys shall be destroyed when changing from one card-application to another.

TE2.7.1 The tester shall verify that session keys generated using a global key are available to all card applications.

TE2.7.2 The tester shall verify that session keys generated using card-application keys are destroyed when changing from one card application to another.

AS2.8 There shall be exactly one security attribute associated with each EF, ADF, or security object.

TE2.8.1 The tester shall verify that there is only one security attribute associated with each EF, ADF, or security object.

AS2.9 The security attribute associated with a file shall be the security attribute associated with all the data objects within that file.

TE2.9.1 The tester shall verify that the security attribute associated with each file is the security attribute associated with all the data objects within each file.

AS2.10 If a security condition is not provided for an access mode by any access rule(s) in the security attribute, then the security condition for the access mode shall be NEVER.

TE2.10.1 The tester shall verify that all security conditions that are not provided for an access mode by any access rule(s) in the security attribute have their security condition for the access mode set to NEVER.

AS2.11 Security attributes shall be encoded specific to physical interface (DO 'A3').

TE2.11.1 The tester shall verify that each security attribute is encoded specific to physical interface (DO 'A3').

AS2.12 Tag 'A3' shall be a concatenation of Physical Interface Type (DO '91') and security attribute in compact format (DO '8C'), as shown in GICS Part 1, Table 5. Any other security attribute tags should not be employed by GICS applications.

TE2.12.1 The tester shall verify that (DO 'A3') shall be a concatenation of Physical Interface Type (DO '91') and security attribute in compact format (DO '8C'), as shown in GICS Part 1, Table 5.

TE2.12.2 The tester shall verify that no other security attribute tags are employed by GICS applications.

AS2.13 The value of the Physical Interface Type (i.e., contact interface or contactless interface) shall be encoded in tag '91' in accordance with GICS Part 1, Table 6.

TE2.13.1 The tester shall verify that the value of the Physical Interface Type (i.e., contact interface or contactless interface) is encoded in DO '91' in accordance with GICS Part 1, Table 6.

AS2.14 There shall be exactly one SCB for each bit (command) set (i.e., equal to one) in the AMB and the SCB shall appear in the order of most significant bit to the least significant bit.

TE2.14.1 The tester shall verify that there is exactly one SCB for each bit (command) set in the AMB.

AS2.15 Since there will be multiple AMBs, each AMB shall be processed, sequentially in order of its appearance, until a successful evaluation. If none of the AMBs evaluate to TRUE, access to the target shall be denied.

TE2.15.1 The tester shall verify that each AMB is processed, sequentially in order of its appearance, until a successful evaluation.

TE2.15.2 The tester shall verify that if none of the AMBs evaluate to TRUE, access to the target shall be denied.

4.3 Assigned Values

AS3.1 Unless otherwise stated, all reserved values (even if not used in this standard) shall be reserved for further use by the INCITS B10 Technical Committee.

No requirement is taken from this statement. Any effort to restrict values does not support interoperability and prevent a platform conformant to a newer version of the standard that incorporates values that are presently reserved from being backwards compatible with this standard.

AS3.2 The class (CLA) byte of a command in the Generic Identity Command Set shall be one of the values in GICS Part 1, Table 9.

TE3.2.1 The tester shall verify that the class (CLA) byte of a command in the Generic Identity Command Set is one of the values in GICS Part 1, Table 9.

AS3.3 The control parameters template (tag '62') associated with an application ADF shall contain data objects with tags listed in GICS Part 1, Table 10; optional conditions shall be tested when present.

TE3.3.1 The tester shall verify that the control parameters template (tag '62') associated with each application ADF contains data objects with tags listed in GICS Part 1, Table 10.

TE3.3.2 The tester shall verify that optional conditions conform to GICS Part 1, Table 10 when present.

AS3.4 The control parameters template shall contain a security attribute template specific to physical interface in compact format.

TE3.4.1 The tester shall verify that the control parameters template contains a security attribute template specific to one or more physical interface in compact format.

AS3.5 The control parameters template shall always be retrievable using the GET DATA command referencing tag '62'. It allows the relying systems to find out all the information '62' provides.

TE3.5.1 The tester shall verify that the control parameters template is always retrievable using the GET DATA command referencing tag '62', and that it allows to find out all the information '62' provides.

AS3.6 The control parameters template (tag '62') associated with a file shall contain data objects with tags listed in GICS Part 1, Table 11; optional conditions shall be tested when present.

TE3.6.1 The tester shall verify that the control parameters template (tag '62') associated with each file contains data objects with tags listed in GICS Part 1, Table 11.

TE3.6.2 The tester shall verify that optional conditions conform to GICS Part 1, Table 11 when present.

AS3.7 The control parameters template shall contain a security attribute template specific to physical interface in compact format.

TE3.7.1 The tester shall verify that the control parameters template contains a security attribute template specific to physical interface in compact format.

- 1098 **AS3.8 The control parameters template shall always be retrievable from a file using the GET**
1099 **DATA command referencing tag '62'. It allows the relying systems to find out all the**
1100 **information '62' provides.**
1101
- 1102 TE3.8.1 The tester shall verify that the control parameters template is always retrievable from each file
1103 using the GET DATA command referencing tag '62', and that it allows the tester to find out all
1104 the information '62' provides.
1105
1106
- 1107 **AS3.9 The control parameters template (tag '62') associated with a security objects shall contain**
1108 **data objects with tags listed in GICS Part 1, Table 12; optional conditions shall be tested**
1109 **when present.**
- 1110 TE3.9.1 The tester shall verify that the control parameters template (tag '62') associated with a security
1111 objects contains data objects with tags listed in GICS Part 1, Table 12.
1112 TE3.9.2 The tester shall verify that optional conditions conform to GICS Part 1, Table 12 when present.
1113
1114
- 1115 **AS3.10 The control parameters template shall contain a security attribute template specific to**
1116 **physical interface in compact format.**
1117
- 1118 TE3.10.1 The tester shall verify that the control parameters template contains a security attribute template
1119 specific to physical interface in compact format.
1120
1121
- 1122 **AS3.11 The control parameters template shall always be retrievable from a security object DO**
1123 **using the GET DATA command referencing tag '62'. It allows the relying systems to find**
1124 **out all the information '62' provides.**
1125
- 1126 TE3.11.1 The tester shall verify that the control parameters template associated with a security object DO
1127 is always retrievable using the GET DATA command referencing tag '62'.
1128
1129
- 1130 **AS3.12 The security parameters template (tag 'AD') associated with the authentication and key**
1131 **data objects shall contain data objects with tags listed in GICS Part 1, Table 13; optional**
1132 **conditions shall be tested when present.**
- 1133 TE3.12.1 The tester shall verify that the security parameters template (tag 'AD') associated with the
1134 authentication and key data objects contains data objects with tags listed in GICS Part 1, Table
1135 13.
1136 TE3.12.2 The tester shall verify that optional conditions conform to GICS Part 1, Table 13 when present.
1137
1138
- 1139 **AS3.13 The value of verification History length shall not be greater than 8.**
- 1140 TE3.13.1 The test shall verify that the platform rejects the creation of a verification history that is larger
1141 than 8.
1142
- 1143 **AS3.14 For numeric and alphanumeric verification data, the bytes comprising the verification data**
1144 **shall be the ASCII encoded value of the verification data: '30'-'39' for digit, '41'-'5A' for**
1145 **upper case characters, and '61'-'7A' for lower case characters. Data transferred to the ICC**
1146 **shall be padded with 'FF' until maximum length characters are available. For case '00', the**
1147 **padding is not supported and the length shall be the maximum verification data length.**
- 1148 TE3.14.1 The tester shall verify that the bytes comprising the verification data are the ASCII encoded
1149 value of the verification data: '30'-'39' for digit, '41'-'5A' for upper case characters, and '61'-'7A'
1150 for lower case characters.

DRAFT Generic Identity Command Set – Part 3: GICS Platform Testing Requirements

- 1151 TE3.14.2 The tester shall verify that data transferred to the ICC is padded with 'FF' until the maximum
1152 length of characters.
1153 TE3.14.3 The tester shall verify that the length is the maximum data length in the case '00'.
1154
1155 **AS3.15 If tag '91' is absent, the retry counter is not used which means no limit on the number of**
1156 **authentication object verification tries. Tags '93' and '85' (Contactless number of tries**
1157 **threshold) under tag 'AF' shall be absent.**
1158 TE3.15.1 The tester shall verify that the retry counter is disabled when tag '91' is absent.
1159 TE3.15.2 The tester shall verify that the platform rejects the creation of tags '93' and '85' when tag '91' is
1160 absent.
1161
1162 **AS3.16 If '91' is present, tags '93' and '85' (Contactless number of tries threshold) under tag 'AF'**
1163 **shall be mandatory.**
1164 TE3.16.1 The tester shall verify that the platform rejects the creation of tag '91' if tags '93' and '85' under
1165 tag 'AF' are not present.
1166
1167 **AS3.17 There shall be no more than one CRT under Tag '7B'**
1168 TE3.17.1 The tester shall verify that the platform rejects the creation of more than one CRT under Tag
1169 '7B'.
1170
1171 **AS3.18 The file management data template (tag '64') associated with an application dedicated file**
1172 **shall contain data objects listed in GICS Part 1, Table 14; optional conditions shall be**
1173 **tested when present.**
1174
1175 TE3.18.1 The tester shall verify that the file management data template (tag '64') associated with an
1176 application dedicated file contains data objects listed in GICS Part 1, Table 14.
1177 TE3.18.2 The tester shall verify that optional conditions conform to GICS Part 1, Table 14 when present.
1178
1179
1180 **AS3.19 The file management template shall always be retrievable from a file using the GET DATA**
1181 **command referencing tag '64'.**
1182
1183 TE3.19.1 The tester shall verify that the file management template is always retrievable from a file using
1184 the GET DATA command referencing tag '64'.
1185
1186
1187 **AS3.20 Each application profile shall provide a definition of Tag '79'.**
1188 TE3.20.1 The tester shall verify that each application profile provides a definition of Tag '79' and that Tag
1189 '79' can be read.
1190
1191
1192 **AS3.21 The file descriptor byte in the control parameter template of a file shall be one of the values**
1193 **in GICS Part 1, Table 16.**
1194 TE3.21.1 The tester shall verify that the file descriptor byte in the control parameter template of a file is
1195 one of the values in GICS Part 1, Table 16.
1196
1197
1198 **AS3.22 The control parameters template shall contain exactly one life cycle status data object (tag**
1199 **'8A'). The LCS shall not be set by PUT DATA command. It shall be managed by the**
1200 **application itself and it shall be read only information.**
1201
1202 TE3.22.1 The tester shall verify that the control parameters template contains exactly one life cycle status
1203 data object (tag '8A').

DRAFT Generic Identity Command Set – Part 3: GICS Platform Testing Requirements

- 1204 TE3.22.2 The tester shall verify that the LCS is not set by PUT DATA command, and that it is managed by
1205 the application itself and it shall be read only information.
1206
- 1207 **AS3.23 The value of a life cycle status data object shall be one of the values in GICS Part 1, Table**
1208 **17. Transitions between life cycle states are defined in Part 2.**
- 1209 TE3.23.1 The tester shall verify that the value of a life cycle status data object is one of the values in GICS
1210 Part 1, Table 17.
- 1211 TE3.23.2 The tester shall verify all life cycle states of the ADF, EF, and DO.
1212
- 1213
- 1214 **AS3.24 The security environment template (tag '7B') shall contain data objects listed in GICS Part**
1215 **1, Table 18; optional conditions shall be tested when present.**
- 1216 TE3.24.1 The tester shall verify that the security environment template (tag '7B') contains data objects
1217 listed in GICS Part 1, Table 18.
- 1218 TE3.24.2 The tester shall verify that optional conditions conform to GICS Part 1, Table 18 when present.
1219
- 1220
- 1221 **AS3.25 The SEID values shall be GICS application specific and shall be defined in tag '7B' within**
1222 **the GICS application. This specification does not provide internal storage requirements for**
1223 **the SEIDs; however, security environment shall always be retrievable using the GET DATA**
1224 **command referencing tag '7B'.**
- 1225
- 1226 TE3.25.1 The tester shall verify that the SEID values are GICS-application specific
- 1227 TE3.25.2 The tester shall verify that the SEID values are defined in tag '7B' within the GICS application,
- 1228 TE3.25.3 The tester shall verify that the security environment is always retrievable using the GET DATA
1229 command referencing tag '7B'.
1230
- 1231
- 1232 **AS3.26 Security environment shall be created using PUT DATA command when the application is**
1233 **in INITIALIZATION state.**
- 1234 TE3.26.1 The tester shall verify that the security environment is created using PUT DATA command when
1235 the application is in INITIALIZATION state.
1236
- 1237
- 1238 **AS3.27 Security environment shall not be modifiable when the application is in OPERATIONAL**
1239 **ACTIVATED state.**
- 1240
- 1241 TE3.27.1 The tester shall verify that the security environment cannot be modifiable when the application is
1242 in OPERATIONAL ACTIVATED state.
1243
- 1244
- 1245 **AS3.28 The access mode byte for data objects in access rules shall be one of the values in GICS**
1246 **Part 1, Table 19.**
- 1247
- 1248 TE3.28.1 The tester shall verify that the access mode byte for data objects in access rules is one of the
1249 values in GICS Part 1, Table 19.
1250
- 1251
- 1252 **AS3.29 The access mode byte for authentication objects shall be defined in GICS Part 1, Table 20.**
1253
- 1254 TE3.29.1 The tester shall verify that the access mode byte for authentication objects is in accordance with
1255 GICS Part 1, Table 20.
1256

