

# ETSI TS 103 457 V1.2.1 (2023-03)



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

[ETSI TS 103 457 V1.2.1 \(2023-03\)](https://standards.iteh.ai/catalog/standards/sist/885ec5d6-4766-4a3e-a253-d6b709300c2c/etsi-ts-103-457-v1-2-1-2023-03)

<https://standards.iteh.ai/catalog/standards/sist/885ec5d6-4766-4a3e-a253-d6b709300c2c/etsi-ts-103-457-v1-2-1-2023-03>

---

**Reference**

---

RTS/CYBER-0088

---

---

**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 - 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](http://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://standards-portal.etsi.org/standards-search> <https://portal.etsi.org/People/CommitteeSupportStaff.aspx> [4a3e-a253-standards@etsi.org](mailto:4a3e-a253-standards@etsi.org)

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**

---

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2023.  
All rights reserved.

# Contents

Intellectual Property Rights .....	6
Foreword.....	6
Modal verbs terminology.....	6
Introduction .....	6
1 Scope .....	8
2 References .....	8
2.1 Normative references .....	8
2.2 Informative references.....	8
3 Definition of terms, symbols and abbreviations.....	9
3.1 Terms.....	9
3.2 Symbols.....	9
3.3 Abbreviations .....	9
4 General .....	10
4.1 TCDI functional requirements.....	10
4.2 TCDI life cycle.....	10
4.2.1 Life cycle Diagram .....	10
4.2.2 Connection between LTD and MTD .....	11
4.2.3 Session .....	11
4.2.4 Keep the trusted connection between the LTD and the MTD.....	12
4.2.5 Releasing and erasing .....	14
5 Interface Elementary Functions.....	14
5.1 General provisions.....	14
5.2 Connection and session management .....	15
5.2.1 General.....	15
5.2.2 TD_OpenConnection .....	15
5.2.3 TD_CloseConnection.....	15
5.2.4 TD_CreateSession .....	16
5.2.5 TD_CloseSession.....	16
5.2.6 TD_TrustRenewal.....	16
5.3 Data and value management.....	17
5.3.1 TD_CreateObject.....	17
5.3.2 TD_GetObjectValue .....	17
5.3.3 TD_PutObjectValue.....	18
5.4 Transferring cryptographic functionality.....	18
5.4.1 Entropy request.....	18
5.4.1.1 General .....	18
5.4.1.2 TD_GetRandom .....	19
5.4.2 Encryption keys request.....	19
5.4.2.1 General .....	19
5.4.2.2 TD_GenerateEncryptionKey.....	19
5.4.3 Trusted timestamping .....	20
5.4.3.1 General .....	20
5.4.3.2 TD_GetTrustedTimestamping .....	20
5.4.4 Secure archive.....	20
5.4.4.1 General .....	20
5.4.4.2 TD_CreateArchive .....	21
5.4.4.3 TD_Archive .....	21
5.4.4.4 TD_CloseArchive .....	22
5.4.5 Secure storage.....	22
5.4.5.1 General .....	22
5.4.5.2 TD_CreateStorage.....	22
5.4.5.3 TD_DeleteStorage.....	23
5.4.5.4 TD_StoreData .....	23

