

# ETSI TS 103 646 V1.1.1 (2021-01)



## Methods for Testing and Specification (MTS); Test specification for foundational Security IoT-Profile (standards.iteh.ai)

[ETSI TS 103 646 V1.1.1 \(2021-01\)](https://standards.iteh.ai/catalog/standards/sist/676377a9-a728-4817-9c5c-ab403b6c00c2/etsi-ts-103-646-v1-1-1-2021-01)

<https://standards.iteh.ai/catalog/standards/sist/676377a9-a728-4817-9c5c-ab403b6c00c2/etsi-ts-103-646-v1-1-1-2021-01>



---

**Reference**DTS/MTS-TST8

---

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

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

**Important notice**

<https://standards.iteh.ai/catalog/standards/sist/676377a9-a728-4817-9c5c-ab4106910670/etsi-ts-103-646-v1-1-1-2021-01>  
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://portal.etsi.org/People/CommiteeSupportStaff.aspx>

---

**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 2021.  
All rights reserved.

**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.

# Contents

Intellectual Property Rights .....	4
Foreword.....	4
Modal verbs terminology.....	4
Introduction .....	4
1 Scope .....	5
2 References .....	5
2.1 Normative references .....	5
2.2 Informative references.....	6
3 Definition of terms, symbols and abbreviations.....	6
3.1 Terms.....	6
3.2 Symbols.....	6
3.3 Abbreviations .....	6
4 Test Suite Structure .....	7
4.1 Assumptions .....	7
4.2 Profile.....	7
5 Test Purposes for base security requirements .....	8
5.1 TP naming convention.....	8
5.2 List of TPs and mapping to functional areas and requirements as given in IEC 62443-4-2.....	9
5.3 Test strategy .....	11
5.4 TP catalogue.....	11
<b>Annex A (normative): TDL code for the Test Purposes .....</b>	<b>32</b>
History .....	33

[ETSI TS 103 646 V1.1.1 \(2021-01\)](https://standards.iteh.ai/catalog/standards/sist/676377a9-a728-4817-9c5c-ab403b6c00c2/etsi-ts-103-646-v1-1-1-2021-01)  
<https://standards.iteh.ai/catalog/standards/sist/676377a9-a728-4817-9c5c-ab403b6c00c2/etsi-ts-103-646-v1-1-1-2021-01>

---

## 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 Methods for Testing and Specification (MTS).

TECHNICAL STANDARD PREVIEW  
(standards.iteh.ai)

---

## Modal verbs terminology

ETSI TS 103 646 V1.1.1 (2021-01)

[https://standards.iteh.ai/catalog/standards/sist/676377a9-a728-4817-9c5c-](https://standards.iteh.ai/catalog/standards/sist/676377a9-a728-4817-9c5c-ab7936c69e22/etsi-ts-103-646-v1-1-1-2021-01)

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

The present document provides a test specification based on selected security requirements as known from IEC 6244-4-2 [1]. The chosen requirements have been collected by defining a dedicated IoT profile. The resulting IoT profile represents a generic minimum security level for IoT devices. Advanced requirements for higher security demands have been excluded.

The present document serves as reference for a test campaign addressing the foundational security requirements of the IoT-Profile. The standardized notation TDL-TO has been applied for the definition of test purposes as it supports a unified presentation and semantics.

---

# 1 Scope

The present document details test purposes to ensure a minimum security level for IoT devices. The underlying requirements are a subset of the IEC 62443-4-2 [1] standard containing functional security requirements for components. IEC 62443-4-2 [1] was initially started with the focus on Industrial Automation and Control systems. Due to its generic nature, the standard turned out to be applicable also to other domains. This is especially possible as the standard allows the application of defined subsets in terms of so-called profiles. Profiles were meant to adapt the set of requirements to particular domains beyond industrial automation and control systems. It resolves the mapping of requirements to one of the four security level. So, the selection is not bound to existing security level, which might be seen as profiles as well.

The IoT profile is a collection of those IEC 62443-4-2 [1] requirements that were seen foundational for any IoT device. Not fulfilling the IoT-profile-requirements does not mean that a device cannot be used at all. But it does mean, that the related risks need to be mitigated by other means. This applies especially to constrained devices with limited capabilities.

