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

TECHNICAL SPECIFICATION

Methods for Testing and Specification (MTS); Test specification for foundational Security IoT-Profile

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

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

Copyright Notification

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 Methods for Testing and Specification (MTS).

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

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 in 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).

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 rRquirement
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 devide, 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

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

5.3 Test strategy

As the base IEC 62443-4-2 [1] contain no explicit strategies for testing. The TPs were generated as a result of analysis of the requirements taken from IEC standard.

5.4 TP catalogue

TP Id	TP_CR_1_1_Identification_authentication_1
Test Objective	Ensure the IUT identifies and authenticates users. Case invalid account identifier/invalid authenticator
Reference	IEC 62443-4-2 [1] CR 1.1, section 5.3.1
PICS Selection	
Initial Conditions	

with {
the IUT being_in the initial_state
}	

Expected Behaviour	

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
}
}	

Final Conditions	

TP Id	TP_CR_1_1_Identification_authentication_2
Test Objective	Ensure the IUT identifies and authenticates users. Case valid account identifier/invalid authenticator
Reference	IEC 62443-4-2 [1] CR 1.1, section 5.3.1
PICS Selection	
Initial Conditions	

with {
the IUT being_in the initial_state
}	

Expected Behaviour	

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
}
}	

Final Conditions	

TP Id	TP_CR_1_1_Identification_authentication_3
Test Objective	Ensure the IUT identifies and authenticates users. Case invalid account identifier/valid authenticator
Reference	IEC 62443-4-2 [1] CR 1.1, section 5.3.1
PICS Selection	
Initial Conditions	

with {
the IUT being_in the initial_state
}	

Expected Behaviour	

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
}
}	

Final Conditions	

TP Id	TP_CR_1_1_Identification_authentication_4
Test Objective	Ensure the IUT identifies and authenticates users. Case valid account identifier/valid authenticator
Reference	IEC 62443-4-2 [1] CR 1.1, section 5.3.1
PICS Selection	
Initial Conditions	

with {
the IUT being_in the initial_state
}	

Expected Behaviour	

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 "valid account authenticator";
}
then {
the IUT grant the access
}
}	

Final Conditions	

TP Id	TP_CR_1_5_a_Account_Changeability
Test Objective	The SUT shall provide capabilities to support the initial authenticator content.
Reference	Precondition for IEC 62443-4-2 [1] CR 1.5, section 5.7.1 a
PICS Selection	
Initial Conditions	

with {
the IUT being_in the original_factory_state and
the Manufacturer provide the initial_credentials containing
account identifier indicating value "initial account identifier",
account authenticator indicating value "initial account authenticator";
}	

Expected Behaviour	

ensure that {
when {
the Evaluator enter the initial_credentials
}
then {
the IUT grant the access
}
}	

Final Conditions	

TP Id	TP_CR_1_5_c_Account_Changeability_1
Test Objective	The SUT shall provide capabilities to function properly with authenticator change/refresh operation (accept valid authenticator).
Reference	Precondition for IEC 62443-4-2 [1] CR 1.5, section 5.7.1 c
PICS Selection	
Initial Conditions	

with {
the Evaluator establish the current_session
}	

Expected Behaviour	

ensure that {
when {
the Evaluator change the credentials containing
account authenticator indicating value "new valid account authenticator";
and the Evaluator close the current_session
and the Evaluator enter the changed_credentials containing
account identifier indicating value "valid account identifier",
account authenticator indicating value "new valid account authenticator";
(NOTE 1: "It is tried to authenticate with new account authenticator")
}
then {
the IUT grant an access token containing
credentials corresponding to the value of entered changed_credentials;
(NOTE 1: "The authentication with changed credentials is successful")
}
}	

Final Conditions	

TP Id	TP_CR_1_5_c_Account_Changeability_2
Test Objective	The SUT shall provide capabilities to function (reject invalid authenticator) properly with authenticator refresh operation.
Reference	Precondition for IEC 62443-4-2 [1] CR 1.5, section 5.7.1 c
PICS Selection	
Initial Conditions	

with {
the Evaluator establish the current_session
}	

Expected Behaviour	

ensure that {
when {
the Evaluator change the credentials containing
account identifier indicating value "valid account identifier",
account authenticator indicating value "new valid account authenticator";
and the Evaluator close the current_session
and the Evaluator enter the credentials containing
account identifier indicating value "valid account identifier",
account authenticator indicating value "valid account authenticator";
(NOTE 1: "The old credentials from initial credential list is used")
}
then {
the IUT deny the access
}
}	