1257
1258 **AS3.30 The access mode byte for asymmetric key objects is defined in GICS Part 1, Table 21.**
1259

1260 TE3.30.1 The tester shall verify that the access mode byte for asymmetric key objects is in accordance
1261 with GICS Part 1, Table 21.
1262

1263
1264 **AS3.31 The access mode byte for symmetric key objects is defined in GICS Part 1, Table 22.**
1265

1266 TE3.31.1 The tester shall verify that the access mode byte for symmetric key objects is in accordance with
1267 GICS Part 1, Table 22.
1268

1269
1270 **AS3.32 GICS platform shall support all the cryptographic mechanisms listed in GICS Part 1, Table**
1271 **23, Cryptographic Mechanism Reference Values.**
1272

1273 TE3.32.1 The tester shall verify that the GICS platform supports all the cryptographic mechanisms listed in
1274 GICS Part 1, Table 23, Cryptographic Mechanism Reference Values.
1275

1276
1277 **AS3.33 Additionally, all GICS platforms shall support partial on-card hashing, full on-card hashing,**
1278 **and off-card hashing.**
1279

1280 TE3.33.1 Tester shall verify that each algorithm listed in GICS Part 1, Table 30 is supported by full on-
1281 card, partial on-card, and off-card hashing in accordance with GICS Part 1, Section 8.1.
1282

1283
1284 **AS3.34 The GICS card shall default to '3 Key Triple DES – ECB' algorithm when the P1 value in the**
1285 **command APDU is set to '00'.**

1286 TE3.34.1 The tester shall verify that the GICS card defaults to '3 Key Triple DES – ECB' algorithm when
1287 the P1 value in the command APDU is set to '00'.
1288

1289 **AS3.35 If a GICS application uses any of the cryptographic mechanisms in GICS Part 1, Table 23,**
1290 **the control parameters of an ADF for a GICS application shall use cryptographic**
1291 **mechanism identifier template (tag 'AC') to indicate which cryptographic mechanisms are**
1292 **used from GICS Part 1, Table 23.**
1293

1294 TE3.35.1 The tester shall verify that if a GICS application uses any of the cryptographic mechanisms in
1295 GICS Part 1, Table 23, that the control parameters of an ADF for a GICS application uses
1296 cryptographic mechanism identifier template (tag 'AC') to indicate which cryptographic
1297 mechanisms are used from GICS Part 1, Table 23.
1298

1299
1300 **AS3.36 A reference data qualifier shall name a reference data value (e.g. PIN, password or**
1301 **cryptographic key) to be used in an authentication protocol.**

1302 TE3.36.1 The tester shall verify that each reference data qualifier name a reference data value (e.g. PIN,
1303 password or cryptographic key) to be used in an authentication protocol.
1304

1305
1306 **AS3.37 For VERIFY, CHANGE REFERENCE DATA, RESET RETRY COUNTER APDUs, '00' means**
1307 **Global PIN. For GENERAL AUTHENTICATE, PERFORM SECURITY OPERATIONS, MANAGE**
1308 **SECURITY ENVIRONMENT APDUs, '00' means '3 key triple DES'.**

DRAFT Generic Identity Command Set – Part 3: GICS Platform Testing Requirements

- 1309 TE3.37.1 Tester shall verify that '00' means 'Global PIN' for the VERIFY, CHANGE REFERENCE DATA,
1310 and RESET RETRY COUNTER APDUs.
1311 TE3.37.2 Tester shall verify that '00' means '3 key triple DES' for GENERAL AUTHENTICATE,
1312 PERFORM SECURITY OPERATIONS, and MANAGE SECURITY ENVIRONMENT APDUs.
1313
1314
1315 **AS3.38 The structure of a Control Reference Template is defined in ISO/IEC 7816-4 Table 55. The**
1316 **GICS shall contain only templates with tags listed in GICS Part 1, Table 26.**
1317
1318 TE3.38.1 The tester shall verify that the structure of each CRT confirms to ISO/IEC 7816-4, Table 55.
1319 TE3.38.2 The tester shall verify that the CRT DO uses tags listed in GICS Part 1, Table 26.
1320
1321
1322 **AS3.39 The control reference templates in GICS Part 1, Table 26 shall contain only data objects**
1323 **listed in GICS Part 1, Table 27 or Table 28.**
1324 TE3.39.1 The tester shall verify that the control reference templates in GICS Part 1, Table 26 contain only
1325 data objects listed in GICS Part 1, Table 27 or Table 28.
1326
1327
1328 **AS3.40 Tag '84' in GICS Part 1, Table 27, Link to the security object number of a key security**
1329 **object, is used to indicate linkage between the keys if the key belongs to a key set. GICS**
1330 **general authenticate command shall reference the MAC static key. In the CP of the MAC**
1331 **key security object, there shall be a tag '84' that references ENC key. In the CP of the ENC**
1332 **key security object, there shall be a tag '84' that references KEK key. In the CP of the KEK**
1333 **key security object, there shall be a tag '84' with value '00 00'. There shall be three keys.**
1334 **They should be managed independently of the other keys. Figure 2, Key Set Organization**
1335 **shows the relationship between keys in a key set.**
1336
1337 TE3.40.1 The tester shall verify that the GICS general authenticate command references the MAC static
1338 key.
1339 TE3.40.2 The tester shall verify that the CP of the MAC key security object contains a tag '84' that
1340 references ENC key.
1341 TE3.40.3 The tester shall verify that the CP of the ENC key security object contains a tag '84' that
1342 references KEK key.
1343 TE3.40.4 The tester shall verify that the CP of the KEK key security object contains a tag '84' with value
1344 '00 00'.
1345 TE3.40.5 The tester shall verify that there are three keys and that they are managed independently of
1346 each other.
1347
1348
1349 **AS3.41 GICS Part 1, Table 23 defines the cryptographic mechanism references for an AT CRT.**
1350 **Note that reference values from '00' to '2E' can only be used for authentication.**
1351
1352 TE3.41.1 The tester shall verify that only values from '00' to '2E' are used only for authentication.
1353
1354 **AS3.42 GICS Part 1, Table 23 defines the cryptographic mechanism references for KAT CRT. Only**
1355 **the reference values from '20' to '2E' of GICS Part 1, Table 23 are applicable with KAT CRT.**
1356 **Also, note that the key establishment protocols in GICS Part 1, Table 23 must be**
1357 **implemented as specified in Clause 8.**
1358
1359 TE3.42.1 The tester shall verify that only the reference values from '20' to '2E' of GICS Part 1, Table 23
1360 are used with KAT CRT.

DRAFT Generic Identity Command Set – Part 3: GICS Platform Testing Requirements

TE3.42.2 The tester shall verify that the key establishment protocols in GICS Part 1, Table 23 must be implemented as specified in Section 8.

AS3.43 GICS Part 1 defines a one to one relationship between the hash and cryptographic algorithms provided in Table 30. The hash algorithm shall correspond to the cryptographic algorithm as mapped in Table 30. Table 30 defines the cryptographic mechanism references for an HT CRT.

TE3.43.1 The tester shall verify that for each cryptographic algorithm is used with the corresponding hash algorithm according GICS Part 1, Table 30.

AS3.44 DST CRT must be defined by GICS Part 1, Table 31.

TE3.44.1 The tester shall verify that DST CRT are defined by GICS Part 1, Table 31.

AS3.45 CT CRT are defined by GICS Part 1, Tables 33 and 34.

TE3.45.1 The tester shall verify that CT CRT are defined by GICS Part 1, Tables 33 and 34.

AS3.46 Only data objects with tags listed in GICS Part 1, Table 35 shall be used to construct data objects in a data field in secure message format.

TE3.46.1 The tester shall verify that only the data objects with tags listed in GICS Part 1, Table 35 are used to construct data objects in a data field in secure message format.

AS3.47 In each secure message field, bit 1 of the last byte of the tag field (tag parity) of each secure message data object indicates whether the secure message data object shall be included (bit 1 set to 1, odd tag number) or shall not be included (bit 1 set to 0, even tag number) in the computation of a data element for authentication (tag '8E' or tag '9E').

TE3.47.1 The tester shall verify that the platform includes the secure message data object in the computation of a data element for authentication when bit one is set to 1.

TE3.47.2 The tester shall verify that the platform does not include the secure message data object in the computation of a data element for authentication when bit one is set to 0.

AS3.48 The padding-content indicator byte used in secure message cryptogram data objects (tag '86') shall be one of the values listed in GICS Part 1, Table 36.

TE3.48.1 The tester shall verify that the padding-content indicator byte used in secure message cryptogram data objects (tag '86') is one of the values listed in GICS Part 1, Table 36.

AS3.49 The PIN Usage policy consists of two bytes. The first byte of a PIN usage policy data object (tag '5F2F') shall be one of the values listed in GICS Part 1, Table 37. The second byte of the PIN Usage Policy encode shall be encoded as described in GICS Part 1, Table 38. The values of all undefined bits shall be set to zero and are reserved for future use.

TE3.49.1 The tester shall verify that the PIN Usage policy consists of two bytes.

TE3.49.2 The tester shall verify that the first byte of a PIN usage policy data object (tag '5F2F') is one of the values listed in GICS Part 1, Table 37.

TE3.49.3 The tester shall verify that the second byte of the PIN Usage Policy encode shall be encoded as described in GICS Part 1, Table 38.

1414 TE3.49.4 The tester shall verify that the values of all undefined bits are set to zero and are reserved for
1415 future use.

1416 **4.4 Generic Identity Command Set – Application**

1417 **4.4.1 SELECT**

1418
1419 **AS4.1** Upon successful selection of an application dedicated file (P1='04') other than the
1420 currently selected card-application, all security states of the previously selected
1421 application shall be set to FALSE. Otherwise, there shall be no change in the current
1422 security status upon the execution of the SELECT command. Also, the Global security
1423 status shall not change.
1424

1425 TE4.1.1 The tester shall verify that all security states of the previously selected application are set to
1426 FALSE upon successful selection of an application dedicated file (P1='04') other than the
1427 currently selected card-application. Otherwise, the tester shall verify that there are no changes
1428 in the current security status upon the execution of the SELECT command.

1429 TE4.1.2 The tester shall verify that the Global security status does not change.
1430

1431
1432 **AS4.2** The SELECT by File Identifier command allows to select a given Elementary file to be
1433 selected in the existing file hierarchy of the currently selected card-application.
1434

1435 TE4.2.1 The tester shall verify that a given elementary file is selected by the SELECT by File Identifier
1436 command.
1437

1438 **AS4.3** In order to unambiguously select any file by its identifier, all EFs immediately under a
1439 given ADF shall have different file identifiers.
1440

1441 TE4.3.1 The tester shall verify that the all EFs immediately under a given ADF have different file
1442 identifiers through use of the CREATE FILE command referenced by TE6.17.1.
1443
1444

1445 **AS4.4** After a successful execution of the command, the selection of an EF sets a pair of current
1446 files: the EF as the currently selected EF and its parent as the currently Selected ADF.
1447

1448 TE4.4.1 The tester shall verify that after successful execution of the command, the selection of an EF
1449 sets a pair of current files: the EF as the currently selected EF and its parent as the currently
1450 Selected ADF.
1451
1452

1453 **AS4.5** If $L_c = 2$ then the command data field shall be a two-byte file identifier that is unique in any
1454 of the files contained in the currently selected ADF.
1455

1456 TE4.5.1 The tester shall verify that if $L_c = 2$ then the command data field is a two-byte file identifier that is
1457 unique in any of the files contained in the currently selected ADF.
1458
1459

1460 **AS4.6** If the command data field contains the value '3FFF' as the file identifier, it indicates the
1461 command has to return the information requested by P2 related to the currently selected
1462 ADF. No change in security status or currently selected files (ADF or EF) occurs.
1463

