ETSI TS 103 834-2 V17.0.0 (2022-12)

TECHNICAL SPECIFICATION

Smart Secure Platform (SSP);
Part 2: Test Specification, SSP Test Tool Interface
(Release 17)

Reference

DTS/SET-00103834-2vh00

Keywords

SCL, SSP, test tool interface, testing

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00   Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

If you find a security vulnerability in the present document, please report it through our
Coordinated Vulnerability Disclosure Program:
https://www.etsi.org/standards/coordinated-vulnerability-disclosure

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

ETSI

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Secure Element Technologies (SET).

The present document is part 2 of a multi-part deliverable covering the Test Tool Interface (TTI) for the Smart Secure Platform (SSP). Full details of the entire series can be found in part 1 [1].

The contents of the present document are subject to continuing work within TC SET and may change following formal TC SET approval. If TC SET modifies the contents of the present document, it will then be republished by ETSI with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x   the first digit:

0   early working draft;

1   presented to TC SET for information;

2   presented to TC SET for approval;

3   or greater indicates TC SET approved document under change control.

y   the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z   the third digit is incremented when editorial only changes have been incorporated in the document.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ETSI TS 103 834-2 V17.0.0 (2022-12)
https://standards.iteh.ai/catalog/standards/sist/69f410d7-a25e-4448-b55a-
f609c572dd40/etsi-ts-103-834-2-v17-0-0-2022-12

1 Scope

The present document is part of a series of documents specifying the Test Tool Interface (TTI) for the Smart Secure Platform. The present document is the test specification for the Test Tool Interface (TTI) shown in the test environment of ETSI TS 103 999-1 [3], testing the implementations in accordance to ETSI TS 103 834-1 [7].

It contains:

- A list of requirements dedicated to the TTI derived from ETSI TS 103 999-1 [3];

- TTI related requirements from ETSI TS 103 834-1 [7];

- TTI related requirements from ETSI TS 103 666-1 [1] and ETSI TS 103 666-2 [2];

- the principle and requirements for testing the SSP Primary Platform (also known as VPP);

- a selection of test cases to verify the implementation of the TTI independently from the respective manufacturers.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

- In the case of a reference to a TC SET document, a non-specific reference implicitly refers to the latest version of that document in the same Release as the present document.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference/.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

[1]   ETSI TS 103 666-1: "Smart Secure Platform (SSP); Part 1: General characteristics".

[2]   ETSI TS 103 666-2: "Smart Secure Platform (SSP); Part 2: Integrated SSP (iSSP) characteristics".

[3]   ETSI TS 103 999-1: "Smart Secure Platform (SSP); Part 1: Test Specification, general characteristics".

[4]   ETSI TS 103 999-2: "Smart Secure Platform (SSP); Part 2: Integrated SSP (iSSP) characteristics Test Specification".

[5]   GlobalPlatform: "Virtual Primary Platform - Network Protocol" Version 2.0.

NOTE: Available at https://globalplatform.org/specs-library/globalplatform-technology-virtual-primary-platform/.

[6]   ETSI TS 102 622: "Smart Cards; UICC - Contactless Front-end (CLF) Interface; Host Controller Interface (HCI)".

[7]   ETSI TS 103 834-1: "Smart Secure Platform (SSP); Part 1: Technical Specification, SSP Test Tool Interface".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

- In the case of a reference to a TC SET document, a non-specific reference implicitly refers to the latest version of that document in the same Release as the present document.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] Recommendation ITU-T X.680: "Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation".

[i.2] Recommendation ITU-T X.690: "Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)".

3 Definition of terms, symbols, abbreviations and formats

3.1 Terms

For the purposes of the present document, the terms given in ETSI TS 103 666-1 [1] and ETSI TS 103 999-1 [3] apply.

3.2 Symbols

For the purposes of the present document, the symbols given in ETSI TS 103 666-1 [1] and ETSI TS 103 999-1 [3] apply.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TS 103 666-1 [1], ETSI TS 103 999-1 [3] and the following apply:

AA   Accessor Authentication
FFS   For Further Study
RDE   Router Data Extractor
TT   Test Tool
TTI   Tests Tool Interface

3.4 Formats

3.4.1 Format of the requirements tables

The columns in the requirement tables in clause 5 have the following meaning.