Final Conditions	

TP Id	TP_CR_1_5_b_Account_Change_Recognition_1
Test Objective	The SUT shall support the recognition of changes to default authenticators made at installation time.
Reference	IEC 62443-4-2 [1] CR 1.5, section 5.7.1 b DKE conformance acceptance criteria
PICS Selection	PIC_initial_pw_change
Initial Conditions	

with {
the IUT being_in the original_factory_state and
the Manufacturer provide the initial_credentials containing
account identifier indicating value "initial account identifier",
account authenticator indicating value "initial account authenticator";
}	

Expected Behaviour	

ensure that {
when {
the Evaluator enter the initial_credentials
}
then {
the IUT request a password change
}
}	

Final Conditions	

TP Id	TP_CR_1_5_b_Account_Change_Recognition_2
Test Objective	The SUT shall support the recognition of changes to default authenticators made at installation time.
Reference	IEC 62443-4-2 [1] CR 1.5, section 5.7.1 b DKE conformance acceptance criteria
PICS Selection	PIC_initial_pw_warning
Initial Conditions	

with {
the IUT being_in the original_factory_state and
the Manufacturer provide the initial_credentials containing
account identifier indicating value "initial account identifier",
account authenticator indicating value "initial account authenticator";
}	

Expected Behaviour	

ensure that {
when {
the Evaluator enter the initial_credentials
}
then {
the IUT indicate a warning and
the IUT establish a session
}
}	

Final Conditions	

TP Id	TP_CR_1_7_Strenght_of_password_based_authentication
Test Objective	The SUT shall provide capabilities to enforce a minimum password length of 8.
Reference	IEC 62443-4-2 [1] CR 2.7, section 5.9.1 NIST SP-800-63B Appendix A
PICS Selection	
Initial Conditions	

with {
the Evaluator is authorized
(NOTE 1: "'becomes authorized' means here, that the becomes fully authorized")
}	

Expected Behaviour	

ensure that {
when {
the Evaluator change the credentials containing
account authenticator indicating value "account authenticator with length less than eight";
}
then {
the IUT did not change the "account authenticator" and
the IUT indicate a notification containing
input indicating value invalid_input;
}
}	

Final Conditions	

TP Id	TP_CR_1_10_Authenticator_feedback_1
Test Objective	Ensure a user cannot gather insights from the SUT feedback as a result of a failed authentication process if account identifier and authenticator are invalid
Reference	IEC 62443-4-2 [1] CR 1.10, section 5.12.1
PICS Selection	

Initial Conditions

```
with {
        the IUT being_in the initial_state and
    the Manufacturer provide the credential_list
}
```

Expected Behaviour

```
ensure that {
  when {
        the Evaluator enter the credentials containing
      account identifier indicating value "invalid account identifier",
      account authenticator indicating value "invalid account authenticator";
  }
  then {
        // NOTE:  invalid_input is EXACTLY the same in all 3 cases (TDL-TO discussion)
      // -> the results of each case have to be compared
     the IUT indicate a notification containing
      input indicating value invalid_authentication;
  }
}
```

Final Conditions

TP Id	TP_CR_1_10_Authenticator_feedback_2
Test Objective	Ensure a user cannot gather insights from the SUT feedback as a result of a failed authentication process if account authenticator is invalid.
Reference	IEC 62443-4-2 [1] CR 1.10, section 5.12.1
PICS Selection	

Initial Conditions

```
with {
        the IUT being_in the initial_state and
    the Manufacturer provide the credential_list
}
```

Expected Behaviour

```
ensure that {
  when {
        the Evaluator enter the credentials containing
      account identifier indicating value "valid account identifier",
      account authenticator indicating value "invalid account authenticator";
  }
  then {
        the IUT indicate a notification containing
      input indicating value invalid_authentication;
  }
}
```

Final Conditions

TP Id	TP_CR_1_10_Authenticator_feedback_3
Test Objective	Ensure a user cannot gather insights from the SUT feedback as a result of a failed authentication process if account identifier is invalid.
Reference	IEC 62443-4-2 [1] CR 1.10, section 5.12.1
PICS Selection	
Initial Conditions	

with {
the IUT being_in the initial_state and
the Manufacturer provide the credential_list
}	

Expected Behaviour	

ensure that {
when {
the Evaluator enter the credentials containing
account identifier indicating value "invalid account identifier",
account authenticator indicating value "valid account authenticator";
}
then {
the IUT indicate a notification containing
input indicating value invalid_authentication;
}
}	

