ETSI TS 103 457 V1.1.1 (2018-10)

CYBER;
Trusted Cross-Domain Interface:
Interface to offload sensitive functions to a trusted domain

Reference
DTS/CYBER-0019

Keywords
cybersecurity, interface

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 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

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 only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

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

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is 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 IPR Policy, no investigation, 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.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Cyber Security (CYBER).

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.

Introduction

Deploying hosted sensitive functions in modern virtualized IT infrastructure is still a concern and a major issue.

The main threats are malicious administrators operating the IT infrastructure including: network, storage and host platform facilities and virtualization management. These threats and related issues are thoroughly discussed in ETSI TR 103 308 [i.1].

ETSI specification group NFV SEC is in charge of defining a secured standard architecture. Proprietary solutions providing trusted security for virtualized environments have started emerging.

These new envisioned architectures add security components at the hosting platform level and into centralized services in charge of security management. The key concept is Hardware Root of Trust to get strong guarantees on the integrity of the deployed elements. These architectures offer secured managed infrastructures that enable deployment, live migration of encrypted VMs.

In addition to these works, the present document proposes a new interoperable interface that should help building sensitive services with trust.

This interface applies in the setting where two trust domains (see ETSI GS NFV-SEC 013 [i.4] for details) are defined:

- The More Trusted Domain (MTD) contains resources (network, storage, processing) where sensitive functions can be offloaded.

- The Less Trusted Domain (LTD) contains resources that can be managed without the risk of compromising sensitive information, since these functionalities are offloaded to the MTD.

This Trusted Cross-Domain interface includes a set of basic functions called by the LTD entity but performed securely within the MTD. This set of basic functions enables the LTD entity to build more complex services.

1 Scope

The present document specifies a high-level service-oriented interface, as an application layer with a set of mandatory functions, to access secured services provided by, and executed in a More Trusted Domain. The transport layer is out of scope and left to the architecture implementation.

This interface is not considered as a replacement of the already existing technologies (such as PKCS#11, KMIP, etc.) but rather operating on top of these.

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.

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.

Not applicable.

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.

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] ETSI TR 103 308: "CYBER; Security baseline regarding LI and RD for NFV and related platforms".

[i.2] ETSI GR NFV-SEC 011: "Network Functions Virtualisation (NFV); Security; Report on NFV LI Architecture".

[i.3] Wikipedia definition of Type-Length-Value.

[i.4] ETSI GS NFV-SEC 013: "Network Functions Virtualisation (NFV) Release 3; Security ; Security Management and Monitoring specification".

3 Definition of terms and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

domain: set of domain services

trusted cross domain interface: domain service with a set of dedicated domain interface functions for communication between domain services of different domains (inter-domain communication)

trusted cross domain interface function: function of a domain interface which is implemented by a domain service of another domain in order to realize inter-domain communication

trusted cross domain object: data generated by a domain service

trusted cross domain service: service with a set of dedicated domain service functions for communication with other domain services of the same domain (intra-domain communication)

trusted cross domain service function: function of a domain service which is implemented by the same or another domain service in order to realize intra-domain communication

trusted cross secured domain interface: domain interface offering access to secured domain services

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AC	Access Control
AES	Advanced Encryption Standard
CN	Common Name
FW	FireWall
HSM	Hardware Security Module
IT	Information Technology
KMIP	Key Management Interoperability Protocol
LI	Lawful Interception
LTD	Less Trusted Domain
MF	Mediation Function
MTD	More Trusted Domain
NFV	Network Function Virtualization
PNRG	Pseudorandom Number Generator
RNG	Random Number Generator
RSA	Rivest-Shamir-Adleman
SEC	Security
TCDI	Trusted Cross-Domain Interface
TCF	Triggering Control Function
TCO	Trusted COntext
TLS	Transport Layer Security
TPM	Trusted Platform Module
TTLV	Tag-Type-Length-Value encoding
VM	Virtual Machine
VMM	Virtual Machine Manager
vPOI	virtual Point Of Interception

4 General

4.1 TCDI functional requirements

TCDI provides services to the application layer. MTD implements, exposes and delivers the required services.

TCDI provides the following high-level services:

- Key Management: TCDI allows symmetric and asymmetric keys to be requested and received.
- Cryptographic operations: TCDI allows basic cryptographic operation to be performed in the MTD.

EXAMPLE: Random number generator.