Column	Meaning

Req.ID	This column shows the ordinal term assigned to a requirement identified in the referenced specification. The following syntax has been used to define the unique R(equirement) terms:
	R<n><XX><YY>_<ZZZ>
	n: Identification letter for the referenced specification
	   Q: ETSI TS 103 666-1 [1]
	   R: ETSI TS 103 666-2 [2]
	   S: ETSI TS 103 999-1 [3]
	   T: GlobalPlatform, Virtual Primary Platform [5]
	   U: ETSI TS 103 834-1 [7]
	XX: Main clause of the core specification in which the requirement is listed.
	YY: Subclause of the main clause in the core specification in which the requirement is listed.
	ZZZ: Continuously increasing number starting with '001'.

Clause	The "Clause" column helps to identify the location of a requirement by listing the clause hierarchy down to the subclause the requirement is located in.
Release	An optional column that is used if the listed requirement is valid for a specific release or a specific range of releases only, up to a specific release, or from a specific release onwards.
Description	In this column the requirement text is shown. Where the text can either be a copy of the original requirement, or a text analogous to the requirement text (e.g. if the requirement text is descriptive and can be shortened or truncated).

3.4.2 Numbers and Strings

The conventions used for decimal numbers, binary numbers and strings are listed in table 3.1.

Table 3.1: Convention of Numbering and Strings

Convention	Description
nnnnn	A decimal number, e.g. PIN value or phone number
'b'	A single digit binary number
'bbbbbbbb'	An 8-bit binary number
'hh'	A single octet hexadecimal number
'hh hh…hh'	A multi-octet hexadecimal number or string
"SSSS"	A character string
NOTE:	If an 'X' is present in a binary or hexadecimal number, then the digit might have any allowed value. This 'X' value does not need to be interpreted within the particular coding shown.

3.4.3 Format of test description clauses

In general clauses with test descriptions use the following basic format:

X.Y.   Group of test descriptions for a particular topic

X.Y.1   Configurations

This header is to be used in every clause that includes configuration descriptions. It may be followed by a sentence explaining that there are no specific configurations required for this particular topic or:

X.Y.1.1   C<aaa>_<nnn> <optional>

Where each sub-header of a required configuration is built from a leading 'C' followed by <aaa>, a minimum three-digit abbreviation for the configuration description group, an underscore and <nnn>, a minimum three-digit number to identify the configuration. This sub-header may include explanatory text following the identification.

Whenever a configuration exists it is presented in a table of the following format:

Configuration ID	C<aaa>_<nnn>
Configuration description	

Configuration description shall show a drawing representing the entities involved and the connections available between instances. It shall not include explanatory text.
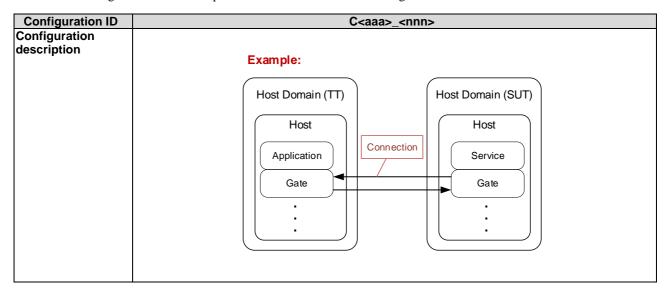
X.Y.2 Procedures

This header is to be used in every clause that includes procedure descriptions. It may be followed by a sentence explaining that there are no specific procedures required for this particular topic or:

X.Y.2.1 P<aaa>_<nnn> <optional>

Where each sub-header of a required procedure is built from a leading 'P' followed by <aaa>, a minimum three-digit abbreviation for the procedure description group, an underscore and <nnn>, a minimum three-digit number to identify the procedure. This sub-header may include explanatory text following the identification.

Whenever a procedure exists it is presented in a table of the following format:

Procedure ID	P<aaa>_<nnn>	
Procedure objectives	Description of the procedure objectives.	
Configuration reference	C<aaa>_<nnn> See note 1	
Initial conditions		
Text and/or list of procedure IDs identifying the initial conditions that need to be fulfilled before the procedure sequence defined in this table can be executed. See note 2.		
Procedure sequence		
Step	**Description**	
1	Description of procedure step #1	
…	…	
n	Description of procedure step #n	
NOTE 1: Reference to the appropriate configuration. NOTE 2: Procedure IDs can be referenced if the integration of existing procedure sequences can avoid required procedure steps duplication to achieve the initial conditions. Referenced procedures are intended to be executed in given order.		

Procedures are sequences that shall be executed to prepare specific initial conditions for a test. As such they shall not include verifications of any requirements.

