



BSI Standards Publication

Common security requirements for radio equipment

Part 3: Internet connected radio equipment processing
virtual money or monetary value

National foreword

This British Standard is the UK implementation of EN 18031-3:2024.

The UK participation in its preparation was entrusted to Technical Committee IST/33/-/8.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

This publication has been prepared under a mandate given to the European Standards Organizations by the European Commission and the European Free Trade Association. It is intended to support requirements of the EU legislation detailed in the European Foreword. A European Annex, usually Annex ZA or ZZ, describes how this publication relates to that EU legislation.

For the Great Britain market (England, Scotland and Wales), if UK Government has designated this publication for conformity with UKCA marking (or similar) legislation, it may contain an additional National Annex. Where such a National Annex exists, it shows the correlation between this publication and the relevant UK legislation. If there is no National Annex of this kind, the relevant Annex ZA or ZZ in the body of the European text will indicate the relationship to UK regulation applicable in Great Britain. References to EU legislation may need to be read in accordance with the UK designation and the applicable UK law. Further information on designated standards can be found at www.bsigroup.com/standardsandregulation.

For the Northern Ireland market, UK law will continue to implement relevant EU law subject to periodic confirmation. Therefore Annex ZA/ZZ in the European text, and references to EU legislation, are still valid for this market.

UK Government is responsible for legislation. For information on legislation and policies relating to that legislation, consult the relevant pages of www.gov.uk.

© The British Standards Institution 2024
Published by BSI Standards Limited 2024

ISBN 978 0 539 28365 5

ICS 33.060.20; 35.030

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 August 2024.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------

English version

Common security requirements for radio equipment - Part 3: Internet connected radio equipment processing virtual money or monetary value

Exigences de sécurité communes applicables aux équipements radioélectriques - Partie 3 : Équipements radioélectriques connectés à l'internet qui traitent une monnaie virtuelle ou de la valeur monétaire

Gemeinsame Sicherheitsanforderungen für mit dem Internet verbundene Funkanlagen, die für die Datenverarbeitung im Zusammenhang mit virtuellen Währungen oder monetären Werten eingesetzt werden

This European Standard was approved by CEN on 1 August 2024.

CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and United Kingdom.



CEN-CENELEC Management Centre:
Rue de la Science 23, B-1040 Brussels

Contents

Page

European foreword	5
Introduction	6
1 Scope.....	7
2 Normative references.....	7
3 Terms and definitions	7
4 Abbreviations.....	12
5 Application of this document.....	13
6 Requirements.....	16
6.1 [ACM] Access control mechanism	16
6.1.1 [ACM-1] Applicability of access control mechanisms	16
6.1.2 [ACM-2] Appropriate access control mechanisms	21
6.2 [AUM] Authentication mechanism.....	25
6.2.1 [AUM-1] Applicability of authentication mechanisms	25
6.2.2 [AUM-2] Appropriate authentication mechanisms	36
6.2.3 [AUM-3] Authenticator validation	42
6.2.4 [AUM-4] Changing authenticators.....	46
6.2.5 [AUM-5] Password strength.....	49
6.2.6 [AUM-6] Brute force protection.....	57
6.3 [SUM] Secure update mechanism.....	61
6.3.1 [SUM-1] Applicability of update mechanisms.....	61
6.3.2 [SUM-2] Secure updates.....	64
6.3.3 [SUM-3] Automated updates	68
6.4 [SSM] Secure storage mechanism	72
6.4.1 [SSM-1] Applicability of secure storage mechanisms	72
6.4.2 [SSM-2] Appropriate integrity protection for secure storage mechanisms	76
6.4.3 [SSM-3] Appropriate confidentiality protection for secure storage mechanisms	81
6.5 [SCM] Secure communication mechanism.....	86
6.5.1 [SCM-1] Applicability of secure communication mechanisms	86
6.5.2 [SCM-2] Appropriate integrity and authenticity protection for secure communication mechanisms	91
6.5.3 [SCM-3] Appropriate confidentiality protection for secure communication mechanisms	97
6.5.4 [SCM-4] Appropriate replay protection for secure communication mechanisms ..	102
6.6 [LGM] Logging Mechanism.....	107
6.6.1 [LGM-1] Applicability of logging mechanisms.....	107
6.6.2 [LGM-2] Persistent storage of log data	110
6.6.3 [LGM-3] Minimum number of persistently stored events.....	113
6.6.4 [LGM-4] Time-related information of persistently stored log data.....	116
6.7 [CCK] Confidential cryptographic keys.....	119
6.7.1 [CCK-1] Appropriate CCKs	119
6.7.2 [CCK-2] CCK generation mechanisms	123
6.7.3 [CCK-3] Preventing static default values for preinstalled CCKs.....	127
6.8 [GEC] General equipment capabilities	131