DRAFT Generic Identity Command Set – Part 3: GICS Platform Testing Requirements

- 1464 TE4.6.1 The tester shall verify that no change in security status or currently selected files (ADF or EF)
1465 occurs if the command data field contains the value '3FFF' as the file identifier.
1466
1467
- 1468 **AS4.7 If the command data field contains the value '0000' as the file identifier, it indicates the**
1469 **command has to return the information requested by P2 related to the currently selected**
1470 **Elementary File. No change in security status or currently selected files (ADF or EF)**
1471 **occurs.**
1472
- 1473 TE4.7.1 The tester shall verify that no change in the security status or currently selected files (ADF or
1474 EF) occurs if the command data field contains the value '0000' as the file identifier.
1475
1476
- 1477 **AS4.8 If P2 is '00', then the response field shall be the APT template (tag '61').**
1478
- 1479 TE4.8.1 The tester shall verify that if P2 is '00', then the response field is the APT template (tag '61').
1480 **AS4.9 If P2 is '04', then the response data field shall be the control parameters template (tag '62')**
1481 **associated with the selected file**
1482
- 1483 TE4.9.1 The tester shall verify that if P2 is '04', then the response data is the control parameters
1484 template (tag '62') associated with the selected file
1485
1486
- 1487 **AS4.10 If P2 is '08', then the response data field shall be the file management data template (tag**
1488 **'64') associated with the selected file.**
1489
- 1490 TE4.10.1 The tester shall verify that if P2 is '08', then the response data field is the file management data
1491 template (tag '64') associated with the selected file.
1492
1493
- 1494 **AS4.11 If P2 is '0C', then the response data field shall be absent.**
1495
- 1496 TE4.11.1 The tester shall verify that if P2 is '0C', then the response data field shall be absent.
1497
1498
- 1499 **AS4.12 If the status word is other than successful execution ('90 00'), then neither the currently**
1500 **selected dedicated file nor the currently selected elementary file shall change.**
1501
- 1502 TE4.12.1 The tester shall verify that if the status word is other than successful execution ('90 00'), then
1503 neither the currently selected dedicated file nor the currently selected elementary file change.
1504
1505
- 1506 **AS4.13 The SELECT Card-application By Name command sets the currently selected Application**
1507 **dedicated File. The command data field shall be an application identifier of one or more**
1508 **bytes selecting an application dedicated file**
1509
- 1510 TE4.13.1 Tester shall verify that an application can be selected with an application identifier of one or
1511 more bytes.
1512
1513
- 1514 **AS4.14 Successful execution shall set the currently selected card-application and the currently**
1515 **selected dedicated file to the named application dedicated file. In this case, the currently**
1516 **selected elementary file shall be undefined.**

- 1517
1518 TE4.14.1 The tester shall verify that successful execution sets the currently selected card-application and
1519 the currently selected dedicated file to the named application dedicated file.
1520 TE4.14.2 In this case, the tester shall verify that the currently selected elementary file is undefined.
1521
1522
1523 **AS4.15 If P2 is '00', then the response field shall be the APT template (tag '61').**
1524
1525 TE4.15.1 The tester shall verify that if P2 is '00', then the response field is the APT template (tag '61').
1526
1527
1528 **AS4.16 If P2 is '04', then the response data field shall be the control parameters template (tag '62')**
1529 **associated with the selected Application dedicated file.**
1530
1531 TE4.16.1 The tester shall verify that if P2 is '04', then the response data field is the control parameters
1532 template (tag '62') associated with the selected Application dedicated file.
1533 **AS4.17 If P2 is '08', then the response data field shall be the file management data template (tag**
1534 **'64') associated with the selected Application dedicated file.**
1535
1536 TE4.17.1 The tester shall verify that if P2 is '08', then the response data field is the file management data
1537 template (tag '64') associated with the selected Application dedicated file.
1538
1539
1540 **AS4.18 If P2 is '0C', then the response data field shall be absent.**
1541
1542 TE4.18.1 The tester shall verify that if P2 is '0C', then the response data field shall be absent.
1543
1544
1545 **AS4.19 The status word returned by the SELECT by-file-identifier shall be one of the status words**
1546 **defined in GICS Part 1, Table 41.**
1547
1548 TE4.19.1 The tester shall verify that the status word returned by the SELECT by-file-identifier are one of
1549 the status words defined in GICS Part 1, Table 41.
1550
1551 **AS4.20 The status word returned by the SELECT card-application-by-name command shall be one**
1552 **of the status words in GICS Part 1, Table 44.**
1553
1554 TE4.20.1 The tester shall verify that the status word returned by the SELECT command is one of the
1555 status words in GICS Part 1, Table 44.
1556
1557
1558 **AS4.21 If the status word is other than successful execution ('90 00'), then the security status**
1559 **remain unchanged.**
1560
1561 TE4.21.1 The tester shall verify that the security status remains unchanged if the status word is other than
1562 successful execution ('90 00').
1563
1564

4.4.2 SELECT DATA

AS4.22 There shall be no change in the current security status upon the execution of the SELECT DATA command.

TE4.22.1 The tester shall verify that there is no change in the current security status upon the execution of the SELECT DATA command.

AS4.23 The select data command sets a unique selected DO, i.e. the target of the command, as current DO. The five functional encodings listed in GICS Part 1, Table 46, are supported.

TE4.23.1 The tester shall verify that P2 encoding for the first occurrence of a DO using a SELECT DATA command is as specified by GICS Part 1, Table 46.

TE4.23.2 The tester shall verify that P2 encoding for the last occurrence of a DO using a SELECT DATA command is as specified by GICS Part 1, Table 46.

TE4.23.3 The tester shall verify that P2 encoding for the next occurrence of a DO using a SELECT DATA command is as specified by GICS Part 1, Table 46.

TE4.23.4 The tester shall verify that P2 encoding for the previous occurrence of a DO using a SELECT DATA command is as specified by GICS Part 1, Table 46.

TE4.23.5 The tester shall verify that P2 encoding for the return of data control information (DO '62') using a SELECT DATA command is as specified by GICS Part 1, Table 46.

AS4.24 The status word returned by the SELECT DATA command shall be one of the status words in GICS Part 1, Table 47.

TE4.24.1 The tester shall verify that all the status words listed in GICS Part 1, Table 47 are returned appropriately.

4.4.3 GET DATA

AS4.25 The GET DATA command shall execute successfully with respect to any data object only if the security condition associated with the GET DATA access mode in the security attribute associated with the data object evaluates to TRUE with respect to the current security status.

TE4.25.1 The tester shall verify that the GET DATA command executes successfully with respect to any data object only if the security condition associated with the GET DATA access mode in the security attribute associated with the data object evaluates to TRUE with respect to the current security status.

AS4.26 There shall be no change in the current security status upon the execution of the GET DATA command.

TE4.26.1 The tester shall verify that there is no change in the current security status upon the execution of the GET DATA command.

AS4.27 P1-P2 shall be the file identifier of a file in the currently selected dedicated file or '3F FF' indicating the currently selected dedicated file or '00 00' indicating the currently selected elementary file. In the case that P1-P2 contains the file identifier of an elementary file in the currently selected dedicated file, that file shall become the currently selected elementary

- 1619 **file. In the case that P1-P2 contains '3F FF', the currently selected dedicated file shall be**
1620 **unchanged and the currently selected elementary file shall be unchanged.**
1621
- 1622 TE4.27.1 The tester shall verify that P1-P2 is the file identifier of a file in the currently selected dedicated
1623 file or '3F FF' indicating the currently selected dedicated file or '00 00' indicating the currently
1624 selected elementary file.
1625 TE4.27.2 The tester shall verify that in the case that P1-P2 contains the file identifier of an elementary file
1626 in the currently selected dedicated file, that file becomes the currently selected elementary file.
1627 TE4.27.3 The tester shall verify that in the case that P1-P2 contains '3F FF', the currently selected
1628 dedicated file is unchanged and the currently selected elementary file is unchanged.
1629
1630
- 1631 **AS4.28 Data objects shall be retrieved according to the addressing span defined by the file**
1632 **identifier indicated in P1-P2. In particular, in the case that P1-P2 is '3F FF' indicating**
1633 **retrieval from the currently selected dedicated file, data objects shall be retrieved from the**
1634 **currently selected dedicated file itself or from any elementary file contained in the**
1635 **currently selected dedicated file as long as the access conditions on the file and file type**
1636 **requirements are fulfilled.**
1637
- 1638 TE4.28.1 The tester shall verify that data objects are retrieved according to the addressing span defined
1639 by the file identifier indicated in P1-P2. In particular, in the case that P1-P2 is '3F FF' indicating
1640 retrieval from the currently selected dedicated file, the tester shall verify that data objects are
1641 retrieved from the currently selected dedicated file itself or from any elementary file contained in
1642 the currently selected dedicated file as long as the access conditions on the file and file type
1643 requirements are fulfilled.
1644
1645
- 1646 **AS4.29 The command data field of a GET DATA command shall not request multiple data objects**
1647 **stored in different file types (e.g. type '39' and type '31'). Such a command shall be rejected**
1648 **indicating "Incorrect parameters in the command data field" ('6A 80').**
1649
- 1650 TE4.29.1 The tester shall verify that the command data field of a GET DATA command does not request
1651 multiple data objects stored in different file types (e.g. type '39' and type '31').
1652 TE4.29.2 The tester shall verify that such a command is rejected indicating "Incorrect parameters in the
1653 command data field" ('6A 80').
1654
1655
- 1656 **AS4.30 It is not allowed to request more than one data object in the command data field of the GET**
1657 **DATA command when P1-P2 references directly a file type '31' or when such a data object**
1658 **is stored in a file type '31'. Such a command shall be rejected indicating "Incorrect**
1659 **parameters in the command data field" ('6A 80').**
1660
- 1661 TE4.30.1 The tester shall verify that a request of more than one data object in the command data field of
1662 the GET DATA command when P1-P2 references directly a file type '31', or when such data
1663 object is stored in a file type '31', is rejected indicating "Incorrect parameters in the command
1664 data field" ('6A 80').
1665
1666
- 1667 **AS4.31 It is not allowed to use extended header list data object (tag '4D') in command data field**
1668 **when P1-P2 references file type '31'. Such a command shall be rejected indicating**
1669 **"Command incompatible with file structure" ('69 81').**
1670

DRAFT Generic Identity Command Set – Part 3: GICS Platform Testing Requirements

- 1671 TE4.31.1 The tester shall verify that a command to use extended header list data object (tag '4D') in
1672 command data field when P1-P2 references file type '31' is rejected indicating "Command
1673 incompatible with file structure" ('69 81').
1674
1675
- 1676 **AS4.32 If none of the requested data objects indicated by either P1-P2 or by the command data**
1677 **field are found, the return status shall be '6A 82'.**
1678
- 1679 TE4.32.1 The tester shall verify that if none of the requested data objects are found the return status is '6A
1680 82'.
1681
1682
- 1683 **AS4.33 If none of the requested data objects has fulfilled the necessary security requirements, the**
1684 **return status shall be '69 82'.**
1685
- 1686 TE4.33.1 The tester shall verify that if none of the requested data objects has fulfilled the necessary
1687 security requirements, the return status is '69 82'.
1688 **AS4.34 The command data field shall contain exactly one of the following data objects: a tag list**
1689 **data object (tag '5C') or an extended header list data object (tag '4D').**
1690
- 1691 TE4.34.1 The tester shall verify that the command data field contains exactly one of the following data
1692 objects: a tag list data object (tag '5C') or an extended header list data object (tag '4D').
1693
- 1694 **AS4.35 If the data object is found in a file type '31', the response data field is a discretionary data**
1695 **object: tag '53' followed by the length followed by the value of the data object. If the data**
1696 **object(s) are in a file type '39', the response data field shall be the concatenation of the**
1697 **data objects requested if found.**
1698
- 1699 TE4.35.1 The tester shall verify that if the data object is found in a file type '31', the response data field is
1700 a discretionary data object: tag '53' followed by the length followed by the value of the data
1701 object.
1702 TE4.35.2 The tester shall verify that if the data object(s) are in a file type '39', the response data field is
1703 the concatenation of the data objects requested if found.
1704
1705
- 1706 **AS4.36 When multiple data objects are requested, they all should belong to the same EF or ADF.**
1707 **When one or more of such data object are not found, then the corresponding part of the**
1708 **response data field shall be absent. This circumstance shall not impact the status word**
1709 **associated with the response should the status word otherwise indicate successful**
1710 **execution ('90 00').**
1711
- 1712 TE4.36.1 The tester shall verify that when multiple data objects are requested that they all belong to the
1713 same EF or ADF.
1714 TE4.36.2 The tester shall verify that when one or more of such data objects are not found, then the
1715 corresponding part of the response data field are absent.
1716 TE4.36.3 The tester shall verify that this circumstance does not impact the status word associated with the
1717 response should the status word otherwise indicate successful execution ('90 00').
1718
1719
- 1720 **AS4.37 An empty tag list (tag '5C 00') shall return all the information in the file referenced in P1-P2.**
1721 **An empty tag list requires all the available data objects. When several data objects within**
1722 **the template have the same tag, all those data objects shall be returned. One or more data**
1723 **objects may be absent, if a conditional argument is present, or for security status reasons.**