Final Conditions	

TP Id	TP_CR_1_10_Authenticator_feedback_4
Test Objective	Ensure that authenticator are not displayed.
Reference	IEC 62443-4-2 [1] CR 1.10, section 5.12.1 DKE conformance acceptence criteria
PICS Selection	
Initial Conditions	

with {
the IUT being_in the initial_state
}	

Expected Behaviour	

ensure that {
when {
the Evaluator enter any credentials containing
account identifier,
account authenticator;
}
then {
the IUT obfuscate the account authenticator
}
}	

Final Conditions	

TP Id	TP_CR_1_11_a_Unsuccessful_login_attempts_1
Test Objective	The SUT shall provide capabilities to enforce a limit of a configurable number of consecutive invalid access attempts by any user during a configurable time period.
Reference	IEC 62443-4-2 [1] CR 1.11, section 5.13.1 a) + b) (denied access)
PICS Selection	

Initial Conditions

```
with {
        the Evaluator provide the "max number of consecutive invalid attempts" and
     the Evaluator provide the "period of time for deny access"
}
```

Expected Behaviour

```
ensure that {
   when {
        /* the following statement is repeated before "(configured) time window for invalid access counts" terminates */
       repeat "max number of consecutive invalid attempts" times {
       the Evaluator enter the credentials containing
         account identifier indicating value "invalid account identifier",
         account authenticator indicating value "invalid account authenticator";
       and the IUT deny the access
       }
   }
   then {
        (.) at time point t1: the Evaluator enter the credentials containing
         account identifier indicating value "valid account identifier",
         account authenticator indicating value "valid account authenticator";
       /* Note 5.8. (AWar): dependency "period of time for deny access" missing: check: to be tested?*/
       and the IUT deny the access
   }
}
```

Final Conditions

```
        (!) "specified period of time for deny access" after t1 : the Evaluator enter the valid credentials and
      /* until "specified period of time for deny access" terminates.
       * Note that this time window differs from the (configured) "max number of consecutive invalid attempts" time
window
       * and may be fixed ("specified")
       */
     the IUT deny the access
```

TP Id	TP_CR_1_11_b_Unsuccessful_login_attempts_1
Test Objective	The SUT shall provide capabilities to allow valid session access (again) after the specified (locking) time period expired.
Reference	IEC 62443-4-2 [1] CR 1.11, section 5.13.1 a) + b) (denied access)
PICS Selection	
Initial Conditions	

with {
        the Evaluator provide the "max number of consecutive invalid attempts" and
     the Evaluator provide the "period of time for deny access"
}	

Expected Behaviour	

ensure that {
   when {
        /* NOTE: The following statement is repeated before "period of time for deny access" terminates */
      repeat "max number of consecutive invalid attempts" times {
      the Evaluator enter the credentials containing
        account identifier indicating value "invalid account identifier",
        account authenticator indicating value "invalid account authenticator"; and
      (.) at time point t1: the IUT deny the access
      }
   }
   then {
        (!) "period of time for deny access" after t1 : the Evaluator enter the credentials containing
        account identifier indicating value "valid account identifier",
        account authenticator indicating value "valid account authenticator"; and
      the IUT grant the access
   }
}	

Final Conditions	

TP Id	TP_CR_2_1_Authorization_enforcement_1
Test Objective	The SUT shall provide capabilities to provide authorization for default accounts (full authorized).
Reference	IEC 62443-4-2 [1] CR 2.1, section 6.3.1
PICS Selection	
Initial Conditions	

with {
        the IUT being_in the original_factory_state and
        the Evaluator enter the initial_credentials
        (NOTE 1: "default account is authorized to change security configuration")
}	

Expected Behaviour	

ensure that {
   when {
        the Evaluator change the security configuration
   }
   then {
        the IUT apply the changes
   }
}	

Final Conditions	

TP Id	TP_CR_2_1_Authorization_enforcement_2
Test Objective	The SUT shall ensure that minimal authorized accounts can not change security configurations.
Reference	IEC 62443-4-2 [1] CR 2.1, section 6.3.1
PICS Selection	PIC_accessible_security_configuration
Initial Conditions	

with {
the Evaluator is minimal authorized
(NOTE 1: "minimal authorized account is not authorized to change security configuration")
}	

Expected Behaviour	

ensure that {
when {
the Evaluator change the security configuration
}
then {
the IUT deny the request
(NOTE 1: "If externally observable, evaluator receives rejection message.")
(NOTE 2: "If internally observable, evaluator starts additional check.")
}
}	