5.4.5.5	TD_GetStorageValue .....	24
5.6	Search capabilities .....	24
5.6.1	Container search .....	24
5.6.1.1	General .....	24
5.6.1.2	TD_GetStorage .....	25
5.6.1.3	TD_Search .....	25
6	Encoding.....	26
6.1	Message identifiers.....	26
6.2	Type (TTLV) codes.....	27
6.3	Tag (TTLV) codes.....	27
6.4	Status Codes .....	28
<b>Annex A (informative):</b>	<b>Use Cases .....</b>	<b>30</b>
A.1	Entropy request scenario .....	30
A.1.1	Description .....	30
A.1.2	Example.....	30
A.2	Encrypted Virtual Machine use case (including LTD execution environment check).....	31
A.2.1	Description .....	31
A.2.2	Example.....	32
A.2.2.1	Introduction.....	32
A.2.2.2	Successful case .....	32
A.2.2.3	Failure case .....	33
A.3	Secure archive use case .....	33
A.3.1	Description .....	33
A.3.2	Example.....	34
A.4	Secure query use case.....	36
A.4.1	Description .....	36
A.4.2	Example.....	36
A.5	Secure Storage use case.....	37
A.5.1	Description .....	37
A.5.2	Example.....	38
A.6	Authentication use case .....	40
A.6.1	Description .....	40
A.6.2	Example.....	40
A.7	Lawful intercept use case .....	41
A.7.1	Description .....	41
A.7.2	Example.....	41
A.8	NFV sec use case.....	42
A.8.1	Description .....	42
A.8.2	Example.....	43
<b>Annex B (informative):</b>	<b>Guidelines .....</b>	<b>45</b>
B.1	Implementation guidelines .....	45
B.1.1	Global architecture .....	45
B.1.2	Connection management .....	45
B.1.3	Void.....	45
B.2	Good practice .....	45
B.3	TTLV encoding examples .....	46
B.3.1	GetRandom.....	46
B.3.2	StoreData.....	46
<b>Annex C (informative):</b>	<b>Bibliography.....</b>	<b>47</b>
<b>Annex D (informative):</b>	<b>Example implementation and demonstrator.....</b>	<b>48</b>

History .....	49
---------------	----

## iTeh STANDARD PREVIEW (standards.iteh.ai)

ETSI TS 103 457 V1.2.1 (2023-03)

<https://standards.iteh.ai/catalog/standards/sist/885ec5d6-4766-4a3e-a253-d6b709300c2c/etsi-ts-103-457-v1-2-1-2023-03>

# 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 Cyber Security (CYBER).

An example implementation and demonstrator is available in Annex D.

# 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 Industry 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.

iTeh STANDARD PREVIEW  
(standards.iteh.ai)

ETSI TS 103 457 V1.2.1 (2023-03)

<https://standards.iteh.ai/catalog/standards/sist/885ec5d6-4766-4a3e-a253-d6b709300c2c/etsi-ts-103-457-v1-2-1-2023-03>

---

# 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.

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

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, symbols 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 Symbols

Void.

### 3.3 Abbreviations

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

AC	Access Control
AES	Advanced Encryption Standard
CN	Common Name
FIPS	Federal Information Processing Standard
FW	FireWall
HSM	Hardware Security Module
IMSI	International Mobile Subscriber Identity
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
PKCS	Public Key Cryptography Standards
PRNG	Pseudo Random Number Generator
RNG	Random Number Generator
RSA	Rivest-Shamir-Adleman
SEC	Security
TCDI	Trusted Cross-Domain Interface
TCF	Triggering Control Function
TCG	Trusted Computing Group
TCO	Trusted COntext
TLS	Transport Layer Security
TPM	Trusted Platform Module
TTLV	Tag-Type-Length-Value encoding
UUID	Universaly Unique IDentifier

VM	Virtual Machine
VMM	Virtual Machine Manager
VNF	Virtual Network Function
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.