6.8.1	[GEC-1] Up-to-date software and hardware with no publicly known exploitable vulnerabilities.....	131
6.8.2	[GEC-2] Limit exposure of services via related network interfaces.....	135
6.8.3	[GEC-3] Configuration of optional services and the related exposed network interfaces.....	139
6.8.4	[GEC-4] Documentation of exposed network interfaces and exposed services via network interfaces.....	143
6.8.5	[GEC-5] No unnecessary external interfaces.....	146
6.8.6	[GEC-6] Input validation.....	148
6.8.7	[GEC-7].....	153
6.8.8	[GEC-8] Equipment Integrity	153
6.9	[CRY] Cryptography	157
6.9.1	[CRY-1] Best practice cryptography.....	157
	Annex A (informative) Rationale	162
A.1	General	162
A.2	Rationale.....	162
A.2.1	Family of standards	162
A.2.2	Security by design.....	162
A.2.3	Threat modelling and security risk assessment	163
A.2.4	Functional sufficiency assessment.....	164
A.2.5	Implementation categories.....	164
A.2.6	Assets	165
A.2.7	Mechanisms	167
A.2.8	Assessment criteria	167
A.2.8.1	Decision trees.....	167
A.2.8.2	Technical documentation.....	168
A.2.8.3	Security testing.....	169
A.2.9	Interfaces.....	169
A.2.9.1	Example: Laptop with a built-in keyboard	170
A.2.9.2	Example: Equipment with a USB-keyboard	170
A.2.9.3	Example: User interface over a network.....	171
A.2.9.4	Example: USB-printer.....	171
A.2.9.5	Example: Network printer.....	172
	Annex B (informative) Mapping with EN IEC 62443-4-2:2019.....	173
B.1	General	173
B.2	Mapping.....	173
	Annex C (informative) Mapping with ETSI EN 303 645 (Cyber Security for Consumer Internet of Things: Baseline Requirements)	176
C.1	General	176
C.2	Mapping.....	176
	Annex D (informative) Mapping with Security Evaluation Standard for IoT Platforms (SESIP)	180
D.1	General	180

D.2 Mapping..... 180

Annex ZA (informative) Relationship between this European Standard and the Delegated Regulation (EU) 2022/30 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d) (e) and (f), of that Directive aimed to be covered 183

Bibliography 184

European foreword

This document (EN 18031-3:2024) has been prepared by Technical Committee CEN/CENELEC JTC 13 “Cybersecurity and Data Protection”, the secretariat of which is held by DIN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by February 2025, and conflicting national standards shall be withdrawn at the latest by February 2025.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN shall not be held responsible for identifying any or all such patent rights.

This document has been prepared under a standardization request addressed to CEN-CENELEC by the European Commission. The Standing Committee of the EFTA States subsequently approves these requests for its Member States.

For the relationship with EU Legislation, see informative Annex ZA, which is an integral part of this document.

Any feedback and questions on this document should be directed to the users’ national standards body. A complete listing of these bodies can be found on the CEN website.

According to the CEN-CENELEC Internal Regulations, the national standards organisations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.

Introduction

Vigilance is required from manufacturers to improve the overall resilience against cybersecurity threats caused by the increased connectivity of radio equipment [34] and the growing ability of malicious threat actors to cause harm to users, organizations, and society.

The security requirements presented in this baseline standard are developed to improve the ability of radio equipment to protect its security and financial assets against common cybersecurity threats and to mitigate publicly known exploitable vulnerabilities.

It is important to note that to achieve the overall cybersecurity of radio equipment, defence in depth best practices will be needed by both the manufacturer and user. In particular, no single measure will suffice to achieve the given objectives, indeed achieving even a single security objective will usually require a suite of mechanisms and measures. Throughout this document, the guidance material includes lists of examples. These examples given are only indicative possibilities, as there are other possibilities that are not listed, and even using the examples given will not be sufficient unless the mechanisms and measures chosen are implemented in a coordinated fashion.

1 Scope

This document specifies common security requirements and related assessment criteria for internet connected radio equipment [35]. That equipment enables the holder or user to transfer money, monetary value or virtual currency [35] (hereinafter referred to as "equipment").

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp/>
- IEC Electropedia: available at <https://www.electropedia.org/>
- ISO Online browsing platform: available at <https://www.iso.org/obp/>

3.1

access control mechanism

equipment functionality to grant, restrict or deny access to specific equipment's *resources*

Note 1 to entry: Access to specific equipment's resources can amongst others be:

- reading specific data; or
- writing specific data to equipment's persistent storage; or
- performing a specific equipment functionality such as recording audio.