X.Y.3 Test descriptions

This header is to be used for every clause that includes test descriptions. It may be followed by:

X.Y.3.1 <aaa>_<nnn> <optional>

Where each sub-header of a test description is built from <aaa>, a minimum three-digit abbreviation for the test description group, an underscore and <nnn>, a minimum three-digit number to identify the test description. This sub-header may include explanatory text following the identification.

Whenever a test description exists it is presented in a table of the following format:

Test ID	<aaa>_<nnn>	
Test objectives	Description of the test objectives. See note 1	
Configuration reference	C<aaa>_<nnn> See note 2	
Initial conditions		
Text and/or list of procedure IDs identifying the initial conditions that need to be fulfilled before the test sequence defined in this table can be executed. See note 3.		
Test sequence		
Step	Description	Req.ID
1	Description of test step #1	
…	…	RQ<XX><YY>_<ZZZ>
n	Description of test step #n	
NOTE 1: The descriptions should reflect the objectives of the requirements verified. NOTE 2: Reference to the appropriate configuration NOTE 3: If possible the initial conditions for the test sequence shall be defined by existing procedures. Referenced procedures are intended to be executed in given order.		

Requirement IDs listed in the Req.ID are references to the requirements listed in clause 5 of the present document. A requirement listed in the test sequence is handled as verified if the response related to the listed requirement has the expected contents. Req.IDs shall always be assigned to a response step.

If there are no test descriptions defined for a group of tests, but related requirements are available, an appropriate clause shall inform about the status of the requirements. E.g.

X.Y.3.Z Requirements not testable, implicitly verified or verified elsewhere

The header of this clause shall be adjusted depending on which condition applies for the identified requirements.

Example text for requirements referenced from a different standardization body:

The following requirements identified in <XYZ> are not tested in accordance to the present document, as they are referencing requirements from a different standardization body (<NAME>): <XX><YY>_<ZZZ>, …

Example text for requirements implicitly tested:

The following requirements identified in <XYZ> are generated from descriptive text. An explicit verification is not possible but with correct execution of the related function the requirements can be handled as implicitly verified: <XX><YY>_<ZZZ>, …

Example text for requirements not tested:

The following requirements identified in <XYZ> are either generated from descriptive text or not testable in the defined test environment. A verification of the listed requirements is not possible: <XX><YY>_<ZZZ>, …

The clause with explanatory text for the untested or implicitly tested requirements shall always be the last clause in the Test description clause. Nevertheless, it can be provided as the first clause if no executable test sequences are defined.

The hierarchy given in this example structure is not fixed. If building sub-groups is useful this may be done on any level of the test description hierarchy. Furthermore, it is not required to generate sub-groups for all the three main sections (Configurations, Procedures, Test descriptions) if adding a sub-group is useful in any of these sections.

E.g. common configurations on hierarchy level 3, common procedures on hierarchy level 3 but subgroups for the test descriptions with a new group header on level 4 and the test descriptions on level 5.

3.4.4 Dynamic content validation in ASN.1 structure

In certain test cases a dynamic content returned by the DUT (e.g. value within ASN.1 structure, signature, integer, …) is processed according to the following textX grammar:

```
operations ::= '<' operation ( logical_operator operation)* '>'

operation ::=  operation_Identifier ' (' variable_identifier (',' parameter)* ')'

operation_identifier ::= 'STORE'|'REPLACE'|'COMPARE'|'ISFIELDNOTEXIST'

logical_operator  ::= 'AND'|'OR'|'XOR'

variable_identifier ::=([A-Z]|[a-z])+[0-9]*
```

where:

- Operation_identifier: is the identifier identifying the operation to perform on a dynamic content of aFieldName as:

    - STORE: store the dynamic content of a aFieldName into a test tool variable identified by a variable identifier.

    - REPLACE: retrieve a variable identified by Variable_identifier and replace the content of aFieldName by the content of the variable.

    - COMPARE: compare the content of aFieldName with the content of a variable and return True or False to the test tool. This operator requires one or more additional parameters. The parameters may be combined for ORing them. The parameters are as follow:

        ▪ GT: the content of the aFieldName shall be strictly greater than the content of a variable.

        ▪ LS: the content of the aFieldName shall be strictly less than the content of a variable.

        ▪ EQ: the content of the aFieldName shall be equal to the content of a variable.

        ▪ DIF: the content of the aFieldName shall be different from the content of a variable.

    - ISFIELDNOTEXIST: return true, if aFieldName field does not exist.