The starting point for the IoT profile were IEC 62443-4-2 [1] requirements mapped to the lowest security level SL1. As IoT devices are typically running standalone without any integration into a central management system, all requirements related to integration into a central management system have been excluded. This applies in especially to requirements related to:

- central account management integration;
- central event management;
- auditing.

The only requirements seen mandatory for all IoT devices although mapped to higher security level in IEC 62443-4-2 [1] relate to:

- software authenticity check (to prevent unauthorized software modifications); and
- session integrity (to prevent e.g. replay attacks).

**ITeH STANDARD PREVIEW**  
**(standards.iteh.ai)**  
ETSI TS 103 646 V1.1.1 (2021-01)  
<https://standards.iteh.ai/catalog/standards/sist/676377a9-a728-4817-9c5c-ab403b6c00c2/etsi-ts-103-646-v1-1-1-2021-01>

---

## 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.

- [1] IEC 62443-4-2: "Security for industrial automation and control systems. Technical security requirements for IACS components".
- [2] ETSI ES 203 119-4: "Methods for Testing and Specification (MTS); The Test Description Language (TDL); Part 4: Structured Test Objective Specification (Extension)".

## 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] ISO/IEC 9646-1: "Information technology -- Open Systems Interconnection -- Conformance testing methodology and framework -- Part 1: General concepts".
- [i.2] ETSI ES 202 951: "Methods for Testing and Specification (MTS); Model-Based Testing (MBT); Requirements for Modelling Notations".

---

## 3 Definition of terms, symbols and abbreviations

### 3.1 Terms

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

**Implementation Under Test (IUT)**: implementation of one or more Open Systems Interconnection (OSI) protocols in an adjacent user/provider relationship, being the part of a real open system, which is to be studied by testing

NOTE: See ISO/IEC 9646-1 [i.1].

**system under test**: real open system in which the implementation under test resides

NOTE: See ETSI ES 202 951 [i.2].

**test purpose**: non-formal high-level description of a test, mainly using text

### 3.2 Symbols

Void.

### 3.3 Abbreviations

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

BSI Federal Office for Information Security

NOTE: German: Bundesamt für Sicherheit in der Informationstechnik.

CR Component Requirement

DKE German Commission for Electrical, Electronic & Information Technologies of DIN and VDE

NOTE: German: Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE.

EDR Embedded Device Requirement

FR Foundational Requirement

HDR Host Device Requirement

ICMP Internet Control Message Protocol

IUT Implementation Under Test

NDR Network Device Requirement

NIST National Institute of Standards and Technology

PICS	Protocol Implementation Conformance Statement
RE	Requirement Enhancement
SAR	Software Application Requirement
SSH	Secure Shell
SUT	System Under Test
TDL	Test Description Language
TDL-TO	Test Description Language - Test Objectives
TLS	Transport Layer Security
TP	Test Purpose
TSS	Test Suite Structure

## 4 Test Suite Structure

### 4.1 Assumptions

The following assumptions have been taken:

- 1) Additionally, implemented functionality will not be considered in TPs, but will be tested:
  - a) Example: CR1.3 (account management).
  - b) IoT devices typically have only one local account.
  - c) therefore CR1.3 was excluded from the IoT profile.
  - d) In case multiple accounts are implemented, account management (disable/removal) needs to work.
- 2) CR1.10 (Authenticator feedback):
  - a) timing difference for error and no error response (as proposed by DKE) is omitted as not seen adequate for basic IoT requirements/tests.
- 3) CR7.1 (DoS):
  - a) TP to ensure recovery after DoS event is seen as functional test and thus not seen mandatory.

### 4.2 Profile

The test suite structure is closely related to requirements and requirement structure as detailed in IEC 62443-4-2 [1], which groups requirements and enhancements into seven Foundational Requirement (FR) areas.

The test suite covers those requirements, which have been considered as basic and are supposed to be fulfilled by any IoT device in a non-critical environment. This subset of requirements may be grouped in so called domain specific profiles. The standardization of an IoT-domain specific profile is out of scope of the present document. Nonetheless, the current proposal of covered requirements will be listed below and might be replaced by e.g. an IEC 62443-4-2 [1] IoT profile in future.