- 1724
1725 TE4.37.1 The tester shall verify that an empty tag list (tag '5C 00') returns all the information in the file
1726 referenced in P1-P2. An empty tag list requires all the available data objects.
1727 TE4.37.2 The tester shall verify that when several data objects within the template have the same tag, all
1728 those data objects are returned. One or more data objects may be absent, if a conditional
1729 argument is present, or for security status reasons.
1730
1731
1732 **AS4.38 In the tag list and extended header list cases, the response data field shall be the**
1733 **concatenation of the data objects derived from the extended header list according to**
1734 **Section 8.4.5 of ISO/IEC 7816-4.**
1735
1736 TE4.38.1 The tester shall verify that, in the tag list and extended header list cases, the response data field
1737 is the concatenation of the data objects derived from the extended header list according to
1738 Section 8.4.5 of ISO/IEC 7816-4.
1739
1740 **AS4.39 The status word returned by the GET DATA command shall be one of the status words in**
1741 **GICS Part 1, Table 49.**
1742
1743 TE4.39.1 The tester shall verify that all the status words listed in GICS Part 1, Table 49 are returned
1744 appropriately.
1745
1746

1747 **4.4.4 PUT DATA**

- 1748
1749 **AS4.40 The PUT DATA command shall execute successfully with respect to a data object only if**
1750 **the security condition associated with the PUT DATA access mode in the security attribute**
1751 **of the data object evaluates to TRUE with respect to the current security status.**
1752
1753 TE4.40.1 The tester shall verify that the PUT DATA command executes successfully with respect to a
1754 data object only if the security condition associated with the PUT DATA access mode in the
1755 security attribute of the data object evaluates to TRUE with respect to the current security
1756 status.
1757
1758
1759 **AS4.41 When the PUT DATA command is used with a parameter P1-P2 = '3F FF' for a data object**
1760 **which does not exist anywhere in the currently selected DF or in any of the elementary**
1761 **files under this DF, the data object will be created in the DF itself.**
1762
1763 TE4.41.1 The tester shall verify that when the PUT DATA command is used with a parameter P1-P2 = '3F
1764 FF' for a data object which does not exist anywhere in the currently selected DF or in any of the
1765 elementary files under this DF, the data object is created in the DF itself.
1766
1767
1768 **AS4.42 If the object life cycle status is used to temporarily deactivate an object, then the LCS shall**
1769 **be set to deactivate and the LCS shall be restored at the end of the chaining.**
1770
1771 TE4.42.1 The tester shall verify if the object life cycle is used to temporarily deactivate an object that the
1772 LCS is set to deactivate and the LCS is restored at the end of the chaining.
1773
1774

- 1775 **AS4.43 With an exception of PIN object, every incomplete update will result in either zeroization of**
1776 **key, deletion of the data object content, unchanged content, or deactivation of the file.**
1777
- 1778 TE4.43.1 The tester shall verify that, with the exception of a PIN object, every incomplete update will
1779 result in either zeroization of key, deletion of the data object content, deactivation of the file, or
1780 preservation of the prior content of the object.
1781
1782
- 1783 **AS4.44 There shall be no change in the current security status upon the execution of the PUT**
1784 **DATA command.**
1785
- 1786 TE4.44.1 The tester shall verify that there is no change in the current security status upon the execution of
1787 the PUT DATA command.
1788
1789
- 1790 **AS4.45 P1-P2 shall be the file identifier of a file in the currently selected dedicated file or '3F FF'**
1791 **indicating the currently selected dedicated file or '00 00' indicating the currently selected**
1792 **elementary file. In the case that P1-P2 contains the file identifier of an elementary file in the**
1793 **currently selected dedicated file, that file shall become the currently selected elementary**
1794 **file.**
1795
- 1796 TE4.45.1 The tester shall verify that P1-P2 is the file identifier of a file in the currently selected dedicated
1797 file or '3F FF' indicating the currently selected dedicated file or '00 00' indicating the currently
1798 selected elementary file.
1799 TE4.45.2 The tester shall verify that in the case that P1-P2 contains the file identifier of an elementary file
1800 in the currently selected dedicated file, that file becomes the currently selected elementary file.
1801
1802
- 1803 **AS4.46 For elementary files type '39', or dedicated files, the data field of the PUT DATA command**
1804 **shall consist of the concatenation of the various data objects (Tag-Length-Value) to add or**
1805 **alter in that file.**
1806
- 1807 TE4.46.1 The tester shall verify that for elementary files type '39', or dedicated files, the data field of the
1808 PUT DATA command consists of the concatenation of the various data objects (Tag-Length-
1809 Value) to add or alter in that file.
1810
1811
- 1812 **AS4.47 For elementary files type '31' the data field of the PUT DATA command shall consist of the**
1813 **following: 1) Tag '5C' followed by the tag of the data object to create/modify; and 2) Tag**
1814 **'53' followed by the length and value of the data object to create / modify.**
1815
- 1816 TE4.47.1 The tester shall verify that for elementary files type '31' the data field of the PUT DATA
1817 command consists of the following: 1) Tag '5C' followed by the tag of the data object to
1818 create/modify; and 2) Tag '53' followed by the length and value of the data object to create /
1819 modify.
1820
1821
- 1822 **AS4.48 It is not allowed to include multiple data objects in command data field when P1-P2**
1823 **references file type '31'. Such a command shall be rejected indicating "Command**
1824 **incompatible with file structure" ('69 81').**
1825

DRAFT Generic Identity Command Set – Part 3: GICS Platform Testing Requirements

- TE4.48.1 The tester shall verify that a command to include multiple data objects in command data field when P1-P2 references file type '31' is rejected indicating "Command incompatible with file structure" ('69 81').
- AS4.49 The command data in PUT DATA may be a tag with no value. If the data object does not exist, a data object with empty value is created. If the data object exists, it shall be deleted. In other words, an existing data object can be deleted by issuing a PUT DATA of that data object with no value, i.e., with an object BER-TLV length set to zero.**
- TE4.49.1 The tester shall verify that if the data object does not exist, a data object with empty value is created.
- TE4.49.2 The tester shall verify that if the data object exists, it is deleted.
- AS4.50 A PUT DATA command with P1-P2 = '3F FF' shall replace the content of the data object(s) found with the content specified in the command data field.**
- TE4.50.1 The tester shall verify that a PUT DATA command with P1-P2 = '3F FF' replaces the content of the data object(s) found with the content specified in the command data field.
- AS4.51 A PUT DATA with a command data field of '5C 00' shall erase the entire content of the file indicated by P1-P2. If P1-P2 = '3F FF' and command data field is '5C 00', the PUT DATA command shall be rejected with the status word '6A 80'. If P1-P2 = '00 00', the current elementary file will be erased assuming the access conditions for this file for PUT DATA command is satisfied.**
- TE4.51.1 The tester shall verify that a PUT DATA with a command data field of '5C 00' erases the entire content of the file indicated by P1-P2.
- TE4.51.2 The tester shall verify that if P1-P2 = '3F FF' and command data field is '5C 00', the PUT DATA command is rejected with the status word '6A 80'.
- TE4.51.3 The tester shall verify that if P1-P2 = '00 00', the current elementary file is erased assuming the access conditions for this file for PUT DATA command is satisfied.
- AS4.52 If the PUT DATA security condition associated with any one data object to be added, altered or deleted by the command is not satisfied, then the PUT DATA command shall cause no change to the content of the file indicated in the command and the status word '69 82' shall be returned.**
- TE4.52.1 The tester shall verify that if the PUT DATA security condition associated with any one data object to be added, altered or deleted by the command is not satisfied, then the PUT DATA command causes no change to the content of the file indicated in the command and the status word '69 82' is returned.
- AS4.53 In a PUT DATA command with P1-P2 = '3F FF', mixing data objects for different files is not allowed. Such a command shall be rejected indicating "Incorrect parameters in the command data field" ('6A 80').**
- TE4.53.1 The tester shall verify that a PUT DATA command with P1-P2 = '3F FF' is rejected indicating "Incorrect parameters in the command data field" ('6A 80').
- AS4.54 The response data field of a PUT DATA command shall be empty.**

TE4.54.1 The tester shall verify that the response data field of a PUT DATA command is empty if no secure messaging applies.

AS4.55 The status word returned by the PUT DATA command shall be one of the status words in GICS Part 1, Table 51.

TE4.55.1 The tester shall verify that all the status words listed in GICS Part 1, Table 51 are returned appropriately

4.4.5 VERIFY

AS4.56 Execution of the VERIFY command shall be initiated only if the value of the retry counter associated with the reference data is greater than zero. If the comparison is successful, then 1) the security state associated with the reference data shall be set to TRUE, 2) the value of the retry counter associated with the reference data shall be set to its initial value.

TE4.56.1 The tester shall verify that execution of the VERIFY command is initiated only if the value of the retry counter associated with the reference data is greater than zero.

TE4.56.2 The tester shall verify that if the comparison is successful that the security state associated with the reference data is set to TRUE.

TE4.56.3 The tester shall further verify that if the comparison is successful, that the value of the retry counter associated with the reference data is also set to its initial value.

AS4.57 If the comparison is unsuccessful, then 1) the security state associated with the reference data shall be set to FALSE, 2) the value of the retry counter associated with the reference data shall be decremented by one.

TE4.57.1 The tester shall verify that if the comparison is unsuccessful, that the security state associated with the reference data is set to FALSE.

TE4.57.2 The tester shall further verify that if the comparison is unsuccessful, that the value of the retry counter associated with the reference data is also decremented by one.

AS4.58 With both INS values, P1='FF' shall be used only with L_c and command data field absent. The command shall set the verification status of the relevant reference data to "not verified".

TE4.58.1 The tester shall verify that, with both INS values, P1='FF' is used only with L_c and command data field absent.

TE4.58.2 The tester shall verify that the command sets the verification status of the relevant reference data to "not verified".

AS4.59 For INS '20', the absence of command data field is used to check whether the verification is required (SW1-SW2 = '63CX' where 'X' encodes the number of further allowed retries), or not (SW1-SW2 = '9000').

- 1929 TE4.59.1 The tester shall verify that if the command data field is absent, then the status word is '63 CX'
1930 where 'X' is the number of remaining retries on the reference data indicated by the reference
1931 data qualifier value.
1932 TE4.59.2 The tester shall verify that the retry counter is not decremented when the data field is absent.
1933
1934
1935 **AS4.60 If command data is present, then the command data field shall contain the verification data**
1936 **to be compared with the value of the reference data indicated by the reference data**
1937 **qualifier.**
1938
1939 TE4.60.1 The tester shall verify that, if present, the command data field contains the verification data to be
1940 compared with the value of the reference data indicated by the reference data qualifier.
1941
1942
1943 **AS4.61 The security status shall be modified as a result of a comparison. The card shall**
1944 **decrement the counter by 1 for each unsuccessful comparison.**
1945 TE4.61.1 The tester shall verify that the card decrements the retry counter by 1 for each unsuccessful
1946 comparison.
1947
1948 **AS4.62 If the actual PIN length is less than maximum length defined in authentication CRT, the PIN**
1949 **value shall be padded in accordance with GICS Part 1, Table 13.**
1950
1951 TE4.62.1 The tester shall verify that if the actual PIN length is less than maximum length defined in
1952 authentication CRT, the PIN value is padded in accordance with GICS Part 1, Table 13.
1953
1954
1955 **AS4.63 If INS is '21', then the command data field shall contain one and only one of three data**
1956 **objects listed in GICS Part 1, Table 53. If INS is '21' and the first byte of the command data**
1957 **field is '4D' and the verification object is empty, then the verification data shall come from**
1958 **a secure sensor directly linked to the card.**
1959
1960 TE4.63.1 This test is only applicable when a secure sensor is directly linked to the card. If a secure sensor
1961 is directly linked to the card, then the tester shall verify that if INS is '21,' and the first byte of the
1962 command data field is '4D,' and the verification object is empty, then the verification data comes
1963 from a secure sensor directly linked to the card.
1964
1965
1966 **AS4.64 The response data field of the VERIFY command shall be empty.**
1967
1968 TE4.64.1 The tester shall verify that the response data field of the VERIFY command is be empty.
1969
1970
1971 **AS4.65 The status word returned by the VERIFY command shall be one of the status words in**
1972 **GICS Part 1, Table 54.**
1973
1974 TE4.65.1 The tester shall verify that the status word returned by the VERIFY command is one of the
1975 status words in GICS Part 1, Table 54.
1976