- Variable_identifier: variable identifier managed by the test tool. The variable identifier shall consist only of a set of alphanumeric characters.

The operations are inserted within a comment associated to a field as follow:

```
aFieldName … /* operations */
```

EXAMPLE:

```
  aParameter {
    aVersion '0000'H /*<COMPARE(TCSVERSION,GT,EQ)>*/where
aTCSVERSION INTEGER ::= 10 /*<STORE(TCSVERSION)>
```

4 Requirements for the TTI

4.0 Introduction

As the TTI shall be usable in test environments as defined in ETSI TS 103 999-1 [3], requirements from various specifications shall be considered. Requirements listed in the following clauses are derived from:

- ETSI TS 103 666-1 [1],

- ETSI TS103 666-2 [2]

- ETSI TS 103 999-1 [3],

- GlobalPlatform, Technology, Virtual Primary Platform [5].

- ETSI TS 103 834-1 [7].

NOTE: To avoid ambiguities in requirements derived from the GlobalPlatform - Virtual Primary Platform [5] specification, the requirement tables use normative text rather than the reference as in the underlying ETSI specification(s).

4.1 Requirements from ETSI TS 103 666-1

4.1.1 Accessor authentication

Reference: ETSI TS 103 666-1 [1], clause 6.13.

RQ number	Clause	Description
6.13.1 Overview		
RQ0613_001	6.13.1	For the accessor authentication service in the TTI Host in general the accessor authentication service requirements listed in ETSI TS 103 999-1 [3], clause 5.2.13 apply.

4.1.2 Protocol layers

Reference: ETSI TS 103 666-1 [1], clause 8.3.

RQ number	Clause	Description
8.3.1 Overview		
RQ0803_001	8.3.1	The MTU shall be 20 bytes or greater.
RQ0803_002	8.3.1	For proper operation, the protocol stack underlying the SCL shall provide a means for managing the underlying flow control.
RQ0803_003	8.3.1	There shall be an optional means for controlling (e.g. activating, deactivating) the underlying protocols.
RQ0803_004	8.3.1	There shall be an optional means for getting the notifications from an underlying protocol (e.g. activation/deactivation of the interface by the terminal).
8.3.2 Network layer		
RQ0803_005	8.3.2	The TTI shall support the exchange of VPN packets as defined in GlobalPlatform, Virtual Primary Platform - Network Protocol [5], clause 4.3.1.
RQ0803_006	8.3.2	UUIDs as defined in GlobalPlatform, Virtual Primary Platform - Network Protocol [5], clause 3.3 shall be used as identifiers for Hosts, Gates and Host Domains to fulfil the requirements to a VPN packet as requested in clause 4.3.1 of [5].
8.3.3 Transport layer		
RQ0803_009	8.3.3	The TTI shall support the routing of HCP packets as defined in GlobalPlatform, Virtual Primary Platform - Network Protocol [5], clause 4.4.
RQ0803_010	8.3.3	For routing of HCP packets using static pipes within the destination host, pipes with pipe identifiers (P_{ID}) as defined in table 3-5 of GlobalPlatform, Virtual Primary Platform - Network Protocol [5] shall be used.
RQ0803_011	8.3.3	For routing of HCP packets using dynamic pipes within the destination host, pipes with pipe identifiers (P_{ID}) as defined in clause 5.5.3.2 of GlobalPlatform, Virtual Primary Platform - Network Protocol [5] shall be used.
RQ0803_012	8.3.3	Fragmentation and reassembly of messages larger than the MTU shall be possible as defined in ETSI TS 102 622 [6], clause 5.3.
RQ0803_013	8.3.3	Dedicated Protocol Accommodations as defined in clause 4.6 of GlobalPlatform, Virtual Primary Platform - Network Protocol [5] shall be supported.
8.3.4 Session layer		
RQ0803_014	8.3.4	The TTI shall support a session layer using pipe sessions as defined in GlobalPlatform, Virtual Primary Platform - Network Protocol [5], clause 3.10.
RQ0803_015	8.3.4	The TTI shall be capable to execute a successful pipe binding operation to open a pipe session as defined in GlobalPlatform, Virtual Primary Platform - Network Protocol [5], clause 5.5.3.2.
RQ0803_016	8.3.4	The TTI shall be capable to explicitly close a pipe session as defined in GlobalPlatform, Virtual Primary Platform - Network Protocol [5], clauses 5.5.3.3 and 3.10.3.