3.2

authentication

provision of assurance that an *entity* is who or what it claims to be

Note 1 to entry: An entity can amongst others claim to be:

- a specific human, owner of a user account, device, or service; or
- a member of specific groups such as an authorized group to access a specific equipment's resource; or
- authorized by another entity to access a specific equipment's resource.

3.3

authentication mechanism

equipment functionality to verify that an *entity* is who or what it claims to be

Note 1 to entry: Typically, the verification is based on examining evidence from one or more elements of the categories:

- knowledge; and
- possession; and

- inherence.

3.4

authenticator

something known or possessed, and controlled by an entity that is used for *authentication*

Note 1 to entry: Typically, it is a physical device or a password.

EXAMPLE A password or token can be used as an authenticator.

3.5

assessment objective

statement, provided as part of the assessment input, which defines the reasons for performing the assessment

[SOURCE: ISO/IEC 33001:2015, 3.2.6 [28]]

3.6

best practice

measures that have been shown to provide appropriate security for the corresponding use case

3.7

brute force attack

attack on a cryptosystem that employs a trial-and-error search of a set of keys, *passwords* or other data

3.8

communication mechanism

equipment functionality that allows communication via a *machine interface*

3.9

confidential cryptographic key

confidential security parameter, excluding *passwords*, which is used in the operation of a cryptographic algorithm or cryptographic protocol

3.10

confidential financial data

financial data whose disclosure can lead to fraud

3.11

confidential financial function configuration

financial function configuration whose disclosure can lead to fraud

3.12

confidential security parameters

security parameter whose disclosure can lead to fraud

3.13

denial of service

prevention or interruption of authorized access to an equipment *resource* or the delaying of the equipment operations and functions

[SOURCE: IEC 62443-1-1:2019, 3.2.42 [29]] modified

3.14**device**

product external to the equipment

3.15**entity**

user, *device*, equipment or service

3.16**entropy**

measure of the disorder, randomness or variability in a closed system

3.17**external interface**

interface of an equipment that is accessible from outside the equipment

3.18**factory default state**

defined state where the configuration settings and configuration of the equipment is set to initial values

Note 1 to entry: A factory default state may include security updates, installed after the equipment being placed on the market.

3.19**financial asset**

sensitive financial data or *confidential financial data* or *sensitive financial function configuration* or *confidential financial function configuration* or *financial functions*

3.20**financial data**

data that represents, provides information about, or is processed for transferring money, monetary assets or virtual currencies [35]

3.21**financial function**

equipment's functionality that processes *financial data*

3.22**financial function configuration**

data processed by the equipment that defines the behaviour of the equipment's *financial functions*

3.23**hard-coded**

software development practice of embedding data directly into the source code of a program or other executable object

3.24**initialization**

process that configures the network connectivity of the equipment for operation

Note 1 to entry: Initialization can provide the possibility to configure authentication features for a user or for network access.

3.25

interface

shared boundary across which *entities* exchange information

3.26

justification

documented information providing evidence that a claim is true under the assumption of common expertise.

Note 1 to entry: Such evidence can be supported for example by:

- a description of the equipment's intended equipment functionality,
- a descriptions of equipment's operational environment of use,
- a description of equipment's technical properties such as security measures
- an analysis of relevant risks related to the operation of the equipment within its reasonably foreseeable use and intended equipment functionality.

3.27

log data

record(s) of certain events (of processes) on a computing equipment

3.28

logging mechanism

equipment functionality to log internal activities

3.29

machine interface

external interface between the equipment and a service or *device*

3.30

network interface

external interface enabling the equipment to have or provide access to a network

Note 1 to entry: Examples for network interfaces are a LAN port (wired) or a wireless network interface enabling WLAN or short range wireless communication, e.g., using a 2.4 GHz antenna.

3.31

operational state

state in which the equipment is functioning normally according its intended equipment functionality [36] and within its intended operational environment of use

3.32

optional service

services which are not necessary to setup the equipment, and which are not part of the basic functionality but are still relevant for the intended equipment functionality [36] and are delivered as part of the factory default.

EXAMPLE An SSH service on the equipment is not required for basic functionality of the equipment, but it can be used to allow a remote access to the equipment.

3.33**password**

sequence of characters (letters, numbers, or other symbols) used to authenticate an *entity*

Note 1 to entry: Personal identification numbers (PINs) are also considered a form of password.

3.34**public security parameter**

sensitive security parameter that is not confidential

3.35**resilient**

able to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber *resources*.