Final Conditions	

TP Id	TP_CR_2_1_Authorization_enforcement_3
Test Objective	The SUT shall provide capabilities to provide authorization for non-admin accounts (after authorization).
Reference	IEC 62443-4-2 [1] CR 2.1, section 6.3.1
PICS Selection	
Initial Conditions	

with {
the Evaluator is minimal authorized
(NOTE 1: "non-admin account is not authorized to change security configuration")
}	

Expected Behaviour	

ensure that {
when {
the Evaluator becomes fully authorized
(NOTE 1: "fully authorized means the is authorized to change everything")
and the Evaluator change the security configuration
}
then {
the IUT apply the change
}
}	

Final Conditions	

TP Id	TP_CR_2_5_a_Session_Lock_1
Test Objective	Ensure the IUT provides the capability to prevent further access by initiating a session lock after a configurable time period of inactivity.
Reference	IEC 62443-4-2 [1] CR 2.5, section 6.7.1a(i)
PICS Selection	
Initial Conditions	

with {
the IUT being_in the initial_state and
the Manufacturer provide the credentials
}	

Expected Behaviour	

ensure that {
when {
the Evaluator provide the time_period_of_inactivity containing
duration set to "session lock duration";
and (.) at time point t1: the Evaluator enter the credentials containing
account identifier indicating value "valid account identifier",
account authenticator indicating value "valid account authenticator";
}
then {
(!) duration after t1: the IUT lock the current_session
and the IUT indicate a notification containing
account access indicating value "access denied",
current_session indicating value invalid;
}
}	

Final Conditions	

TP Id	TP_CR_2_5_a_Session_Lock_2
Test Objective	Ensure the IUT provides the capability to prevent further access by initiating a session lock after a manual initiation.
Reference	IEC 62443-4-2 [1] CR 2.5, section 6.7.1a(ii)
PICS Selection	
Initial Conditions	

with {
the IUT being_in the initial_state and
the Manufacturer provide the credentials
}	

Expected Behaviour	

ensure that {
when {
the Evaluator enter the credentials containing
account identifier indicating value "valid account identifier",
account authenticator indicating value "valid account authenticator";
and the Evaluator establish the "session lock"
}
then {
the IUT lock the current_session
and the IUT indicate a notification containing
account access indicating value "access denied",
current_session indicating value invalid;
}
}	

Final Conditions	

TP Id	TP_CR_2_5_b_Session_Lock_3
Test Objective	Ensure the session lock remain in effect until the human user who owns the session re-establishes access using appropriate identification and authentication procedures.
Reference	IEC 62443-4-2 [1] CR 2.5, section 6.7.1b(i)
PICS Selection	
Initial Conditions	

with {
the IUT being_in the initial_state and
the IUT lock the current_session
}	

Expected Behaviour	

ensure that {
when {
/* here, the credentials the human user who owns the session have to be used */
the Evaluator enter the credentials containing
account identifier indicating value "valid account identifier",
account authenticator indicating value "valid account authenticator";
}
then {
the IUT establish the current_session
and the IUT indicate a notification containing
account access indicating value "access permitted",
current_session indicating value valid;
}
}	

Final Conditions	

TP Id	TP_CR_2_5_b_Session_Lock_4
Test Objective	Ensure the session lock remain in effect until another authorized human user re-establishes access using appropriate identification and authentication procedures.
Reference	IEC 62443-4-2 [1] CR 2.5, section 6.7.1b(ii)
PICS Selection	
Initial Conditions	

with {
the IUT being_in the initial_state and
the IUT lock the current_session and
the Evaluator is authorized by the IUT
}	

Expected Behaviour	

ensure that {
when {
/* here, the credentials of the Evaluator have to be used */
the Evaluator enter the credentials containing
account identifier indicating value "valid account identifier",
account authenticator indicating value "valid account authenticator";
}
then {
the IUT establish the current_session
and the IUT indicate a notification containing
account access indicating value "access permitted",
current_session indicating value valid;
}
}	

Final Conditions	

TP Id	TP_CR_3_5_Input_validation_during_session
Test Objective	The SUT shall not accept invalid syntax, length and content input that is used as control input.
Reference	IEC 62443-4-2 [1] CR 3.5, section 7.7.1
PICS Selection	

Initial Conditions

```
with {
      the IUT being_in the initial_state and
     the IUT establish the current_session and
     the Evaluator provide the invalid_data
}
```