This basic IoT profile is meant to define an entry security level in especially for consumer IoT in a non-critical environment, but to be fulfilled by any IoT device. It may be superseded by other profiles in case a higher security level is demanded i.e. in an industrial environment. The basic IoT profile bases on requirements that are marked for the lowest Security Level (SL1) in IEC 62443-4-2 [1]. It excludes those requirements, which are considered not being applicable for standard IoT. Not considered requirements are e.g. those requirements that require integration into a network management system or are not feasible due to IoT typical limitations. This is why e.g. requirements related to auditing, centralized management, secure boot and DoS or malicious code protections have been excluded from this proposal:

- 1) FR 1 - Identification and authentication control
  - a) CR 1.1 Human user identification and authentication
  - b) CR 1.5 Authenticator management case a) use of initial authenticator

- c) CR 1.5 Authenticator management case b) recognition of changes to default authenticators
  - d) CR 1.5 Authenticator management case c) authenticator change
  - e) CR 1.5 Authenticator management case d) protect authenticators
  - f) CR 1.7 Strength of password-based authentication
  - g) CR 1.10 Authenticator feedback
  - h) CR 1.11 Unsuccessful login attempts
- 2) FR 2 - Use control
- a) CR 2.1 Authorization enforcement
  - b) CR 2.5 Session lock
- 3) FR 3 - System integrity
- a) CR 3.1 Communication integrity
  - b) CR 3.4 Software and information integrity
  - c) CR 3.5 Input validation
  - d) CR 3.7 Error handling
  - e) CR 3.8 Session integrity (case a))
- 4) FR 4 - Data confidentiality
- a) CR 4.1 Information confidentiality (case b))
  - b) CR 4.3 Use of cryptography
- 5) FR 7 - Resource availability
- a) CR 7.6 Network and security configuration settings
  - b) CR 7.7 Least functionality
- 6) Software application, embedded device, host device and network device requirements
- a) xDR - Case c) of the requirement Mobile code from [1]
  - b) xDR - Mobile code RE1
  - c) xDR - Support for updates

iTech STANDARD PREVIEW  
(standards.iteh.ai)

<https://standards.iteh.ai/catalog/standards/sist/676377a9-a728-4817-9c5c-ab403b6c00c2/etsi-ts-103-646-v1-1-1-2021-01>

ETSI TS 103 646 V1.1.1 (2021-01)

---

## 5 Test Purposes for base security requirements

### 5.1 TP naming convention

TPs are numbered, starting at 01, within each requirement ID that will be used like in the IEC 62443-4-2 standard [1]. The requirement IDs are organized according to the TSS. Some TPs may not have a requirement enhanced ID or may not be numbered.



Table 1: TP identifier naming convention scheme

Identifier: TP_<requirement ID>_<requirement number>_<requirement sub-number>_<req. enhanced ID>_<section name>_<number>		
TP	= Test Purpose	Fixed to "TP"
<requirement ID>	= Requirement ID in IEC 62443-4-2	"CR"   "SAR"   "EDR"   "HDR"   "NDR"   "xDR"
<requirement number>	= Requirement number in IEC 62443-4-2	Number with delimiter "_"
<requirement sub-number>	= Requirement sub-number in IEC 62443-4-2	Number with delimiter "_"
<req. enhanced ID>*	= Enhanced req. in IEC 62443-4-2	"RE" + Number with delimiter "_"
<section_name>	= Section name in IEC 62443-4-2	Name with delimiter "_"
<number>*	= Sequential number	Optional, from 01 to 99
*optional		

## 5.2 List of TPs and mapping to functional areas and requirements as given in IEC 62443-4-2

IEC 62443-4-2 [1] groups the Component Requirements (CR) and software related requirements (SAR, EDR, HDR, NDR) into Functional Requirement areas (FR). Each test purpose is mapped to such a requirement. The test purposes (marked *italic* below) follow the naming convention as described:

- 1) FR 1 - Identification and authentication control:
  - a) CR 1.1 Human user identification and authentication TPs:
    - i) TP\_CR\_1\_1\_Identification\_authentication\_1
    - ii) TP\_CR\_1\_1\_Identification\_authentication\_2
    - iii) TP\_CR\_1\_1\_Identification\_authentication\_3
    - iv) TP\_CR\_1\_1\_Identification\_authentication\_4
  - b) CR 1.5 Authenticator management case a) use of initial authenticator TP:
    - i) TP\_CR\_1\_5\_a\_Account\_Changeability
  - c) R 1.5 Authenticator management case b) recognition of changes to default authenticators TPs:
    - i) TP\_CR\_1\_5\_b\_Account\_Changeability\_1
    - ii) TP\_CR\_1\_5\_b\_Account\_Changeability\_2
  - d) CR 1.5 Authenticator management case c) authenticator change TPs:
    - i) TP\_CR\_1\_5\_c\_Account\_Changeability\_1
    - ii) TP\_CR\_1\_5\_c\_Account\_Changeability\_2
  - e) CR 1.5 Authenticator management case d) protect authenticators:
    - i) % (TP for CR 1.5 d) covered by CR 4.1 b))
  - f) CR 1.7 Strength of password-based authentication TP:
    - i) TP\_CR\_1\_7\_Strength\_of\_password\_based\_authentication
  - g) CR 1.10 Authenticator feedback TPs:
    - i) TP\_CR\_1\_10\_Authenticator\_feedback\_1

- ii) TP\_CR\_1\_10\_Authenticator\_feedback\_2
    - iii) TP\_CR\_1\_10\_Authenticator\_feedback\_3
  - h) CR 1.11 Unsuccessful login attempts TPs:
    - i) TP\_CR\_1\_11\_a\_Unsuccessful\_login\_attempts\_1
    - ii) TP\_CR\_1\_11\_b\_Unsuccessful\_login\_attempts\_1
- 2) FR 2 - Use control:
  - a) CR 2.1 Authorization enforcement TPs:
    - i) TP\_CR\_2\_1\_Authorization\_enforcement\_1
    - ii) TP\_CR\_2\_1\_Authorization\_enforcement\_2
    - iii) TP\_CR\_2\_1\_Authorization\_enforcement\_3
  - b) CR 2.5 Session lock:
    - i) TP\_CR\_2\_5\_a\_Session\_Lock\_1
    - ii) TP\_CR\_2\_5\_a\_Session\_Lock\_2
    - iii) TP\_CR\_2\_5\_b\_Session\_Lock\_3
- 3) FR 3 - System integrity:
  - a) CR 3.1 Communication integrity TP:
    - i) % (TP for CR 3.1 covered by TPs for CR 4.3 (use of cryptography))
  - b) CR 3.4 Software and information integrity TP:
    - i) % (Software integrity checks covered by TP\_xDR\_2\_4\_SAR\_2\_4\_Mobile\_code\_integrity\_check)
  - c) CR 3.5 Input validation TPs:
    - i) TP\_CR\_3\_5\_Input\_validation\_during\_session
    - ii) TP\_CR\_3\_5\_Input\_validation\_session\_establishment
  - d) CR 3.7 Error handling TP:
    - i) % (TP for CR 3.7 covered by TPs for CR 1.10)
  - e) CR 3.8 Session integrity (case a)) TP:
    - i) TP\_CR\_3\_8\_Session\_Integrity\_replay\_prevention
- 4) FR 4 - Data confidentiality:
  - a) CR 4.1 Information confidentiality (case b)) TPs:
    - i) TP\_CR\_4\_1\_b\_Information\_confidentiality\_in\_transit\_read\_direction\_TLS
    - ii) TP\_CR\_4\_1\_b\_Information\_confidentiality\_in\_transit\_write\_direction\_TLS
    - iii) TP\_CR\_4\_1\_b\_Information\_confidentiality\_in\_transit\_read\_direction\_SSH
  - b) CR 4.3 Use of cryptography TPs:
    - i) TP\_CR\_4\_3\_Use\_of\_cryptography\_IUT\_as\_TLS\_client
    - ii) TP\_CR\_4\_3\_Information\_confidentiality\_in\_transit\_IUT\_as\_TLS\_server\_with\_valid\_TLS\_capabilities