[SOURCE: NIST SP 800-172 [30]]

3.36**resource**

functional unit or data item needed to perform required operations

[SOURCE: IEC [31]]

3.37**risk**

combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:2014 [32]]

3.38**security asset**

sensitive security parameter or *confidential security parameter* or *security function*

3.39**security function**

functionality on the equipment that protects *security assets* or *financial assets* from being misused for fraud

3.40**security parameter**

data processed by the equipment that defines the behaviour of the equipment's *security function*

3.41**security strength**

number associated with the amount of work that is required to break a cryptographic algorithm or system

Note 1 to entry: The amount of work can for example be the number of operations required to break a cryptographic algorithm or system.

3.42**sensitive financial data**

financial data whose manipulation can lead to fraud

3.43

sensitive financial function configuration

financial function configuration whose unauthorized modification can lead to fraud

3.44

sensitive security parameters

security parameter whose manipulation can lead to fraud

3.45

security update

software update that addresses security vulnerabilities through software patches or other mitigations

3.46

software

assembly of programs, procedures, rules, documentation, and data, pertaining to the operation of an equipment

Note 1 to entry: Software also includes firmware.

3.47

storage mechanism

equipment functionality that allows to store information

3.48

update mechanism

equipment functionality that allows to change equipment's *software*

3.49

user interface

external interface between the equipment and a user

3.50

vulnerability

weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the equipment, network, application, or protocol involved.

[SOURCE: (ITSEC) (definition given by ENISA, "computer system" has been replaced by "equipment") [33]]

4 Abbreviations

ACM	access control mechanism
API	application programming interface
AU	assessment unit
AUM	authentication mechanism
CCK	confidential cryptographic key(s)
CRY	cryptography
CSP	confidential security parameter
CWE	common weakness enumeration
DN	decision node
DT	decision tree
E	evidence
E.Info	evidence.information
E.Just	evidence.justification

GEC	general equipment capabilities
IC	implementation category
IP	internet protocol
LAN	local area network
LGM	logging mechanism
MitM	Man-in-the-Middle
OS	operating system
OTP	one-time password
PIN	personal identification number
PKI	public key infrastructure
PSP	public security parameter
SCM	secure communication mechanism
SDO	standards developing organization
SQL	structured query language
SSM	secure storage mechanism
SSP	sensitive security parameter
SUM	secure update mechanism
USB	universal serial bus
WLAN	wireless local area network

5 Application of this document

This document uses the concept of mechanisms to instruct the user of this document when to apply certain security measures. Mechanisms address the applicability and appropriateness through a set of requirements including assessment criteria. An applicable/non-applicable decision is taken for each of the items specified. If applicable it is followed by a pass/fail appropriateness decision for each of the items specified. For example, when checking the applicability of a requirement on external interfaces, then the decision whether the requirement needs to be fulfilled is determined for each external interface independently.

The mechanisms and their application are documented using the structure shown in the table below:

Table 1 — Requirements structure

Clause #	Title		Description on how to apply the document
6.x	XXX Mechanism		Mechanism for each specific item (e.g., external interface or security asset)
6.x.1	XXX-1 Applicability of mechanisms		Applicability of the mechanism
6.x.1.1	Requirement		For each specific item determine and assess if the mechanism is required. NOTE A mechanism might combine applicability and appropriateness in a single requirement.
6.x.1.2	Rationale		
6.x.1.3	Guidance		
6.x.1.4	Assessment criteria		
6.x.1.4.1		Assessment objective	
6.x.1.4.2		Implementation categories	
6.x.1.4.3		Required information	
6.x.1.4.4		Conceptual assessment	
6.x.1.4.5		Functional completeness assessment	

Clause #	Title	Description on how to apply the document
6.x.1.4.6	Functional sufficiency assessment	
6.x.2	XXX-2 Appropriate mechanisms	Appropriateness of the mechanism
6.x.2.1	Requirement	For each specific item for which the mechanism is required as determined by XXX-1, determine and assess whether the mechanism is implemented properly. NOTE A mechanism might have multiple appropriateness sub-clauses to focus on specific properties.
6.x.2.2	Rationale	
6.x.2.3	Guidance	
6.x.2.4	Assessment criteria	
6.x.2.4.1	Assessment objective	
6.x.2.4.2	Implementation categories	
6.x.2.4.3	Required information	
6.x.2.4.4	Conceptual assessment	
6.x.2.4.5	Functional completeness assessment	
6.x.2.4.6	Functional sufficiency assessment	
6.x.y	XXX-# Supporting Requirements	Applicability and appropriateness of supporting requirements for the mechanism
6.x.y.1	Requirement	For each specific item for which the mechanism is required as determined by XXX-1, determine and assess if the supporting requirement needs to be implemented (there might be specific conditions, for instance if the equipment is a toy) and if it needs to be implemented, whether it is implemented properly. NOTE Some chapters contain multiple requirements, which leads to slight deviations in terms of numbering.
6.x.y.2	Rationale	
6.x.y.3	Guidance	
6.x.y.4	Assessment criteria	
6.x.y.4.1	Assessment objective	
6.x.y.4.2	Implementation categories	
6.x.y.4.3	Required information	
6.x.y.4.4	Conceptual assessment	
6.x.y.4.5	Functional completeness assessment	
6.x.y.4.6	Functional sufficiency assessment	