1977 **4.4.6 CHANGE REFERENCE DATA**
1978

- 1979 **AS4.66 Execution of the CHANGE REFERENCE DATA command shall be initiated only if the value**
1980 **of the retry counter associated with the reference data is greater than zero.**
1981
- 1982 TE4.66.1 The tester shall verify that execution of the CHANGE REFERENCE DATA command is initiated
1983 only if the value of the retry counter associated with the reference data is greater than zero.
1984
- 1985 **AS4.67 If the comparison is successful, then 1) the security state associated with the reference**
1986 **data shall be set to TRUE, 2) the value of the retry counter associated with the reference**
1987 **data shall be set to its reset value and 3) the reference data in the command data field shall**
1988 **replace the reference data associated with the given reference data qualifier value.**
1989
- 1990 TE4.67.1 The tester shall verify that, if the comparison is successful, that the security state associated
1991 with the reference data is set to TRUE.
1992
- 1993 TE4.67.2 The tester shall verify that, if the comparison is successful, that the value of the retry counter
1994 associated with the reference data is also set to its reset value.
1995
- 1996 TE4.67.3 The tester shall verify that, if the comparison is successful, that the reference data in the
1997 command data field also replaces the reference data associated with the given reference data
1998 qualifier value.
1999
- 2000 **AS4.68 If the reference data qualifier is for PIN Authentication data object and PIN history is**
2001 **defined, the new reference data should be compared to the PINs from the PIN history list**
2002 **and if the same, the function fails. If successful and PIN history is defined, the new**
2003 **reference data should be recorded in the PIN history list.**
2004
- 2005 TE4.68.1 The tester shall verify that if the reference data qualifier is for PIN Authentication data object and
2006 PIN history is defined, the new reference data is compared to the PINs from the PIN history list
2007 and if the same, the function fails.
2008
- 2009 TE4.68.2 The tester shall verify that if successful and PIN history is defined, the new reference data is
2010 recorded in the PIN history list.
2011
- 2012 **AS4.69 If the comparison is unsuccessful, then the security state associated with the reference**
2013 **data shall be set to FALSE and the value of the retry counter associated with the reference**
2014 **data shall be decremented by one.**
- 2015 TE4.69.1 The tester shall verify that if the comparison is unsuccessful, then the security state associated
2016 with the reference data is set to FALSE and the value of the retry counter associated with the
2017 reference data is decremented by one.
2018
- 2019 **AS4.70 The command data field shall contain the verification data to be compared with the value**
2020 **of the reference data followed by the new reference data. If the verification data is PIN and**
2021 **the actual PIN length is less than maximum length defined in authentication CRT, the PIN**
2022 **value shall be padded in accordance with GICS Part 1, Table 13.**
2023
- 2024 TE4.70.1 The tester shall verify that if the verification data is PIN and the actual PIN length is less than
2025 maximum length defined in authentication CRT, the PIN value is padded in accordance with
2026 GICS Part 1, Table 13.
2027
- 2028 **AS4.71 In order to change biometric on-card-comparison reference data, the PUT DATA command**
2029 **with tag '5F 2E' shall be used.**
2030

TE4.71.1 The tester shall verify that in order to change biometric on-card-comparison reference data, the PUT DATA command with tag '5F 2E' is used.

AS4.72 If P1 = '00', then the command data field shall contain the verification data to be compared with the value of the reference data followed by the new reference data.

TE4.72.1 The tester shall verify that if P1 = '00', then the command data field contains the verification data to be compared with the value of the reference data followed by the new reference data.

AS4.73 If P1 = '01', then the command data field shall contain only the new reference data. P1 = '01' shall only be allowed when the data objects life cycle state is in INITIALIZATION.

TE4.73.1 The tester shall verify that if P1 = '01', then the command data field contains only the new reference data.

TE4.73.2 The tester shall verify that P1 = '01' is only allowed during card initialization.

AS4.74 The response data field of the CHANGE REFERENCE DATA command shall be empty.

TE4.74.1 The tester shall verify that the response data field of the CHANGE REFERENCE DATA command is empty.

AS4.75 The status word returned by the CHANGE REFERENCE DATA command shall be one of the status words in GICS Part 1, Table 56.

TE4.75.1 The tester shall verify that all the status words listed in GICS Part 1, Table 56 are returned appropriately.

4.4.7 RESET RETRY COUNTER

AS4.76 Execution of the RESET RETRY COUNTER command shall be initiated only if the value of the reset counter associated with the reference data is greater than zero.

TE4.76.1 The tester shall verify that execution of the RESET RETRY COUNTER command is initiated only if the value of the reset counter associated with the reference data is greater than zero.

AS4.77 If the comparison is successful, then 1) the security state associated with the reference data shall be unchanged, 2) the reference data in the command data field shall replace the reference data associated with the reference data qualifier and 3) the value of the retry counter associated with the reference data shall be set to its reset value.

TE4.77.1 The tester shall verify that, if the comparison is successful, that the security state associated with the reference data is unchanged.

TE4.77.2 The tester shall verify that, if the comparison is successful, that the reference data in the command data field also replaces the reference data associated with the reference data qualifier.

- TE4.77.3 The tester shall verify that, if the comparison is successful, that the value of the retry counter associated with the reference data is also set to its reset value.
- AS4.78 If the comparison is unsuccessful, then the security state associated with the reference data shall be set to FALSE and the value of the reset counter associated with the reference data shall be decremented by one.**
- TE4.78.1 The tester shall verify that if the comparison is unsuccessful, then the security state associated with the reference data is set to FALSE and the value of the reset counter associated with the reference data is decremented by one.
- AS4.79 If P1 = '00', then the command data field shall contain the resetting code followed by the value of the new reference data. The existing reference data is replaced by the new reference data.**
- TE4.79.1 The tester shall verify that if P1 = '00', then the command data field contains the resetting code followed by the value of the new reference data, and that the existing reference data is replaced by the new reference data.
- AS4.80 If P1 = '01', then the command data field shall contain only the resetting code. The existing reference data is left unchanged.**
- TE4.80.1 The tester shall verify that if P1 = '01', then the command data field contains only the resetting code and the existing reference data is left unchanged.
- AS4.81 The response data field of the RESET RETRY COUNTER command shall be empty.**
- TE4.81.1 The tester shall verify that the response data field of the RESET RETRY COUNTER command is empty.
- AS4.82 The status word returned by the RESET RETRY COUNTER command shall be one of the status words in GICS Part 1, Table 58.**
- TE4.82.1 The tester shall verify that all the status words listed in GICS Part 1, Table 58 are returned appropriately.

4.4.8 MANAGE SECURITY ENVIRONMENT (Set)

- AS4.83 The MANAGE SECURITY ENVIRONMENT command shall execute successfully with respect to a data object only if the security condition associated with the MANAGE SECURITY ENVIRONMENT access mode in the security attribute of the data object evaluates to TRUE with respect to the current security status.**
- TE4.83.1 The tester shall verify that the MANAGE SECURITY ENVIRONMENT command executes successfully with respect to a data object only if the security condition associated with the MANAGE SECURITY ENVIRONMENT access mode in the security attribute of the data object evaluates to TRUE with respect to the current security status.

AS4.84 **MANAGE SECURITY ENVIRONMENT** command shall only maintain context for the immediately following **PERFORM SECURITY OPERATION** command.

TE4.84.1 The tester shall verify that **MANAGE SECURITY ENVIRONMENT** command only maintains context for the immediately following **PERFORM SECURITY OPERATION** command.

AS4.85 **There shall be no change in the current security status upon the execution of the MANAGE SECURITY ENVIRONMENT** command.

TE4.85.1 The tester shall verify that there is no change in the current security status upon the execution of the **MANAGE SECURITY ENVIRONMENT** command.

AS4.86 **The value of P1 shall be one of those in GICS Part 1, Table 60.**

TE4.86.1 The tester shall verify that all the status words listed in GICS Part 1, Table 60 are returned appropriately

AS4.87 **The value of P2 shall be one of those listed in GICS Part 1, Table 26.**

TE4.87.1 The tester shall verify that all the status words listed in GICS Part 1, Table 26 are returned appropriately.

AS4.88 **If the control reference template referenced by P2 exists in the current security environment, then it shall be replaced in its entirety by the control reference template in the command field of the MANAGE SECURITY ENVIRONMENT** command.

TE4.88.1 The tester shall verify that if the control reference template referenced by P2 exists in the current security environment, then it is temporarily replaced in its entirety by the control reference template in the command field of the **MANAGE SECURITY ENVIRONMENT** command.

AS4.89 **The command data field shall consist of a sequence of zero or more data objects that comprise a valid value field of the control reference template whose tag is in P2.**

TE4.89.1 The tester shall verify that the command data field consists of a sequence of zero or more data objects that comprise a valid value field of the control reference template whose tag is in P2.

AS4.90 **If the command data field is absent, then the control reference template referenced by P2 shall be deleted from the current security environment.**

TE4.90.1 The tester shall verify that if the command data field is absent, then the control reference template referenced by P2 is deleted from the current security environment.

AS4.91 **The response data field of a MANAGE SECURITY ENVIRONMENT** command shall be empty.

TE4.91.1 The tester shall verify that the response data field of a **MANAGE SECURITY ENVIRONMENT** command is empty.

AS4.92 The status word returned by the MANAGE SECURITY ENVIRONMENT command shall be one of the status words in GICS Part 1, Table 61.

TE4.92.1 The tester shall verify that all the status words listed in GICS Part 1, Table 61 are returned appropriately.

4.4.9 GENERAL AUTHENTICATE

AS4.93 For each data object used by the GENERAL AUTHENTICATE command the security condition associated with the GENERAL AUTHENTICATE access mode in the security attribute associated with the data object shall evaluate to TRUE with respect to the current security status.

TE4.93.1 The tester shall verify that for each data object used by the GENERAL AUTHENTICATE command the security condition associated with the GENERAL AUTHENTICATE access mode in the security attribute associated with the data object evaluates to TRUE with respect to the current security status

AS4.94 If the execution is successful, then the security state associated with the reference data shall be set to TRUE.

TE4.94.1 The tester shall verify that if the execution is successful, then the security state associated with the reference data is set to TRUE.

AS4.95 If the execution is unsuccessful, then the security state associated with the reference data shall be set to FALSE.

TE4.95.1 The tester shall verify that if the execution is unsuccessful, then the security state associated with the reference data is set to FALSE.

AS4.96 The reference data qualifier is application specific and should be defined as specified in Part 4 of this standard. If more than one reference data qualifier value is used in the authentication protocol, then P2 shall be set to '00' and the current security environment shall contain the required reference data qualifier values.

TE4.96.1 The tester shall verify that if more than one reference data qualifier value is used in the authentication protocol, then P2 is set to '00' and the current security environment contains the required reference data qualifier values.

AS4.97 If odd instruction is used, the command data field shall include a dynamic authentication template (tag '7C') containing one or more of the data objects listed in GICS Part 1, Table 63.

TE4.97.1 If odd instruction is used the tester shall verify that the command data field includes a dynamic authentication template (tag '7C') containing one or more of the data objects listed in GICS Part 1, Table 63.

AS4.98 If even instruction is used, the command data field shall consist of a sequence of bytes which comply with the standard of the algorithm referenced in P1.

TE4.98.1 If even instruction is used the tester shall verify that the command data field consists of a sequence of bytes which comply with the standard of the algorithm referenced in P1.

AS4.99 The response data field(s) of the GENERAL AUTHENTICATE command shall be determined by the algorithm qualifier referenced in P1.

TE4.99.1 The tester shall verify that the response data field(s) of the GENERAL AUTHENTICATE command are determined by the algorithm qualifier referenced in P1.

AS4.100 The status word returned by the GENERAL AUTHENTICATE command shall be one of the status words in GICS Part 1, Table 64.

TE4.100.1 The tester shall verify that all the status words listed in GICS Part 1, Table 64 are returned appropriately.

4.4.10 PERFORM SECURITY OPERATION

AS4.101 For each data object used by the PERFORM SECURITY OPERATION command the security condition associated with the PERFORM SECURITY OPERATION access mode in the security attribute associated with the data object shall evaluate to TRUE with respect to the current security status.

TE4.101.1 The tester shall verify that for each data object used by the PERFORM SECURITY OPERATION command the security condition associated with the PERFORM SECURITY OPERATION access mode in the security attribute associated with the data object evaluates to TRUE with respect to the current security status.

AS4.102 There shall be no change in the current security status upon the execution of the PERFORM SECURITY OPERATION command.

TE4.102.1 The tester shall verify that there is no change in the current security status upon the execution of the PERFORM SECURITY OPERATION command.

AS4.103 The value of P1-P2 shall be one of the P1-P2 pairs listed in GICS Part 1, Table 66.

TE4.103.1 The tester shall verify that the value of P1-P2 is one of the P1-P2 pairs listed in GICS Part 1, Table 66.

AS4.104 The cryptographic and authentication mechanisms appearing in these cryptographic reference templates shall be those of GICS Part 1, Table 23.

TE4.104.1 The tester shall verify that the cryptographic and authentication mechanisms appearing in these cryptographic reference templates are those of GICS Part 1, Table 23.

AS4.105 If P1 or P2 indicates the use of secure message data objects (SM) in GICS Part 1, Table 66, then the command data field shall be a sequence of secure message data objects listed in GICS Part 1, Table 35.