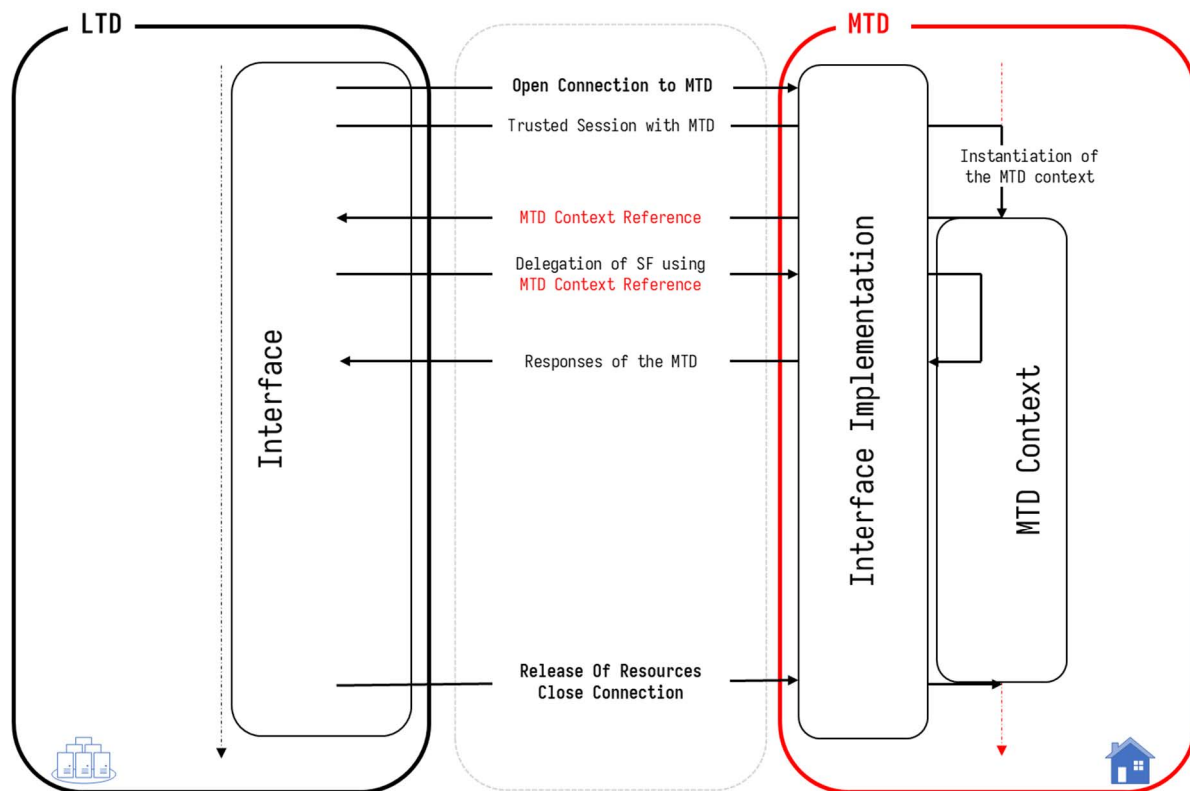


Figure 1: Interface Life Cycle

#### 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.