The assessments are conducted by examining the documented assessment cases, not all assessment cases might be provided for every mechanism:

— Conceptual assessment

Examine if the provided documentation and rationale provide the required evidence (for example the rationale why a mechanism is not applicable for a specific network interface).

— Functional completeness assessment

Examine and test if the provided documentation is complete (for example use network scanners to verify that all external interfaces are properly identified, documented and assessed)

— Functional sufficiency assessment

Examine and test if the implementation is adequate (for example run fuzzing tools on a network interface to check if it is resilient to attacks with malformed data)

Each of the assessments is further divided into the following sub-clauses which might use a decision tree to guide the assessment:

- Assessment purpose
- Preconditions
- Assessment units
- Assignment of verdict

Required information lists the information to be provided through technical documentation. This document does not require each required information element to be provided as a separate document.

For the section assessment criteria, the following identifiers with the defined syntax are used to structure the elements which are needed to perform an assessment:

- Required information
 - E.<Type>.<MechanismAbbreviation-<Nr>>.<CategoryName>
 - Identifier for the category of the required information excluding DTs
- Required information for decision trees
 - E.<Type>.DT.<MechanismAbbreviation-<Nr>>
 - Identifier for the category of the required information in the context of DTs
- Implementation Category
 - IC.<MechanismAbbreviation-<Nr>>.<ImplementationCategoryName>
 - Identifier for the implementation category
- Assessment Unit
 - AU.<MechanismAbbreviation-<Nr>>.<AssessmentUnitName>
 - Identifier for the assessment unit
- Decision Tree Nodes
 - DT.<MechanismAbbreviation-<Nr>>.DN-<Number>
 - Identifier for a specific node inside the DT

The placeholders are used as follows:

- <Type>: “Info” or “Just” to indicate the kind of required documentation which could be by information” or justification.
- <CategoryName>: Name of the category for the required documentation. A <CategoryName> could contain additional Sub-Category-Names divided with ".".

- <ImplementationCategoryName>: Name of the implementation category which describes the defined implementation.
- <AssessmentUnitName>: Name of the assessment unit for a specific implementation category.
- <MechanismAbbreviation-<Nr>>: Abbreviation of the name from the specific requirement which belongs to the assessment criteria.

6 Requirements

6.1 [ACM] Access control mechanism

6.1.1 [ACM-1] Applicability of access control mechanisms

6.1.1.1 Requirement

The equipment shall use access control mechanisms to manage entities' access to security assets and financial assets, except for access to security assets or financial assets where:

- public accessibility is the equipment's intended functionality; or
- physical or logical measures in the equipment's targeted operational environment limit their accessibility to authorized entities; or
- legal implications do not allow for access control mechanisms.

6.1.1.2 Rationale

Security and financial assets might be exposed to unauthorized access attempts. Access control mechanisms limit the ability of any unauthorized entity to access these assets.

6.1.1.3 Guidance

The requirement does not demand access control mechanisms on assets that it does not cover (for example, the dispense button on a coffee machine). Further it does not demand access control mechanisms for security assets or financial assets that are in principle covered, but where the intended equipment functionality [36] is to be generally accessible by the public or where the intended operational environment of use ensures that only authorized access is possible. If the equipment relies on the access control given by the intended operational environment, it is to be ensured that this access control is appropriate as described in ACM-2.

Radio interfaces might be accessible even if the equipment is in an environment preventing physical manipulation by an unauthorized entity, for instance a wireless network is often accessible from outside a user's home.

For example, depending on the equipment's technical properties, intended equipment functionality and intended operational environment of use access control mechanisms might not be necessary for relevant security assets or financial assets where:

- all entities with access to the equipment (the equipment is intended to be operated in an area which has physical access control) are authorized to access these assets (for example, the WPS button on a home router);
- the equipment's functionality only provides information (on security assets or financial assets) that is intended to be publicly accessible (for instance broadcasting Bluetooth advertising beacons).