TE4.105.1 The tester shall verify that if P1 or P2 indicates the use of secure message data objects (SM) in GICS Part 1, Table 66, then the command data field is a sequence of secure message data objects listed in GICS Part 1, Table 35.

AS4.106 Explicit indication of the use of a particular cryptographic mechanism with a **PERFORM SECURITY OPERATION** command shall be made by including a cryptographic mechanism reference (tag '80') in the control reference template associated with the operation. The value field of this data object shall reference the value field of the corresponding reference data object (tag '80') in the cryptographic mechanism (tag 'AC') data object in the control parameters template of the currently selected dedicated file.

TE4.106.1 The tester shall verify that explicit indication of the use of a particular cryptographic mechanism with a **PERFORM SECURITY OPERATION** command is made by including a cryptographic mechanism reference (tag '80') in the control reference template associated with the operation.

TE4.106.2 The tester shall verify that the value field of this data object references the value field of the corresponding reference data object (tag '80') in the cryptographic mechanism (tag 'AC') data object in the control parameters template of the currently selected dedicated file.

AS4.107 The response data field shall be the data element indicated by P1.

TE4.107.1 The tester shall verify that the response data field is the data element indicated by P1.

AS4.108 The status word returned by the **PERFORM SECURITY OPERATION** command shall be one of the status words in GICS Part 1, Table 67.

TE4.108.1 The tester shall verify that all the status words listed in GICS Part 1, Table 67 are returned appropriately.

4.4.11 GET RESPONSE (For Transmission Handling)

AS4.109 There shall be no change in the current security status upon the execution of the **GET RESPONSE** command.

TE4.109.1 The tester shall verify that there are no changes in the current security status upon the execution of the **GET RESPONSE** command.

AS4.110 The command data field shall be empty.

TE4.110.1 The tester shall verify that the command data field is empty.

AS4.111 If the L_e field is set to '00', then all the available bytes should be returned within the limit of 256 for a short L_e field, or 65,536 for an extended L_e field.

TE4.111.1 The tester shall verify that if the L_e field is set to '00', then all the available bytes should be returned within the limit of 256 for a short L_e field, or 65,536 for an extended L_e field.

AS4.112 The status word returned by the GET RESPONSE command shall be one of the status words in GICS Part 1, Table 69.

TE4.112.1 The tester shall verify that all the status words listed in GICS Part 1, Table 69 are returned appropriately.

4.5 Operation

4.5.1 Model of Computation

AS5.1 Access to a particular GICS-application shall be initiated by using the SELECT command with P1='04' to set as the currently selected dedicated file the application dedicated file that is the root of the file hierarchy containing the data elements comprising the GICS-application.

TE5.1.1 The tester shall verify that access to a particular GICS-application is initiated by using the SELECT command with P1='04' to set as the currently selected dedicated file the application dedicated file that is the root of the file hierarchy containing the data elements comprising the GICS-application.

AS5.2 Access to the GICS-application's data objects stored in the application dedicated file shall be achieved by using the GET DATA and PUT DATA commands.

TE5.2.1 The tester shall verify that access to the GICS-application's data objects stored in the application dedicated file is achieved by using the GET DATA and PUT DATA commands.

4.5.2 Interindustry Data Objects

AS5.3 Subject to the security condition for the GET DATA access mode, the interindustry data objects in GICS Part 1, Table 70 shall be retrievable from the indicated file type using the GET DATA command.

TE5.3.1 The tester shall verify that subject to the security condition for the GET DATA access mode, the interindustry data objects in GICS Part 1, Table 70 are retrievable from the indicated file type using the GET DATA command.

4.6 Signature and Key Establishment Protocols

- AS6.1 This section describes how signature and key establishment protocols defined in GICS Part 1, Table 23 shall be implemented using the GICS commands defined in Section 6.**
- TE6.1.1 The tester shall verify that signature and key establishment protocols defined in GICS Part 1, Table 23 are implemented using the GICS commands defined in Section 6.
- AS6.2 If a GICS application uses any of the protocols defined in GICS Part 1, Table 23, the control parameters of an ADF for a GICS application shall use cryptographic mechanism identifier template (tag 'AC') to indicate which cryptographic mechanisms are used from GICS Part 1, Table 23.**
- TE6.2.1 The tester shall verify that if a GICS application uses any of the protocols defined in GICS Part 1, Table 23, that the control parameters of an ADF for a GICS application use cryptographic mechanism identifier template (tag 'AC') to indicate which cryptographic mechanisms are used from GICS Part 1, Table 23.

4.6.2 Signature Protocols

- AS6.3 Initial Vector (IV) shall contain intermediate hash || counter number of bytes.**
- TE6.3.1 The tester shall verify that Initial Vector (IV) contains intermediate hash || counter number of bytes.
- AS6.4 Signature with partial on-card hashing shall be implemented in accordance with GICS Part 1, Table 71.**
- TE6.4.1 The tester shall verify that signature with partial on-card hashing is implemented in accordance with GICS Part 1, Table 71.
- AS6.5 Signature with full on-card hashing shall be implemented in accordance with GICS Part 1, Table 72.**
- TE6.5.1 The tester shall verify that signature with full on-card hashing is implemented in accordance with GICS Part 1, Table 72.
- AS6.6 Signature with off-card hashing shall be implemented in accordance with GICS Part 1, Table 73.**
- TE6.6.1 The tester shall verify that signature with off-card hashing is implemented in accordance with GICS Part 1, Table 73.
- AS6.7 Signature with off-card hashing using GENERAL AUTHENTICATE shall be implemented in accordance with GICS Part 1, Table 74.**
- TE6.7.1 The tester shall verify that signature with off-card hashing using GENERAL AUTHENTICATE is implemented in accordance with GICS Part 1, Table 74.

AS6.8 Signature with ECC using GENERAL AUTHENTICATE shall be implemented in accordance with GICS Part 1, Table 75.

TE6.8.1 The tester shall verify that signature with ECC using GENERAL AUTHENTICATE is implemented in accordance with GICS Part 1, Table 75.

4.6.3 Key Establishment Protocols

AS6.9 Key Establishment using Symmetric Key (Internal Authenticate) Command Interface

TE6.9.1 The tester shall verify that the command interface for Key Establishment using Symmetric Key (Internal Authenticate) is implemented in accordance with GICS Part 1, Table 76.

AS6.10 Key Establishment using Symmetric Key (Mutual Authenticate)

TE6.10.1 The tester shall verify that the command interface for Key Establishment using Symmetric Key (Mutual Authenticate) is implemented in accordance with GICS Part 1, Table 77.

AS6.11 Key Establishment using Symmetric Key (Mutual Authenticate and Data Integrity)

TE6.11.1 The tester shall verify that the command interface for Key Establishment using Symmetric Key (Mutual Authenticate and Data Integrity) is implemented in accordance with GICS Part 1, Table 78.

AS6.12 RSA Key Transport

TE6.12.1 The tester shall verify that the command interface for RSA Key Transport is implemented in accordance with GICS Part 1, Table 83.

AS6.13 Key Establishment using an RSA Key Pair

TE6.13.1 The tester shall verify that the command interface for Key Establishment using an RSA Key Pair is implemented in accordance with GICS Part 1, Table 84.

AS6.14 Key Establishment with an ECC Key Pair, Diffie-Hellman C(1,1,ECC CDH)

TE6.14.1 The tester shall verify that the command interface for Key Establishment with an ECC Key Pair, Diffie-Hellman C(1,1,ECC CDH) is implemented in accordance with GICS Part 1, Table 86.

4.6.4 Session Key Establishment

AS6.15 Session Key Establishment

TE6.15.1 The tester shall verify that the session keys are generated in accordance with the procedure described in Section 8.3 of GICS Part 1.

2483

2484 **4.7 Secure Messaging**

2485

2486 **AS7.1 Bit three (b3) and four (b4) in the class byte of the command shall be set to one to indicate**
2487 **secure messaging. Moreover, all the indications of secure messaging shall be set**
2488 **consistently in P1, P2, and Command data field.**

2489

2490 TE7.1.1 The tester shall verify that bit three (b3) and four (b4) in the class byte of the command are set
2491 to one to indicate secure messaging.

2492 TE7.1.2 The tester shall verify that all the indications of secure messaging are set consistently in P1, P2,
2493 and Command data field.

2494

2495

2496 **AS7.2 The response data field of a response to a command in which bit three (b3) and four (b4) in**
2497 **the class byte has been set to one shall be in secure message format.**

2498

2499 TE7.2.1 The tester shall verify that the response data field of a response to a command in which bit three
2500 (b3) and four (b4) in the class byte has been set to one are in secure message format.

2501

2502 **AS7.3 A data field in secure message format shall be constructed according to Secure Messaging**
2503 **described in this section. By default security messaging shall always incorporate MAC.**
2504 **Encryption in secure messaging may or may not be used depending on the authentication**
2505 **protocol or the access control rule on the data object. If encryption is used, the data is**
2506 **encrypted using AES in Cipher Block Chaining (CBC) mode with the SK_{ENC} session key. A**
2507 **data field in secure message format shall be constructed using one or more data objects**
2508 **with tags listed in GICS Part 1, Table 35.**

2509

2510 TE7.3.1 The tester shall verify that a data field in secure message format is constructed according to
2511 Secure Messaging described in this section.

2512 TE7.3.2 By default security messaging shall always incorporate MAC. Encryption in secure messaging
2513 may or may not be used depending on the authentication protocol or the access control rule on
2514 the data object. A data field in secure message format shall be constructed using one or more
2515 data objects with tags listed in GICS Part 1, Table 35.

2516

2517 **AS7.4 When bit five (b5) is also set to one, compute secure messaging on the entire message**
2518 **before command fragmentation for data transportation.**

2519 TE7.4.1 The tester shall verify that when bit five (b5) is set to one, that secure messaging on the entire
2520 message is computed before command fragmentation for data transportation.

2521

2522 **4.7.2 AES Secure Messaging**

2523

2524 **AS7.5 Implementation of AES Secure Messaging.**

2525 TE7.5.1 The tester shall verify that implementation of AES secure messaging is in accordance with GICS
2526 Part 1, Section 9.1.

2527

4.8 Card Manager Application (INCITS 504 Part 2 Test Requirements)

4.8.1 Overview

AS8.1 In accordance with ISO/IEC 7816-13 a card-manager-application shall always be present and unique.

TE8.1.1 The tester shall verify that a card-manager-application is always present

TE8.1.2 The tester shall verify that the card-manager-application is always unique

AS8.2 The-card-manager application shall provide the required characteristics, resources and functions of the alpha card-application defined in ISO/IEC 24727-2.

TE8.2.1 The tester shall verify that shall verify that the card-manager applications AID is the alpha card-AID of ISO/IEC 24727-2.

AS8.3 The card-manager-application is an ISO/IEC 7816-4 Application DF (ADF), and its DF name or Application Identifier (AID) shall be 'E8 28 81 C1 17 02'.

TE8.3.1 The tester shall verify that the DF name, or AID, for the card-manager application is 'E8 28 81 C1 17 02'.

AS8.4 The card-manager-application AID is always present in EF.DIR.

TE8.4.1 The tester shall verify that the card-manager-application AID is always present in EF.DIR.

AS8.5 The card-manager-application shall always be selectable using the SELECT command.

TE8.5.1 The tester shall verify that the card-manager-application is always be selectable using the SELECT command.

AS8.6 The card-manager-application shall behave like any card-application and return the application template and control parameter (CP) values upon selection.

TE8.6.1 The tester shall verify that the card-manager-application returns the application template and control parameter (CP) values upon selection.

AS8.7 The card-manager-application shall expose at its interface the Data Objects (DO) specified in GICS Part 2, Table 2. These DOs can be accessed with the GET DATA command.

TE8.7.1 The tester shall verify that the card-manager-application exposes at its interface the Data Objects (DO) specified in GICS Part 2, Table 2.

TE8.7.2 The tester shall verify that these DOs can be accessed with the GET DATA command.

AS8.8 The selection of the card-manager-application in operational activated mode followed with a GET DATA with P1-P2='3FFF' and command data field containing respectively '5C027F62' '5C027F63', and '5C027F64', shall return respectively the CCD, ACD and card management service template contents. This is in compliance with the discovery rules of ISO/IEC 24727-2 Section 6.4.2 and 6.4.3.

TE8.8.1 The tester shall verify that the selection of the card-manager-application in operational activated mode followed with a GET DATA with P1-P2='3FFF' and command data field containing respectively '5C027F62' '5C027F63', and '5C027F64', returns respectively the CCD, ACD and card management service template contents.

AS8.9 The establishment of GICS platform persistent states using directly ISO/IEC 24727 mechanisms at the card interface shall be possible.

TE8.9.1 The tester shall verify that the establishment of GICS platform persistent states using directly ISO/IEC 24727 mechanisms at the card interface is possible.

AS8.10 The card-manager-application status shall always be "Operational Activated".