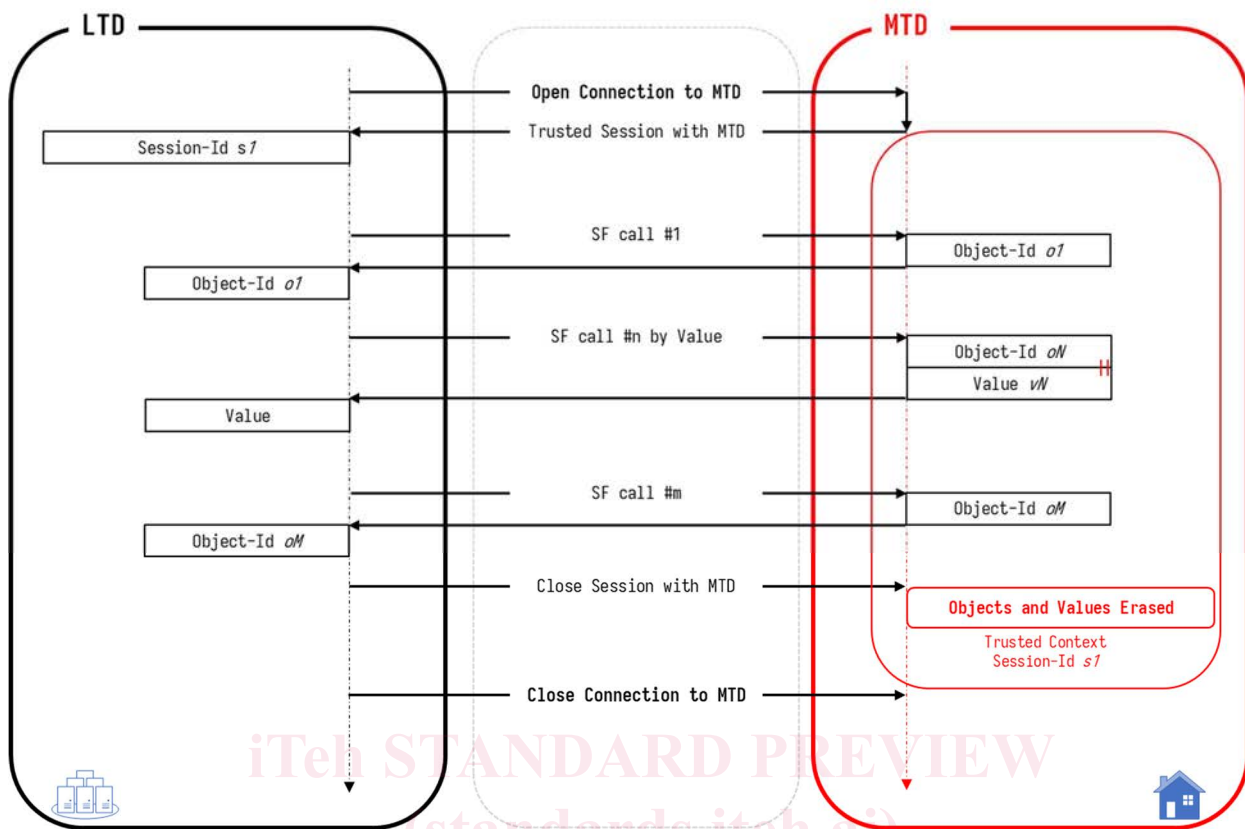


Figure 2: Session based calls to sensitive functions

#### 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.