- File/Database/Storage access: TCDI provides services to append, push and store sensitive data in containers such as files or database.

TCDI shall allow the use of sensitive objects in several functions without regeneration and compromise.

TCDI shall allow the sharing of MTD domain objects by LTD entities.

A LTD entity shall provide attestations on demand to the MTD, and the MTD shall verify those attestations to ensure the trust relation between the domains.

TCDI shall allow cascading the execution of domain service functions of the LTD on domain objects of the MTD within a single session.

4.2 TCDI life cycle

4.2.1 Life cycle Diagram

The interface allows a LTD entity to establish a trusted connection to a server in the MTD to execute sensitive operations and compose results within a TCO guaranteed by the MTD server (illustrated in figure 1). Only one connection per LTD entity shall be accepted.

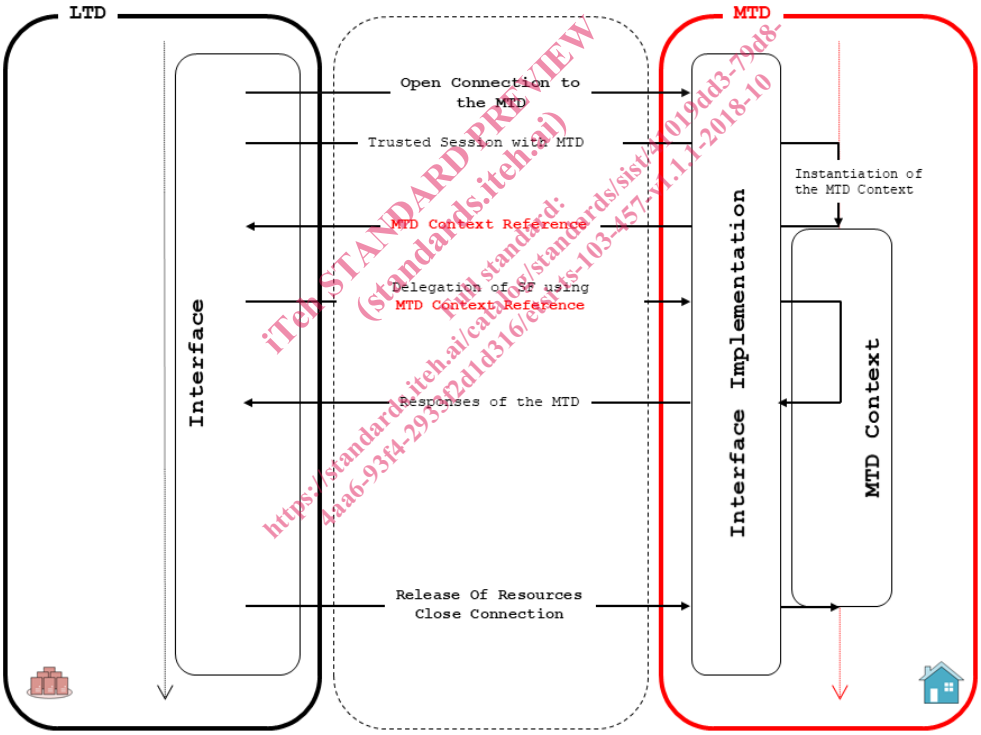

Figure 1: Interface Life Cycle

4.2.2 Connection between LTD and MTD

The use of TCDI is initiated by one LTD with the establishment of a connection to one MTD service. The MTD may close the connection after some period of inactivity (see Good Practice section for recommendations).

The MTD shall support two modes of operation depending on the LTD trust level:

- Trusted mode enables the MTD to verify that the LTD is running in an authorized environment (see Good Practice section for recommendations).
- Untrusted hardware mode enables the use of TCDI when the LTD does not have access to a TPM.

The MTD shall have a database of authorized RSA key pairs and the LTD shall be able to sign data as a TPM would.

MTD is responsible for granting the appropriate level of services available to a LTD connection depending on the trust level and the requested LTD-Role. MTD shall deny connections if the requested LTD-Role does not match the trust level.

MTD shall accept only one connection per LTD, and simultaneous connections from multiple LTD. New connections to the MTD shall get rejected if the supported limit of simultaneous connections is reached.

4.2.3 Session

A session describes a set of transactions between the LTD and MTD for which an ephemeral TCO is created to secure all the sensitive data generated or managed, either simple objects or containers.