Expected Behaviour

```
ensure that {
  when {
      // NOTE:  The following statement is repeated before a specified period (to be specified) terminates and the
used invalid data should be different to previous attempts
    /* is done for every configuration interface / IUT or usage of different TP variant */
    repeat invalid_data times {
     the Evaluator enter an invalid_date
     }
  }
  then {
      the IUT ignore the input
    (NOTE 1:    "external observations: no restart, no configuration changes")
    (NOTE 2:    "internal observations: no invalid data written into log file")
  }
}
```

Final Conditions

TP Id	TP_CR_3_5_Input_validation_session_establishment
Test Objective	The SUT shall not accept invalid syntax, length and content input that is used as control input.
Reference	IEC 62443-4-2 [1] CR 3.5, section 7.7.1
PICS Selection	

Initial Conditions

```
with {
      the IUT being_in the initial_state and
   the Evaluator provide the invalid_data
}
```

Expected Behaviour

```
ensure that {
  when {
      // NOTE:  The following statement is repeated before a specified period (to be specified) terminates
      repeat invalid_data times {
        the Evaluator enter the invalid_date
      }
  }
  then {
      the IUT ignore the input
      (NOTE 1: "external observations: no restart, no configuration changes")
      (NOTE 2: "internal observations: no invalid data written into log file")
  }
}
```

Final Conditions

<table>
<tr><td><b>TP Id</b></td><td>TP_CR_3_8_Session_Integrity_replay_prevention</td></tr>
<tr><td><b>Test Objective</b></td><td>Protect the integrity of communication sessions including invalidation of session invalidation upon user logout</td></tr>
<tr><td><b>Reference</b></td><td>IEC 62443-4-2 [1] CR 3.8, section a)</td></tr>
<tr><td><b>PICS Selection</b></td><td></td></tr>
<tr><td colspan="2"><b>Initial Conditions</b></td></tr>
<tr><td colspan="2">with {
        the IUT authorized the Evaluator and
    the Evaluator change the modifyable_information_to_be_protected and
    the Evaluator record the transmitted_information_sequence
}</td></tr>
<tr><td colspan="2"><b>Expected Behaviour</b></td></tr>
<tr><td colspan="2">ensure that {
  when {
        the Evaluator change the modifyable_information_to_be_protected /* back to the original value */ and
      the Evaluator close the current_session and
     the Evaluator replay the transmitted_information_sequence
  }
  then {
        the IUT ignore the modification_attempt
  }
}</td></tr>
<tr><td colspan="2"><b>Final Conditions</b></td></tr>
<tr><td colspan="2"></td></tr>
</table>

<table>
<tr><td><b>TP Id</b></td><td>TP_CR_4_1_b_Information_confidentiality_in_transit_read_direction_TLS</td></tr>
<tr><td><b>Test Objective</b></td><td>Ensure the protection of the confidentiality of information in transit when data is _read_ from IUT</td></tr>
<tr><td><b>Reference</b></td><td>IEC 62443-4-2 [1] CR 4.1, section 8.3.1b</td></tr>
<tr><td><b>PICS Selection</b></td><td>PIC_TLS</td></tr>
<tr><td colspan="2"><b>Initial Conditions</b></td></tr>
<tr><td colspan="2">with {
        the IUT authorized the Evaluator and
    the Evaluator identify the readable_information_to_be_protected
    (NOTE 1:"validation, that authorization is required for ALL _readable_ information that can be regarded sensitive")
}</td></tr>
<tr><td colspan="2"><b>Expected Behaviour</b></td></tr>
<tr><td colspan="2">ensure that {
  when {
        the Evaluator request the readable_information_to_be_protected
  }
  then {
        the Evaluator ensures the TLS_usage_for_data_transmission
  }
}</td></tr>
<tr><td colspan="2"><b>Final Conditions</b></td></tr>
<tr><td colspan="2"></td></tr>
</table>