Access control mechanisms need properties to tie access rights to. Such properties can amongst others be:

- verified claims of entities (for instance being owner of a user account, member of specific group, authorized by another entity);
- certain states of the equipment or the equipment's environment (for instance an electronic flight bag might have different access rights for a local user when it is operated in the air, than when it is stored at the ground);
- the external interface an access is performed from (for instance a local access, where physical access control is obviously in place, might have different access rights than a remote access);
- various combinations of the properties mentioned, as well as additional ones.

6.1.1.4 Assessment criteria

6.1.1.4.1 Assessment objective

The assessment addresses the requirement ACM-1.

6.1.1.4.2 Implementation categories

Not applicable.

6.1.1.4.3 Required information

[E.Info.ACM-1.SecurityAsset]: Description of each security asset that is accessible by entities, including:

- [E.Info.ACM-1.SecurityAsset.Access]: possible entities' accesses to the security asset on the equipment; and
- (if access control by the equipment is absent for public accessibility of the security asset is the equipment's intended functionality) [E.Info.ACM-1.SecurityAsset.PublicAccess]: Description of the equipment's intended functionality concerning the public accessibility of the security asset; and
- (if access control by the equipment is absent because physical or logical measures in the equipment's targeted operational environment exists, that limit accessibility to authorized entities) [E.Info.ACM-1.SecurityAsset.Environment]: Description of:
 - physical or logical access control measures in the equipment's targeted operational environment; and
 - how entities are authenticated/authorized in the equipment's targeted operational environment; and
- (if legal implications do not allow for access control mechanisms) [E.Info.ACM-1.SecurityAsset.Legal]: References to all corresponding paragraph(s) or passages in all relevant legal documents, including a description on how this is applicable for the equipment or affected asset; and
- (if access control mechanisms are claimed to be required for entities access to the security asset) [E.Info.ACM-1.SecurityAsset.ACM]: Description of each access control mechanism that manages entities' access to the security asset.

[E.Info.ACM-1.FinancialAsset]: Description of each financial asset that is accessible by entities, including:

- [E.Info.ACM-1.NetworkAsset.Access]: possible entities' accesses to the financial asset on the equipment; and
- (if access control by the equipment is absent for public accessibility of the financial asset is the equipment's intended functionality) [E.Info.ACM-1.FinancialAsset.PublicAccess]: Description of the equipment's intended functionality concerning the public accessibility of the financial asset; and
- (if access control by the equipment is absent because physical or logical measures in the equipment's targeted operational environment exists, that limit accessibility to authorized entities) [E.Info.ACM-1.FinancialAsset.Environment]: Description of:
 - physical or logical access control measures in the equipment's targeted operational environment; and
 - how entities are authenticated/authorized in the equipment's targeted operational environment; and
- (if legal implications do not allow for access control mechanisms) [E.Info.ACM-1.FinancialAsset.Legal]: References to all corresponding paragraph(s) or passages in all relevant legal documents, including a description on how this is applicable for the equipment or affected asset; and
- (if access control mechanisms are claimed to be required for entities access to the financial asset) [E.Info.ACM-1.FinancialAsset.ACM]: Description of each access control mechanism that manages entities' access to the financial asset.

[E.Info.DT.ACM-1]: Description of the selected path through the decision tree in Figure 1 for each security and financial asset documented in [E.Info.ACM-1.SecurityAsset] and [E.Info.ACM-1.FinancialAsset], respectively.

[E.Just.DT.ACM-1]: Justification for the selected path through the decision tree documented in [E.Info.DT.ACM-1], with the following properties:

- (if a decision from [DT.ACM-1.DN-1] results in "NOT APPLICABLE") the justification for the decision [DT.ACM-1.DN-1] is based on [E.Info.ACM-1.SecurityAsset.PublicAccess] or [E.Info.ACM-1.FinancialAsset.PublicAccess]; and
- (if a decision from [DT.ACM-1.DN-2] results in "NOT APPLICABLE") the justification for the decision [DT.ACM-1.DN-2] is based on [E.Info.ACM-1.SecurityAsset.Environment] or [E.Info.ACM-1.FinancialAsset.Environment]; and
- (if a decision from [DT.ACM-1.DN-3] results in "NOT APPLICABLE") the justification for the decision [DT.ACM-1.DN-3] is based on [E.Info.ACM-1.SecurityAsset.Legal] or [E.Info.ACM-1.FinancialAsset.Legal]; and
- the justification for the decision [DT.ACM-1.DN-4] is based on [E.Info.ACM-1.SecurityAsset.ACM] or [E.Info.ACM-1.FinancialAsset.ACM].

6.1.1.4.4 Conceptual assessment

6.1.1.4.4.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether access control mechanisms are implemented when they are required per ACM-1.