The MTD generates and associates a unique identifier to sensitive data and guarantees their unicity:

- Session-Id to each session.
- Object-Id to each object.
- Container-Id to each container.

Session creation within an existing session returns an error.

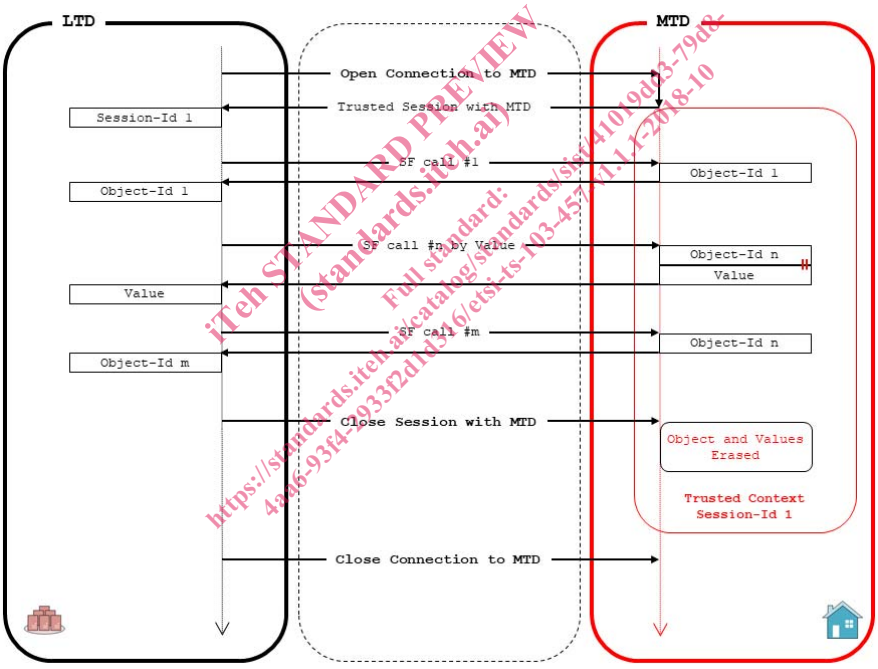

Figure 2: Session based calls to sensitive functions

4.2.4 Keep the trusted connection between the LTD and the MTD

Depending on the deployment scenario, the MTD may have different requirements for the acceptable interval between re-attestations. The MTD may take different actions depending on the attestation state of the LTD.

EXAMPLE: The MTD can give access to certain resources only when certain pre-conditions are met by an LTD attestation.

The LTD manages its connection's lifetime by renewing the trust connection.

Upon expired connection, the MTD terminates the current session with the LTD entity.

If the MTD ends a session and connection because of expired connection's lifetime, the LTD shall set up a new connection and a new session to re-start the delegation of sensitive functions.