<table>
<tr><td><b>TP Id</b></td><td>TP_CR_4_1_b_Information_confidentiality_in_transit_write_direction_TLS</td></tr>
<tr><td><b>Test Objective</b></td><td>Ensure the protection of the confidentiality of information in transit when data is _written_ to IUT</td></tr>
<tr><td><b>Reference</b></td><td>IEC 62443-4-2 [1] CR 4.1, section 8.3.1b</td></tr>
<tr><td><b>PICS Selection</b></td><td>PIC_TLS</td></tr>
<tr><td colspan="2"><b>Initial Conditions</b></td></tr>
<tr><td colspan="2">with {
the IUT authorized the Evaluator and
the Evaluator identify the modifyable_information_to_be_protected
(NOTE 1: "validation, that authorization is required for ALL _writable_ information that can be regarded sensitive")
}</td></tr>
<tr><td colspan="2"><b>Expected Behaviour</b></td></tr>
<tr><td colspan="2">ensure that {
when {
the Evaluator change the modifyable_information_to_be_protected
}
then {
the Evaluator ensures the TLS_usage_for_data_transmission
}
}</td></tr>
<tr><td colspan="2"><b>Final Conditions</b></td></tr>
<tr><td colspan="2"></td></tr>
</table>

<table>
<tr><td><b>TP Id</b></td><td>TP_CR_4_1_b_Information_confidentiality_in_transit_read_direction_SSH</td></tr>
<tr><td><b>Test Objective</b></td><td>Ensure the protection of the confidentiality of information in transit when data is _read_ from IUT</td></tr>
<tr><td><b>Reference</b></td><td>IEC 62443-4-2 [1] CR 4.1, section 8.3.1b</td></tr>
<tr><td><b>PICS Selection</b></td><td>PIC_SSH</td></tr>
<tr><td colspan="2"><b>Initial Conditions</b></td></tr>
<tr><td colspan="2">with {
the IUT authorized the Evaluator and
the Evaluator identify the readable_information_to_be_protected
(NOTE 1:"validation, that authorization is required for ALL _readable_ information that can be regarded sensitive")
}</td></tr>
<tr><td colspan="2"><b>Expected Behaviour</b></td></tr>
<tr><td colspan="2">ensure that {
when {
the Evaluator request the readable_information_to_be_protected
}
then {
the Evaluator ensures the SSH_usage_for_data_transmission
}
}</td></tr>
<tr><td colspan="2"><b>Final Conditions</b></td></tr>
<tr><td colspan="2"></td></tr>
</table>

TP Id	TP_CR_4_1_b_Information_confidentiality_in_transit_write_direction_SSH
Test Objective	Ensure the protection of the confidentiality of information in transit when data is _written_ to IUT
Reference	IEC 62443-4-2 [1] CR 4.1, section 8.3.1b
PICS Selection	PIC_SSH
Initial Conditions	

with {
the IUT authorized the Evaluator and
the Evaluator identify the modifyable_information_to_be_protected
(NOTE 1: "validation, that authorization is required for ALL _writable_ information that can be regarded sensitive")
}	

Expected Behaviour	

ensure that {
when {
the Evaluator change the modifyable_information_to_be_protected
}
then {
the Evaluator ensures the SSH_usage_for_data_transmission
}
}	

Final Conditions	

TP Id	TP_CR_4_1_b_Information_confidentiality_in_transit_wireless
Test Objective	Ensure the protection of the confidentiality of information in case of wireless transmission.
Reference	IEC 62443-4-2 [1] CR 4.1, section 8.3.1b, DKE conformance acceptance criteria
PICS Selection	PIC_WIRELESS
Initial Conditions	

with {
the IUT being_in the wireless_connection_state
}	

Expected Behaviour	

ensure that {
when {
the Evaluator change the modifyable_information_to_be_protected
(NOTE 1: "write direction ")
}
then {
the IUT establish an encryped_connection
(NOTE 2: "e.g. via wireless trace analysis")
}
}	

Final Conditions	

TP Id	TP_CR_4_3_Use_of_cryptography_IUT_as_TLS_client
Test Objective	Ensure the protection of the confidentiality of information in transit by using recommended Protocol Versions and Cyber Suites for TLS according e.g. to NIST recommendations
Reference	IEC 62443-4-2 [1] CR 4.3, section 8.5.1
PICS Selection	PIC_TLS
Initial Conditions	

with {
the IUT being_in the initial_state
}	

Expected Behaviour	

ensure that {
when {
the IUT establish the TLS_connection
}
then {
the Evaluator receive the IUT_TLS_capabilities containing /* e.g. via tracing */
TLS version indicating value TLS_version is_subset_of commonly_accepted_TLS_versions,
TLS cipher indicating value TLS_cipher is_subset_of commonly_accepted_ciphers;
}
}	