- iii) TP\_CR\_4\_3\_Information\_confidentiality\_in\_transit\_IUT\_as\_TLS\_server\_with\_invalid\_TLS\_version
  - iv) TP\_CR\_4\_3\_Information\_confidentiality\_in\_transit\_IUT\_as\_TLS\_server\_with\_invalid\_TLS\_ciphers
  - v) TP\_CR\_4\_3\_Use\_of\_cryptography\_IUT\_as\_SSH\_client
- 5) FR 7 - Resource availability:
- a) CR 7.6 Network and security configuration settings TP:
    - i) TP\_CR\_7\_6\_Network\_and\_security\_configuration\_settings
  - b) CR 7.7 Least functionality TPs:
    - i) TP\_CR\_7\_7\_Least\_functionality\_ping\_disabled
    - ii) TP\_CR\_7\_7\_Least\_functionality\_unused\_ports\_disabled
- 6) xDR - Mobile code case c) TP:
- i) TP\_xDR\_2\_4\_SAR\_2\_4\_Mobile\_code\_integrity\_check
- 7) xDR - Mobile code RE1 TP:
- i) TP\_xDR\_2\_4\_SAR\_2\_4\_Mobile\_code\_authenticity\_check
- 8) xDR - Support for updates:
- i) TP\_xDR\_3\_10\_Update\_support

iTech STANDARD PREVIEW  
(standards.iteh.ai)

### 5.3 Test strategy

ETSI TS 103 646 V1.1.1 (2021-01)

As the base IEC 62443-4-2 [1] contains no explicit strategies for testing, the TPs were generated as a result of analysis of the requirements taken from IEC standard 600c2/etsi-ts-103-646-v1-1-1-2021-01

### 5.4 TP catalogue

<b>TP Id</b>	TP_CR_1_1_Identification_authentication_1
<b>Test Objective</b>	Ensure the IUT identifies and authenticates users. Case invalid account identifier/invalid authenticator
<b>Reference</b>	IEC 62443-4-2 [1] CR 1.1, section 5.3.1
<b>PICS Selection</b>	
<b>Initial Conditions</b>	
with { the IUT being_in the initial_state }	
<b>Expected Behaviour</b>	
ensure that { when { // for each application level interface with sensitive data the IUT request the credentials and the Evaluator enter the credentials containing account identifier indicating value "invalid account identifier", account authenticator indicating value "invalid account authenticator"; } then { the IUT deny the access } }	
<b>Final Conditions</b>	

<b>TP Id</b>	TP_CR_1_1_Identification_authentication_2
<b>Test Objective</b>	Ensure the IUT identifies and authenticates users. Case valid account identifier/invalid authenticator
<b>Reference</b>	IEC 62443-4-2 [1] CR 1.1, section 5.3.1
<b>PICS Selection</b>	
<b>Initial Conditions</b>	
with { the IUT being_in the initial_state }	
<b>Expected Behaviour</b>	
ensure that { when { // for each application level interface with sensitive data the IUT request the credentials and the Evaluator enter the credentials containing account identifier indicating value "valid account identifier", account authenticator indicating value "invalid account authenticator"; } then { the IUT deny the access } }	
<b>Final Conditions</b>	

<b>TP Id</b>	TP_CR_1_1_Identification_authentication_3
<b>Test Objective</b>	Ensure the IUT identifies and authenticates users. Case invalid account identifier/valid authenticator
<b>Reference</b>	IEC 62443-4-2 [1] CR 1.1, section 5.3.1
<b>PICS Selection</b>	
<b>Initial Conditions</b>	
with { the IUT being_in the initial_state }	
<b>Expected Behaviour</b>	
ensure that { when { // for each application level interface with sensitive data the IUT request the credentials and the Evaluator enter the credentials containing account identifier indicating value "invalid account identifier", account authenticator indicating value "valid account authenticator"; } then { the IUT deny the access } }	
<b>Final Conditions</b>	

<b>TP Id</b>	TP_CR_1_1_Identification_authentication_4
<b>Test Objective</b>	Ensure the IUT identifies and authenticates users. Case valid account identifier/valid authenticator
<b>Reference</b>	IEC 62443-4-2 [1] CR 1.1, section 5.3.1
<b>PICS Selection</b>	
<b>Initial Conditions</b>	
with { the IUT being_in the initial_state }	
<b>Expected Behaviour</b>	
ensure that { when { // for each application level interface with sensitive data the IUT request the credentials and the Evaluator enter the credentials containing account identifier indicating value "valid account identifier", } }	