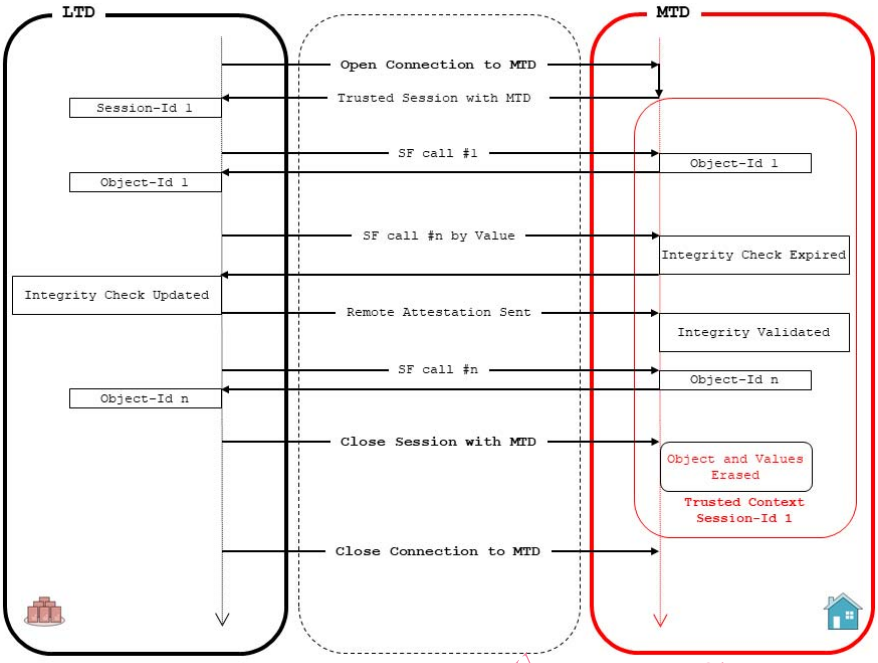

Figure 3: Attestation Check Success

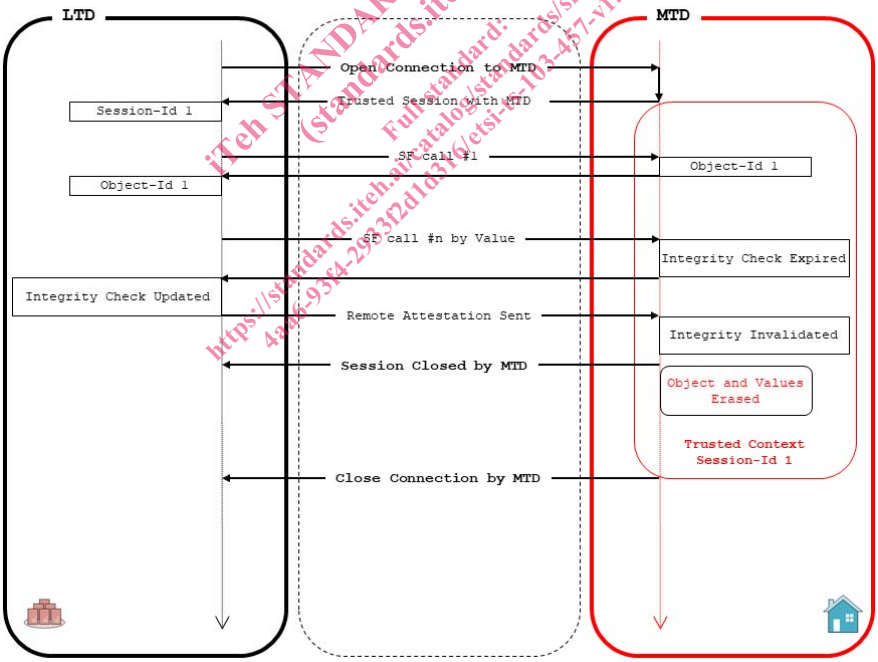

Figure 4: Attestation Check Failure

4.2.5 Releasing and erasing

When a LTD entity has finished offloading SFs or decides to request the erasing of the trusted context, the LTD entity may close the current session.

The MTD shall securely erase the trusted context of the session upon closure initiated by the LTD entity or when the connection's lifetime expires.

5 Interface Elementary Functions

5.1 General provisions

Elementary functions are achieved using simple communication command/response pattern where the MTD executes and returns response on the solicitation of the LTD entity.

Responses have the form of an optional result data value or a reference Object-id to that value and a status error code of the operation.

Every function runs inside a TCO initiated by a session.

Each function waits a synchronous response; therefore, functions shall be called sequentially.

Results may be void in the response message in case of error.

Protocol messages are composed of a one-byte message identifier, followed by a sequence of TTLV encoded parameters.

As described in [i.3], variable length typed element of information is binary encoded into 4 concatenated parts:

- Tag, 1 byte, used as a symbolic type for the element.
- Type, 2 bytes, used as the practical type of encoding.
- Length, 4 bytes.
- Value, variable sized information.

Several literal types, such as integer, Unicode or binary string, or symbolic constant are used for simple information. Some composed types such as DBKeyValue pairs are used for more structured information.

The complete list of Message identifiers is defined in clause 6.1. The list of Tags and Types for TTLV is defined in clauses 6.2 and 6.3.

For each message command and response defined in clauses 5.2 to 5.6, message parameters are defined in tables. In the column "status" the abbreviations have the following meaning:

M: Mandatory.
The parameter shall be present.

R: Recommended.
The parameter should be present.

O: Optional.
The parameter may be present.

C: Conditional.
The parameter shall be present when the defined conditions are met.

The description of and common provisions for message parameters are defined in clauses 6.3 and 6.4.

5.2 Connection and session management

5.2.1 General

The MTD is responsible of storing a configuration of database type for LTD entities based on their LTD-Role. A Container-Id reference to the configuration of the MTD is returned at connection opening. The configuration shall be read-only.