Final Conditions	

TP Id	TP_CR_4_3_Information_confidentiality_in_transit_IUT_as_TLS_server_with_valid_TLS_capabilities
Test Objective	IUT as client: Ensure the protection of the confidentiality of information in transit by using recommended Protocol Versions and Cyber Suites for TLS according e.g. to NIST recommendations
Reference	IEC 62443-4-2 [1] CR 4.3, section 8.5.1
PICS Selection	PIC_TLS
Initial Conditions	

with {
the IUT being_in the initial_state
}	

Expected Behaviour	

ensure that {
when {
the Evaluator provide the IUT_TLS_capabilities containing
TLS version indicating value TLS_version,
TLS cipher indicating value TLS_cipher;
and the Evaluator request the TLS_connection
}
then {
the IUT accept
(NOTE 1: "Selection of capability refers to the TLS protocol")
}
}	

Final Conditions	

TP Id	TP_CR_4_3_Information_confidentiality_in_transit_IUT_as_TLS_server_with_invalid_TLS_version
Test Objective	Ensure the protection of the confidentiality of information in transit by denying not accepted Protocol Versions for TLS according e.g. to NIST recommendations
Reference	IEC 62443-4-2 [1] CR 4.3, section 8.5.1
PICS Selection	PIC_TLS
Initial Conditions	

with {
the IUT being_in the initial_state
}	

Expected Behaviour	

ensure that {
when {
the Evaluator provide the IUT_TLS_capabilities containing
TLS version indicating value invalid TLS_version,
TLS cipher indicating value valid TLS_cipher;
(NOTE 1: "invalid TLS_version means here 'not accepted'")
and the Evaluator request the TLS_connection
}
then {
repeat IUT_TLS_capabilities times {
the IUT deny
}
}
}	

Final Conditions	

TP Id	TP_CR_4_3_Information_confidentiality_in_transit_IUT_as_TLS_server_with_invalid_TLS_ciphers
Test Objective	Ensure the protection of the confidentiality of information in transit by denying not accepted Cyber Suites for TLS according e.g. to NIST recommendations
Reference	IEC 62443-4-2 [1] CR 4.3, section 8.5.1
PICS Selection	PIC_TLS
Initial Conditions	

with {
the IUT being_in the initial_state
}	

Expected Behaviour	

ensure that {
when {
the Evaluator provide the IUT_TLS_capabilities containing
TLS version indicating value valid TLS_version,
TLS cipher indicating value invalid TLS_cipher;
(NOTE 1: "invalid TLS_cipher means here 'not accepted'")
and the Evaluator request the TLS_connection
}
then {
repeat IUT_TLS_capabilities times {
the IUT deny
}
}
}	

Final Conditions	

TP Id	TP_CR_4_3_Use_of_cryptography_IUT_as_SSH_client
Test Objective	IUT as client: Ensure the protection of the confidentiality of information in transit by using recommended Protocol Versions and Cyber Suites for SSH according e.g. to BSI recommendations
Reference	IEC 62443-4-2 CR 4.3, section 8.5.1
PICS Selection	PIC_SSH
Initial Conditions	

with {
        the IUT being_in the initial_state
}	

Expected Behaviour	

ensure that {
   when {
        the IUT establish the TLS_connection
   }
   then {
        the Evaluator receive the "IUT SSH capabilities" containing /* e.g. via tracing */
      SSH version indicating value SSH_version is_subset_of commonly_accepted_SSH_versions,
      SSH cipher indicating value SSH_cipher is_subset_of commonly_accepted_ciphers;
   }
}	

Final Conditions	

TP Id	TP_CR_7_6_Network_and_security_configuration_settings
Test Objective	Ensure that network and security configurations can be configured as described in guideline.
Reference	IEC 62443-4-2 [1] CR 7.6, section 11.8
PICS Selection	
Initial Conditions	

with {
        the IUT being_in the initial_state and
        the Manufacturer provide the configuration_guidelines
}	

Expected Behaviour	

ensure that {
   when {
        the Evaluator follow the configuration_guidelines
           (NOTE 1:   "Guidelines might be executed")
   }
   then {
        the IUT apply the configurations
   }
}	

Final Conditions	

TP Id	TP_CR_7_7_Least_functionality_ping_disabled
Test Objective	Ensure that ICMP (echo) functionality is disabled by default
Reference	IEC 62443-4-2 [1] CR 7.7, section 11.9
PICS Selection	
Initial Conditions	

with {
the IUT being_in the initial_state
}	

Expected Behaviour	

ensure that {
when {
the Evaluator request an ICMP_echo_reply
}
then {
the IUT ignore the ICMP_echo_request
}
}	