TE8.10.1 The tester shall verify that the card-manager-application status is always "Operational Activated".

4.8.2 Initial –GICS State

AS8.11 An Initial state of the GICS platform is specified. In this state any card-application life cycle status is 'Creation', except the card-manager-application life cycle status which is 'Operational Activated'.

TE8.11.1 The tester shall verify that in the initial state of the GICS platform any card-application life cycle status is 'Creation', except the card-manager-application life cycle status which is 'Operational Activated'.

AS8.12 In the Initial-GICS state, the card-manager-application shall be configured with the data structures defined in GICS Part 2, Section 3.5.

TE8.12.1 The tester shall verify that, in the Initial-GICS state, the card-manager-application is configured with the data structures defined in GICS Part 2, Section 3.5.

AS8.13 In the Initial-GICS state, the card-manager-application shall have registered from a Key Manager and make available two initial key sets:
1) Three symmetric AES-256 keys for Key Establishment with Symmetric Key – mutual authentication (KESK-SCP03) session key establishment through the contact interface. The minimum security level for secure messaging is command MAC only
2) One asymmetric Elliptic Curve P-256 private key, the associated Card Verifiable Certificate (CVC) and one issuer public signature verification keys for Opacity FS session key establishment, through either the contact interface or the contactless interface.

TE8.13.1 The tester shall verify that one of those initial key sets is three symmetric AES-256 keys for Key Establishment with Symmetric Key – mutual authentication (KESK-SCP03) session key establishment through the contact interface. The minimum security level for secure messaging is command MAC only.

TE8.13.2 The tester shall verify that the other initial key sets is one asymmetric Elliptic Curve P-256 private key, the associated Card Verifiable Certificate (CVC) and one issuer public signature verification keys for Opacity FS session key establishment, through either the contact interface or the contactless interface.

AS8.14 The initial key sets are global security objects for use on commands during key establishment and secure messaging operations. Regardless the communication interface involved (contact or contactless), those keys sets protect commands from the card-manager application but they may also be used by any other GICS card-applications"

TE8.14.1 The tester shall verify that the initial key sets protect commands from the card-manager application

4.8.3 Updates

AS8.15 The card-manager-application shall support the addition, update and removal of keys and supporting DOs with the following conditions or capabilities:

- **Key usage shall be restricted to either KESK-SCP03 or Opacity FS cryptographic mechanisms.**
- **Key domain parameters, cipher suites and security attributes of new security object DOs may differ from those used for the security object DOs of the Initial GICS state.**
- **CREATE DO Command is used to create Security Object DOs.**
- **Elementary Files (EF) are used to store the associated CVC DO and signature verification public keys.**
- **For other mechanisms than KESK-SCP03 or Opacity FS, global security objects DOs and EFs containing security object DOs shall be created from other card-applications.**
- **DELETE DO Command is used to delete Security Object DOs. This command destroys the associated key.**
- **Key replacement or destruction is supported for all card-manager-application keys.**
- **Any security object DOs previously created from the card-manager-application may be deleted from the card-manager-application.**
- **All security objects creation, update or removal commands are protected with secure messaging.**

TE8.15.1 The tester shall verify that key usage shall be restricted to either KESK-SCP03 or Opacity FS cryptographic mechanisms.

TE8.15.2 The tester shall verify that key domain parameters, cipher suites and security attributes of new security object DOs are allowed to differ from those used for the security object DOs of the Initial GICS state.

TE8.15.3 The tester shall verify that CREATE DO Command is used to create Security Object DOs.

TE8.15.4 The tester shall verify that Elementary Files (EF) are used to store the associated CVC DO and signature verification public keys.

TE8.15.5 The tester shall verify that for mechanisms other than KESK-SCP03 or Opacity FS, global security objects DOs and EFs containing security object DOs are created from other card-applications.

TE8.15.6 The tester shall verify that the DELETE DO Command is used to delete Security Object Dos and that this command destroys the associated key.

TE8.15.7 The tester shall verify that key replacement or destruction is supported for all card-manager-application keys.

- 2679 TE8.15.8 The tester shall verify that any security object DOs previously created from the card-manager-
2680 application can be deleted from the card-manager-application.
2681 TE8.15.9 The tester shall verify that all security objects creation, update or deletion commands are
2682 protected with secure messaging.
2683
2684
2685 **AS8.16 The card-manager-application shall support the creation of additional card-applications**
2686 **using the APPLICATION MANAGEMENT REQUEST command when the card-manager-**
2687 **application is the currently selected application.**
2688
2689 TE8.16.1 The tester shall verify that the card-manager-application supports the creation of additional card-
2690 applications using the APPLICATION MANAGEMENT REQUEST command when the card-
2691 manager-application is the currently selected application.
2692
2693
2694 **AS8.17 The card-manager-application shall support the removal of additional card-applications**
2695 **using the REMOVE APPLICATION command when the card-manager-application is the**
2696 **currently selected application.**
2697
2698 TE8.17.1 The tester shall verify that the card-manager-application supports the deletion of additional card-
2699 applications using the REMOVE APPLICATION command when the card-manager-application
2700 is the currently selected application.
2701
2702
2703 **AS8.18 The card-manager-application shall support the activation (respectively deactivation) of**
2704 **card-applications other than the card-manager-application itself, The ACTIVATE (ADF)**
2705 **command (resp. DEACTIVATE (ADF) command) shall be used when the card-manager-**
2706 **application is the currently selected application.**
2707
2708 TE8.18.1 The tester shall verify that the card-manager-application supports the activation (resp.
2709 deactivation) of card-applications other than the card-manager-application itself.
2710 TE8.18.2 The tester shall verify that the ACTIVATE (ADF) command (resp. DEACTIVATE (ADF)
2711 command) is used when the card-manager-application is the currently selected application.
2712

2713 **4.8.4 Commands**

- 2714
2715 **AS8.19 The card-manager-application exposes all the commands in GICS Part 2, Table 1 at its**
2716 **interface.**
2717 TE8.19.1 The tester shall verify that the card-manager-application exposes all the commands in GICS
2718 Part 2, Table 1 at its interface:
2719

2720 **4.8.5 Data Structure**

- 2721 **AS8.20 All the DOs for discovery and management in GICS Part 2, Table 2 must be present and**
2722 **accessible from the card-manager-application at the Initial-GICS state.**
2723 TE8.20.1 All the DOs for discovery and management in GICS Part 2, Table 2 must be present and
2724 accessible from the card-manager-application at the Initial-GICS state.
2725
2726
2727 **AS8.21 All the DOs controlling the management and use of Security Objects in GICS Part 2, Table**
2728 **3 shall be present in the card-manager-application at the Initial-GICS state.**

DRAFT Generic Identity Command Set – Part 3: GICS Platform Testing Requirements

- 2729 TE8.21.1 All the DOs controlling the management and use of Security Objects in GICS Part 2, Table 3
2730 shall be present in the card-manager-application at the Initial-GICS state.
2731
2732
- 2733 **AS8.22 Security object values are set with PUT DATA once the Security Object DO is selected with**
2734 **SELECT DATA.**
- 2735 TE8.22.1 Security object values are set with PUT DATA once the Security Object DO is selected with
2736 SELECT DATA.
2737
2738
- 2739 **AS8.23 The security environment template (tag '7B') shall contain data objects as listed in GICS**
2740 **Part 2, Table 5.**
- 2741 TE8.23.1 The security environment template (tag '7B') shall contain data objects as listed in GICS Part 2,
2742 Table 5.
- 2743 **AS8.24 The card-manager-application CP is defined in GICS Part 2, Table 6.**
- 2744 TE8.24.1 The tester shall verify that the card-manager-application CP is implemented as defined in GICS
2745 Part 2, Table 6.
2746
2747
- 2748 **AS8.25 The Access Mode Field of the card-manager-application is '00 9B 3F', and encodes the**
2749 **card-manager-application commands in the following order:**
2750 **ACTIVATE EF/ADF**
2751 **DEACTIVATE EF/ADF**
2752 **CREATE FILE (EF creation)**
2753 **DELETE FILE**
2754 **CREATE DO**
2755 **DELETE DO**
2756 **APPLICATION MANAGEMENT REQUEST**
2757 **REMOVE APPLICATION**
2758 **PUT DATA**
2759 **GET DATA**
2760
- 2761 TE8.25.1 The tester shall verify that the AMF of the card-manager application is '00 9B 3F'.
- 2762 TE8.25.2 The tester shall verify that the card-manager application commands are encoded in the following
2763 order:
2764 **ACTIVATE EF/ADF**
2765 **DEACTIVATE EF/ADF**
2766 **CREATE FILE (EF creation)**
2767 **DELETE FILE**
2768 **CREATE DO**
2769 **DELETE DO**
2770 **APPLICATION MANAGEMENT REQUEST**
2771 **REMOVE APPLICATION**
2772 **PUT DATA**
2773 **GET DATA**
2774
2775
- 2776 **AS8.26 The security condition byte for the card-manager application shall be as defined in GICS**
2777 **Part 2, Tables 7 and 8.**
- 2778
- 2779 TE8.26.1 The tester shall verify that the security condition byte for the card-manager application is defined
2780 according to GICS Part 2, Tables 7 and 8.
2781

AS8.27 EF '13 11' contains the list of CVC that are trusted by the card manager and shall be used to authenticate the host.

TE8.27.1 The tester shall verify that EF '13 11' is used to authenticate the host.

AS8.28 The *Card Management Service Template* is a collection of Data Objects describing the card-manager- application capabilities. This template shall be accessible from the ADF of the card-manager-application with the PUT DATA and GET DATA commands defined in GICS Part 1. The access control rules are defined within the CP of the ADF. For retrieval, a GET DATA 'CB' command with P1-P2 = "3FFF", Lc = '04', Data= '5C02 7F64' and Le = '00' shall return the mandatory card management service template in the response data field when the card manager application is selected.

TE8.28.1 The tester shall verify that the *Card Management Service Template* is accessible from the ADF of the card-manager-application with the PUT DATA and GET DATA commands defined in GICS Part 1.

TE8.28.2 The tester shall verify that, for retrieval, a GET DATA 'CB' command with P1-P2 = "3FFF", Lc = '04', Data= '5C02 7F64' and Le = '00' returns the mandatory card management service template in the response data field when the card manager application is selected

AS8.29 The *Card Management Service Template* shall include the values in GICS Part 2, Table 17.

TE8.29.1 The tester shall verify that the *Card Management Service Template* includes the values in GICS Part 2, Table 17.

AS8.30 The *Card Data Template* is a collection of Data Objects identifying the card, its state and its applications for the purpose of managing or synchronizing the card from a Card Management System. The template shall be accessible from the ADF of the card manager application through the PUT DATA and GET DATA commands defined in GICS Part 1. The access control rules are defined within the CP of the ADF.

TE8.30.1 The tester shall verify that the *Card Data Template* is accessible from the ADF of the card manager application through the PUT DATA and GET DATA commands defined in GICS Part 1.

4.8.6 Card Identification Scheme

AS8.31 The GICS Card Identification Scheme is unique, fixed and refers to the location, access method, syntax and semantic rules that specify interoperable card identification information of a GICS platform. The GICS Card Identification Scheme is specified as an OID within the data object (Tag '82') of the card management service template (Tag '7F64'). The Object Identifier (OID) referencing the collection of objects defined in this standard is:

```
gics-OID ::= {iso(1) member-body(2) country-USA(840) incits
(114402) incits-committee-identifier(21012) grouping (2) }

gics-identification-scheme-OID ::= {gics-OID parameter(1)}
```

According to the GICS Card Identification Scheme, the value of the Card Issuer Data Object (Tag '45') in the Card Data template contains interoperable identification information. The value shall be determined by the card issuer to uniquely identify a card in the context of

operation. The format is the concatenation of the Issuer Identification Number (IIN - 6 bytes) and the Card Identification Number (CIN - 10 bytes).

TE8.31.1 Testing this out of scope for GICS Part 3.

4.8.7 Card Management Scheme

AS8.32 The GICS card management scheme is unique, fixed and refers to the card management scheme of a GICS platform. It is specified as an OID within the data object (Tag '81') of the card management service template (Tag '7F64'):

`gics-management-scheme-OID ::= { gics-OID parameter(2) }`

In accordance with the GICS Card Management Scheme, all commands, discovery mechanisms and data structures of the card manager application shall be implemented according to Clause 3.

TE8.32.1 Covered by other AS; no separate testing required for this AS.

4.9 Application Management

4.9.1 Application Life Cycle

AS9.1 A life cycle status is associated with each application.

TE9.1.1 The tester shall verify that a life cycle status is associated with each application.

AS9.2 Application life cycle states are defined as per GICS Part 2, Table 19.

TE9.2.1 The tester shall verify that application life cycle states are defined as per GICS Part 2, Table 19.

AS9.3 The supported application life cycle state transitions are defined as the first and second bytes of the card management capabilities per GICS Part 2, Tables 20 and 21.