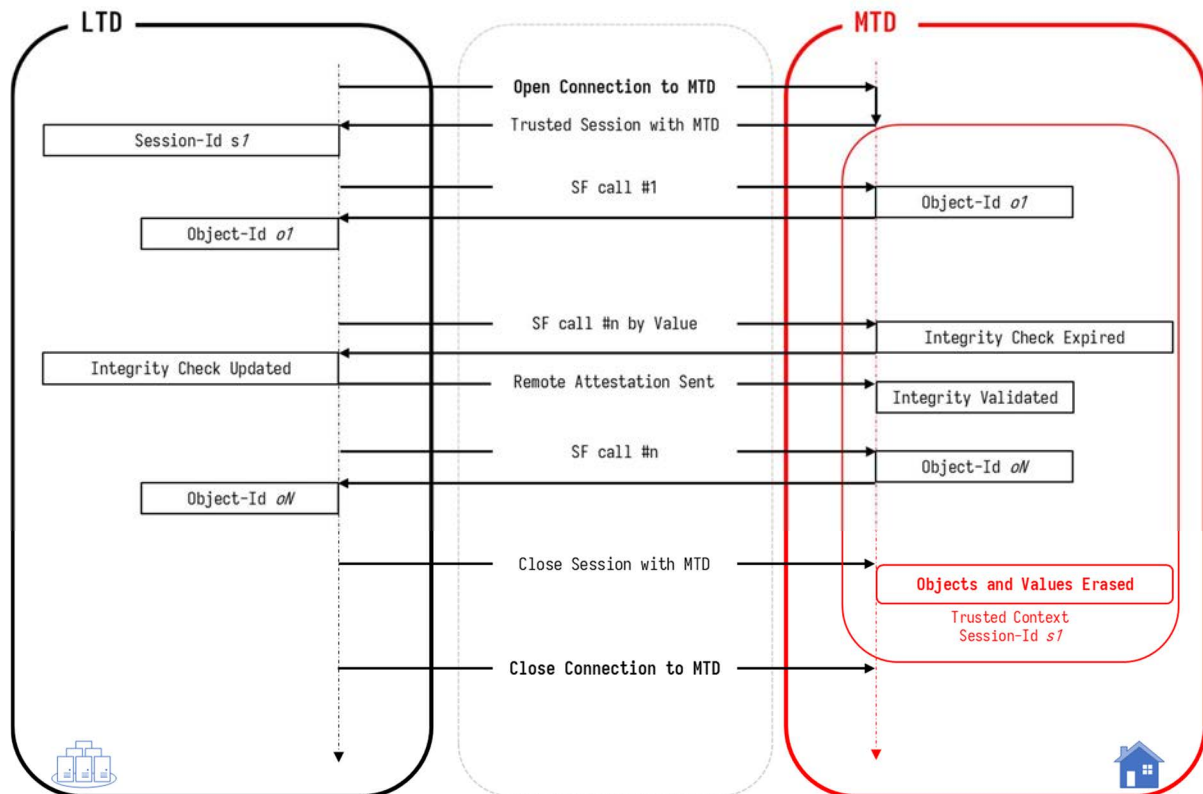


Figure 3: Attestation Check Success

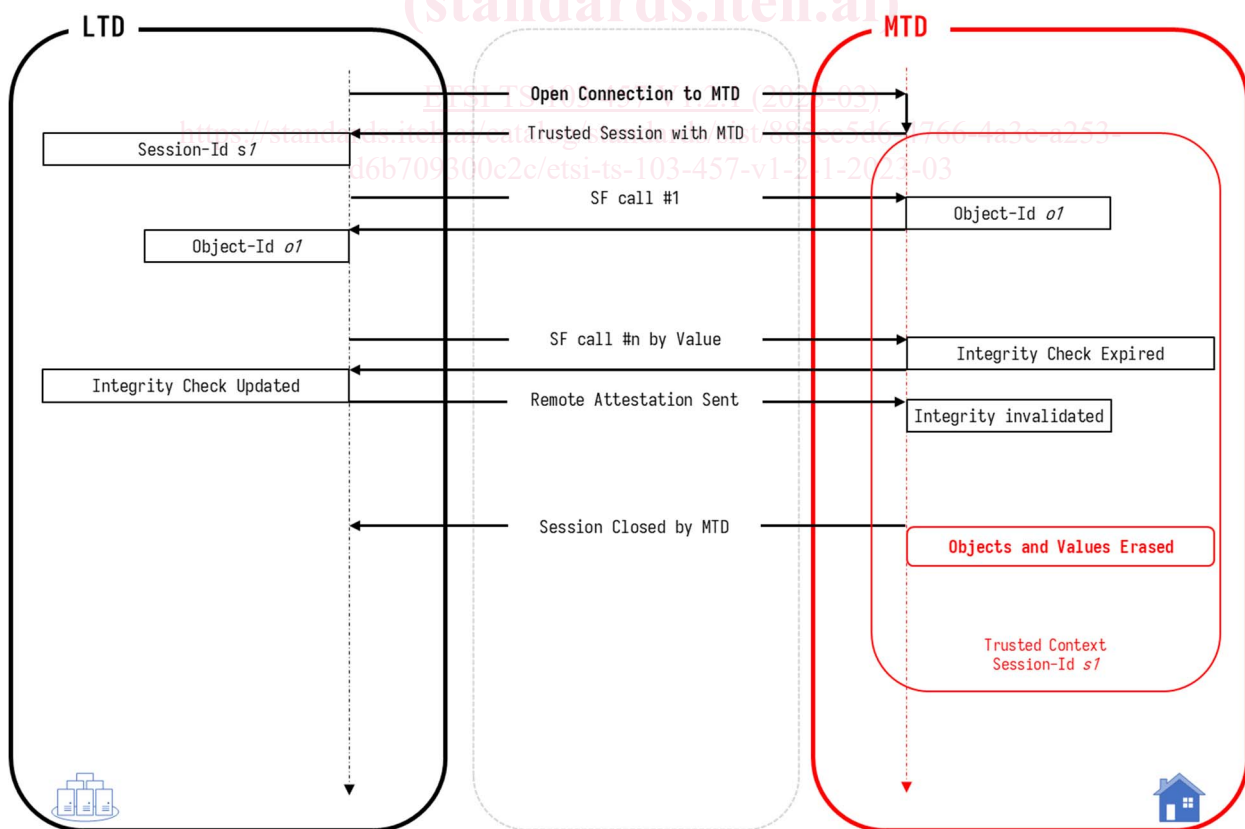


Figure 4: Attestation Check Failure