6.1.1.4.4.2 Preconditions

None.

6.1.1.4.4.3 Assessment units

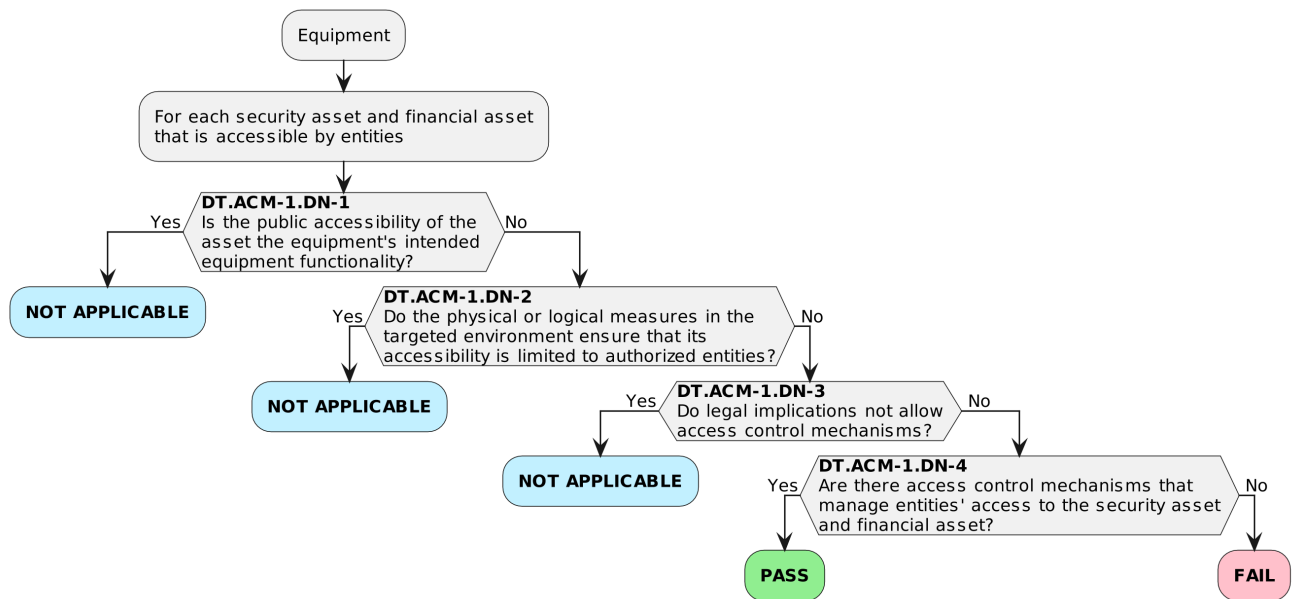


Figure 1 — Decision Tree for requirement ACM-1

For each security asset documented in [E.Info.ACM-1.SecurityAsset] and each financial asset documented in [E.Info.ACM-1.FinancialAsset], check whether the path through the decision tree documented in [E.Info.DT.ACM-1] ends with “NOT APPLICABLE” or “PASS”.

For each path through the decision tree documented in [E.Info.DT.ACM-1], examine its justification documented in [E.Just.DT.ACM-1].

6.1.1.4.4.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

- at least one path through the decision tree documented in [E.Info.DT.ACM-1] ends with “PASS”; and
- no path through the decision tree documented in [E.Info.DT.ACM-1] ends with “FAIL”; and
- the information provided in [E.Just.DT.ACM-1] are correct justifications for all paths through the decision tree documented in [E.Info.DT.ACM-1].

The verdict FAIL for the assessment case is assigned if:

- a path through the decision tree documented in [E.Info.DT.ACM-1] ends with “FAIL”; or
- a justification provided in [E.Just.DT.ACM-1] is not correct or missing for a path through the decision tree documented in [E.Info.DT.ACM-1].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.1.1.4.5 Functional completeness assessment

6.1.1.4.5.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether all the security assets and financial assets that are accessible by entities, are documented in [E.Info.ACM-1.FinancialAsset] or [E.Info.ACM-1.SecurityAsset].

6.1.1.4.5.2 Preconditions

The equipment is in an operational state.

6.1.1.4.5.3 Assessment units

Functionally assess whether there are security assets, that are accessible by entities, in the equipment, which are not documented in [E.Info.ACM-1.SecurityAsset] and whether there are network assets, that are accessible by entities, in the equipment, which are not documented in [E.Info.ACM-1.FinancialAsset], e.g. by inspecting all parts of the software such as built-in software, installed applications and interfaces for connected peripherals.

6.1.1.4.5.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if all security assets found are documented in [E.Info.ACM-1.SecurityAsset] and all financial assets found are documented in [E.Info.ACM-1.FinancialAsset].