TE9.3.1 The tester shall verify that application life cycle state transitions are defined as the first and second bytes of the card management capabilities per GICS Part 2, Tables 20 and 21.

4.9.2 Security Attributes

AS9.4 The first byte of AMF (Access Mode Field) shall be '00'.

TE9.4.1 The tester shall verify that the first byte of AMF shall be '00'.

4.10 File Management

4.10.1 File Life Cycle

AS10.1 File life cycle states are defined as in ISO/IEC 7816-9 in Section 5.

TE10.1.1 The tester shall verify all life cycle statuses of GICS Part 2, Table 24

AS10.2 LCS bytes can only be modified with the commands executing the transitions of GICS Part 2, Table 25.

TE10.2.1 The tester shall verify that LCS bytes can only be modified with the commands executing the transitions of GICS Part 2, Table 25.

4.10.2 Data Structures for File Management

AS10.3 The CPs of an ADF are set using the APPLICATION MANAGEMENT REQUEST command.

TE10.3.1 The tester shall verify that the CPs of an ADF are set by using the APPLICATION MANAGEMENT REQUEST command as per GICS Part 2, Table 34.

AS10.4 The Access Mode Byte for the EFs shall be used as defined in GICS Part 2, Table 26.

TE10.4.1 The tester shall verify that the Access Mode Byte for EFs are in accordance with GICS Part 2, Table 26.

4.11 Key Management

4.11.1 Key Life Cycle

AS11.1 To allow for Security Object management, card-application state shall be either in Initialized or Operational Activated state.

TE11.1.1 To allow for Security Object management, card-application state shall be either in Initialized or Operational Activated state.

4.12 Authentication Objects Management

Authentication Objects Life Cycle

AS12.1 To allow for Authentication Object management, Authentication Objects state shall be either in Initialized or Operational Activated state as per GICS Part 2, Table 30.

2918 TE12.1.1 The tester shall verify that Authentication Objects state are either in Initialized or Operational
2919 Activated states as per GICS Part 2, Table 30.
2920

2921 **4.13 Administrative Command Set**

2922 **4.13.1 APPLICATION MANAGEMENT REQUEST**

2923
2924 **AS13.1 The APPLICATION MANAGEMENT REQUEST command shall execute successfully the**
2925 **application life cycle transition only if the security condition associated with the access**
2926 **mode APPLICATION MANAGEMENT REQUEST in the security attribute of the currently**
2927 **selected card-application manager evaluates to TRUE with respect to the current security**
2928 **status.**
2929

2930 TE13.1.1 The tester shall verify that the APPLICATION MANAGEMENT REQUEST command executes
2931 successfully the application life cycle transition only if the security condition associated with the
2932 access mode APPLICATION MANAGEMENT REQUEST in the security attribute of the currently
2933 selected card-application manager evaluates to TRUE with respect to the current security
2934 status.
2935

2936
2937 **AS13.2 If a card-application becomes Operational Activated, it shall be present in EF.DIR.**
2938

2939 TE13.2.1 The tester shall verify that if a card-application becomes Operational Activated, it is present in
2940 EF.DIR.
2941

2942
2943 **AS13.3 Response Data Field shall be present. '00' by default.**
2944

2945 TE13.3.1 The tester shall verify that Response Data Field is present and is '00' by default.

2946 **AS13.4 The status word returned by the APPLICATION MANAGEMENT REQUEST command shall**
2947 **be one of the status words in GICS Part 2, Table 35.**
2948

2949 TE13.4.1 The tester shall verify that all the status words listed in GICS Part 2, Table 35 are returned
2950 appropriately.
2951

2952

2953 **4.13.2 REMOVE APPLICATION**

2954 **AS13.5 The REMOVE APPLICATION command shall delete an application (*). The Application**
2955 **returns in creation state, i.e. the program modules are present, and the application is not**
2956 **selectable. The card manager application verifies presence of the AID in the card when**
2957 **removing information.**

2958 TE13.5.1 The tester shall verify that the REMOVE APPLICATION command deletes an application and
2959 that the resources supporting the application are fully reclaimed.

2960 TE13.5.2 The tester shall verify that the Application returns in creation state, ie. the program modules are
2961 present, and the application is not selectable.

2962 TE13.5.3 The tester shall verify that the card manager application verifies presence of the AID in the card
2963 when removing information
2964
2965 .

AS13.6 If a card-application returns in Creation state, it shall be removed from EF.DIR.

TE13.6.1 The tester shall verify that if a card-application returns in Creation state, the card-application is removed from EF.DIR.

AS13.7 The REMOVE APPLICATION command shall execute successfully when deleting an application only if the security condition associated with the access mode REMOVE APPLICATION in the security attribute of the currently selected card-application manager evaluates to TRUE with respect to the current security status.

TE13.7.1 The tester shall verify that the REMOVE APPLICATION command executes successfully when deleting an application only if the security condition associated with the access mode REMOVE APPLICATION in the security attribute of the currently selected card-application manager evaluates to TRUE with respect to the current security status.

AS13.8 Response data field shall be present. Default value is '00'.

TE13.8.1 The tester shall verify that response data field is present and is '00' by default.

AS13.9 The status word returned by the REMOVE APPLICATION command shall be one of the status words in GICS Part 2, Table 39.

TE13.9.1 The tester shall verify that all the status words listed in GICS Part 2, Table 39 are returned appropriately.

4.13.3 CREATE DO

AS13.10 The CREATE DO command shall execute successfully when creating a data object only if the security condition associated with the access mode CREATE DO (DO creation) in the security attribute of the currently selected Application DF evaluates to TRUE with respect to the current security status.

TE13.10.1 The tester shall verify that the CREATE DO command executes successfully when creating a data object only if the security condition associated with the access mode CREATE DO (DO creation) in the security attribute of the currently selected Application DF evaluates to TRUE with respect to the current security status.

AS13.11 The command data field shall be a CP template (tag '62') containing only data objects described in GICS Part 1, Section 5.2.3, Control Parameters for Security Object DO.

TE13.11.1 The tester shall verify that the command data field is a CP template (tag '62') containing only data objects described in GICS Part 1, Section 5.2.3, Control Parameters for Security Object DO.

AS13.12 The status word returned by the CREATE DO command shall be one of the status words in GICS Part 2, Table 41.

TE13.12.1 The tester shall verify that the status word returned by the CREATE DO command is one of the status words in GICS Part 2, Table 41.

4.13.4 DELETE DO

AS13.13 The DELETE DO command shall execute successfully when deleting a security object contained in the currently selected Application DF only if the security condition associated with the access mode DELETE DO in the security attribute of the currently selected Application DF evaluates to TRUE with respect to the current security status.

TE13.13.1 The tester shall verify that the DELETE DO command executes successfully when deleting a security object contained in the currently selected Application DF only if the security condition associated with the access mode DELETE DO in the security attribute of the currently selected Application DF evaluates to TRUE with respect to the current security status.

AS13.14 The status word returned by the DELETE DO command shall be one of the status words in GICS Part 2, Table 43.

TE13.14.1 The tester shall verify that the status word returned by the DELETE DO command is one of the status words in GICS Part 2, Table 43.

4.13.5 CREATE FILE

AS13.15 The CREATE FILE command shall execute successfully when creating an elementary file only if the security condition associated with the access mode CREATE FILE (EF creation) in the security attribute of the currently selected dedicated file evaluates to TRUE with respect to the current security status.

TE13.15.1 The tester shall verify that the CREATE FILE command executes successfully when creating an elementary file only if the security condition associated with the access mode CREATE FILE (EF creation) in the security attribute of the currently selected dedicated file evaluates to TRUE with respect to the current security status.

AS13.16 The command data field shall be an CP template (tag '62') containing only data objects described in GICS Part 1, Section 5.2.2, Control Parameters for Files

TE13.16.1 The tester shall verify that the command data field is an CP template (tag '62') containing only data objects described in GICS Part 1, Section 5.2.2, Control Parameters for Files.

AS13.17 The status word returned by the CREATE FILE command shall be one of the status words in GICS Part 2, Table 47.

TE13.17.1 The tester shall verify that the status word returned by the CREATE FILE command is one of the status words in GICS Part 2, Table 47.

3067

3068 4.13.6 DELETE FILE

3069

3070 **AS13.18 The DELETE FILE command shall execute successfully when deleting an elementary file**
3071 **contained in the currently selected dedicated file only if the security condition associated**
3072 **with the access mode DELETE FILE in the security attribute of the currently selected**
3073 **dedicated file evaluates to TRUE with respect to the current security status.**

3074

3075 TE13.18.1 The tester shall verify that the DELETE FILE command executes successfully when deleting an
3076 elementary file contained in the currently selected dedicated file only if the security condition
3077 associated with the access mode DELETE FILE in the security attribute of the currently selected
3078 dedicated file evaluates to TRUE with respect to the current security status.

3079 **AS13.19 The status word returned by the DELETE FILE command shall be one of the status words**
3080 **in GICS Part 2, Table 49.**

3081

3082 TE13.19.1 The tester shall verify that the status word returned by the DELETE FILE command is one of the
3083 status words in GICS Part 2, Table 49.

3084

3085

3086 4.13.7 ACTIVATE FILE

3087

3088 **AS13.20 The ACTIVATE FILE shall execute successfully only if the security condition associated**
3089 **with the ACTIVATE FILE access mode in the security attribute associated with file**
3090 **evaluates to TRUE.**

3091 TE13.20.1 The tester shall verify that the ACTIVATE FILE executes successfully only if the security
3092 condition associated with the ACTIVATE FILE access mode in the security attribute associated
3093 with file evaluates to TRUE.

3094

3095 **AS13.21 The status word returned by the ACTIVATE FILE command shall be one of the status**
3096 **words in GICS Part 2, Table 52.**

3097

3098 TE13.21.1 The tester shall verify that the status word returned by the ACTIVATE FILE command is one of
3099 the status words in GICS Part 2, Table 52.

3100

3101

3102 4.13.8 DEACTIVATE FILE

3103

3104 **AS13.22 The DEACTIVATE FILE shall execute successfully only if the security condition associated**
3105 **with the DEACTIVATE FILE access mode in the security attribute associated with file**
3106 **evaluates to TRUE.**

3107

3108 TE13.22.1 The tester shall verify that the DEACTIVATE FILE executes successfully only if the security
3109 condition associated with the DEACTIVATE FILE access mode in the security attribute
3110 associated with file evaluates to TRUE.

3111

3112

3113 **AS13.23 The status word returned by the DEACTIVATE FILE command shall be one of the status**
3114 **words in GICS Part 2, Table 55.**

TE13.23.1 The tester shall verify that the status word returned by the DEACTIVATE FILE command is one of the status words in GICS Part 2, Table 55.

4.13.9 GENERATE ASYMMETRIC KEY PAIR

AS13.24 The GENERATE ASYMMETRIC KEY PAIR command generates and stores an asymmetric key pair, and returns the resulting public key. If an existing key pair is present with the same reference data qualifier value then it is destroyed before a new key pair is generated. The resulting public key is returned with the response data field, or using GET DATA with Tag '7F49' on the corresponding Key EF.

TE13.24.1 The tester shall verify that the GENERATE ASYMMETRIC KEY PAIR command generates and stores an asymmetric key pair, and returns the resulting public key.

TE13.24.2 The tester shall verify that if an existing key pair is present with the same reference data qualifier value then it is destroyed before a new key pair is generated, and that the resulting public key is returned with the response data field, or using GET DATA with Tag '7F49' on the corresponding Key EF.

AS13.25 The corresponding Key EF shall be in initialization or operational activated state.

TE13.25.1 The tester shall verify that the corresponding Key EF is in initialization or operational activated state.

AS13.26 The status word returned by the GENERATE ASYMMETRIC KEY PAIR command shall be one of the status words in GICS Part 2, Table 60.

TE13.26.1 The tester shall verify that the status word returned by the GENERATE ASYMMETRIC KEY PAIR command is one of the status words in GICS Part 2, Table 60.

4.13.10 PUT DATA (Key)

AS13.27 For keys with multiple components, one PUT DATA command must be submitted for each component.

TE13.27.1 The tester shall verify that for keys with multiple components, one PUT DATA command is submitted for each component.

AS13.28 PUT_DATA (key) resets the key usage counters

TE13.28.1 The tester shall verify that PUT_DATA (key) resets the key usage counters

AS13.29 If the data object '87' is too long for a single command, then command chaining shall apply; the value field of the data object is the concatenation of the command data fields.

3164 TE13.29.1 The tester shall verify that if the data object '87' is too long for a single command, then
3165 command chaining applies; the value field of the data object is the concatenation of the
3166 command data fields.
3167

3168
3169 **AS13.30 The status word returned by the PUT DATA command shall be one of the status words in**
3170 **GICS Part 2, Table 63.**
3171

3172 TE13.30.1 The tester shall verify that all the status words listed in GICS Part 2, Table 63 are returned
3173 appropriately.