Final Conditions	

TP Id	TP_CR_7_7_Least_functionality_unused_ports_disabled
Test Objective	Ensure that only ports/services needed for initial configuration are enabled by default
Reference	IEC 62443-4-2 [1] CR 7.7, section 11.9
PICS Selection	
Initial Conditions	

with {
the IUT being_in the initial_state
}	

Expected Behaviour	

ensure that {
when {
the IUT provide the configuration_services
}
then {
the IUT deny the access to_non_configuration_services
}
}	

Final Conditions	

TP Id	TP_xDR_2_4_SAR_2_4_Mobile_code_integrity_check
Test Objective	Ensure the integrity for mobile code prior to execution
Reference	IEC 62443-4-2 [1] SAR 2.4, section 12.2.1 case c) IEC 62443-4-2 [1] EDR 2.4, section 13.2.1 case c) IEC 62443-4-2 [1] HDR 2.4, section 14.2.1 case c) IEC 62443-4-2 [1] NDR 2.4, section 15.4.1 case c)
PICS Selection	PIC_Mobile_code
Initial Conditions	

with {
the IUT being_in the initial_state and
the Evaluator is authorized by the IUT
}	

Expected Behaviour	

ensure that {
when {
the Evaluator enter the non_integer_mobile_code
(NOTE 1: '"entering' may be the mobile code download or activation")
}
then {
the IUT deny the mobile_code_execution
}
}	

Final Conditions	

<table>
<tr><td><b>TP Id</b></td><td>TP_xDR_2_4_SAR_2_4_Mobile_code_authenticity_check</td></tr>
<tr><td><b>Test Objective</b></td><td>Ensure the authenticity for mobile code to verify the origin</td></tr>
<tr><td><b>Reference</b></td><td>IEC 62443-4-2 [1] SAR 2.4 RE(1), section 12.2.3
IEC 62443-4-2 [1] EDR 2.4 RE(1), section 13.2.3
IEC 62443-4-2 [1] HDR 2.4 RE(1), section 14.2.3
IEC 62443-4-2 [1] NDR 2.4 RE(1), section 15.4.3</td></tr>
<tr><td><b>PICS Selection</b></td><td>PIC_Mobile_code</td></tr>
<tr><td colspan="2"><b>Initial Conditions</b></td></tr>
<tr><td colspan="2">with {
        the IUT being_in the initial_state and
          the Evaluator is authorized by the IUT
}</td></tr>
<tr><td colspan="2"><b>Expected Behaviour</b></td></tr>
<tr><td colspan="2">ensure that {
   when {
        the Evaluator enter the untrusted_mobile_code
           (NOTE 1:   '"entering' may be the mobile code download or activation")
   }
   then {
        the IUT deny the mobile_code_execution
   }
}</td></tr>
<tr><td colspan="2"><b>Final Conditions</b></td></tr>
<tr><td colspan="2"></td></tr>
</table>

<table>
<tr><td><b>TP Id</b></td><td>TP_xDR_3_10_Update_support</td></tr>
<tr><td><b>Test Objective</b></td><td>Ensure the ability of updates (upgrades)</td></tr>
<tr><td><b>Reference</b></td><td>IEC 62443-4-2 [1] EDR 3.10, section 13.5.1
IEC 62443-4-2 [1] HDR 3.10, section 14.5.1
IEC 62443-4-2 [1] NDR 3.10, section 15.7.1</td></tr>
<tr><td><b>PICS Selection</b></td><td></td></tr>
<tr><td colspan="2"><b>Initial Conditions</b></td></tr>
<tr><td colspan="2">with {
        the IUT being_in the initial_state and
        the Evaluator is authorized
}</td></tr>
<tr><td colspan="2"><b>Expected Behaviour</b></td></tr>
<tr><td colspan="2">ensure that {
   when {
        the Evaluator enter the update containing
              version identifier indicating value "new version";
   }
   then {
        the IUT indicate a version containing
              version identifier indicating value "new version";
   }
}</td></tr>
<tr><td colspan="2"><b>Final Conditions</b></td></tr>
<tr><td colspan="2"></td></tr>
</table>

Annex A (normative): TDL code for the Test Purposes

This Test purpose catalogue has been produced using the Test Description Language (TDL-TO) according to ETSI ES 203 119-4 [2]. The TDL-TO library modules corresponding to the Test purpose catalogue are contained in archive ts_103646v010101p0.zip which accompanies the present document.

History

Document history		
V1.1.1	January 2021	Publication