The verdict FAIL for the assessment case is assigned if a security asset is found which is not documented in [E.Info.ACM-1.SecurityAsset] or a financial asset is found which is not documented in [E.Info.ACM-1.FinancialAsset].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.1.1.4.6 Functional sufficiency assessment

6.1.1.4.6.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether access control mechanisms are implemented when it is required per ACM-1.

6.1.1.4.6.2 Preconditions

The equipment is in an operational state.

6.1.1.4.6.3 Assessment units

For each security asset documented in [E.Info.ACM-1.SecurityAsset] and each network asset documented in [E.Info.ACM-1.FinancialAsset] functionally confirm the existence of access control mechanisms according to [E.Info.ACM-1.SecurityAsset.ACM] or [E.Info.ACM-1.FinancialAsset.ACM] by accessing the

assets following [E.Info.ACM-1.FinancialAsset.PublicAccess] and [E.Info.ACM-1.SecurityAsset.PublicAccess].

6.1.1.4.6.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if there is no evidence that an access control mechanism documented in [E.Info.ACM-1.SecurityAsset.ACM] or [E.Info.ACM-1.FinancialAsset.ACM] is not implemented.

The verdict FAIL for the assessment case is assigned if there is evidence that an access control mechanism documented in [E.Info.ACM-1.SecurityAsset.ACM] or [E.Info.ACM-1.FinancialAsset.ACM] is not implemented.

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.1.2 [ACM-2] Appropriate access control mechanisms

6.1.2.1 Requirement

Access control mechanisms that are required per ACM-1 shall ensure that only authorized entities have access to the protected security assets and financial assets.

6.1.2.2 Rationale

Security assets and financial assets may be exposed by unauthorized access attempts. Appropriate access control mechanisms ensure these assets are protected from unauthorized access.

6.1.2.3 Guidance

This requirement is intended to ensure that the access control mechanisms used to protect the relevant security assets or financial assets are chosen and configured such that unauthorized access is denied. With a variety of asset access methods and control mechanisms (for instance display on a wearable's screen), equipment use-cases and operational environments, it is difficult to specify a generic model for entities and associated access rights.

Whether an access control mechanism can deny unauthorized access, always depends on external assumptions that need to be fulfilled. For example, that the sharing of passwords or unauthorized physical access are not permitted.

Depending on the equipment's technical properties, intended operational environment of use, the access control mechanisms use appropriate properties to tie access rights to and that all involved entities are provided with authorization information.

When access control mechanisms rely on authentication mechanisms, see AUM, for example:

- an authorized entity, e.g., specific human, owner of a user account, device, or service, can after authentication access their security asset or financial asset, such as changing security configuration; or
- a member of specific authorized groups can after authentication access a security asset or financial asset; or
- an entity, authorized by another entity authorized to do so, can access a specific security asset or financial asset.

For the determination of the appropriate access control mechanisms on security assets and financial assets the following aspects are important:

- the risk associated with an entity's access to a security asset or financial asset,
- the form of access an equipment's functionality allows to a security asset or financial asset,
- the interface the security asset or financial asset is accessed through and
- the impact of access control provided by the intended operational environment of use.

For the determination of entities' access rights on security assets and financial assets (authorized entities for certain access on assets), the following aspects are important:

- the risk associated with an entity's access to a security asset or financial asset,
- the "need-to-know principle": Does an entity need to obtain some information from a security asset or financial asset,
- the "need-to-use principle": Does an entity have a valid need to use a functionality based on a security asset or financial asset,
- the "least privileges principle": everything is forbidden unless permitted,
- the equipment's clearly advertised functionality e.g., concerning accessibility of security assets or financial assets or interoperability with components of an existing infrastructure.

6.1.2.4 Assessment criteria

6.1.2.4.1 Assessment objective

The assessment addresses the requirement ACM-2.

6.1.2.4.2 Implementation categories

[IC.ACM-2.RBAC]: The methods to validate the appropriateness of the access control mechanism solely rely on role-based access control.

[IC.ACM-2.DAC]: The methods to validate the appropriateness of the access control mechanism solely rely on discretionary access control.

[IC.ACM-2.MAC]: The methods to validate the appropriateness of the access control mechanism solely rely on mandatory access control.

[IC.ACM-2.Generic]: The methods to validate the appropriateness of the access control mechanism do not solely rely on any of the methods described in ACM-2-RBAC, ACM-2-DAC or ACM-2-MAC.

6.1.2.4.3 Required information

[E.Info.ACM-2.SecurityAsset]: Description of each security asset for which ACM-1 requires access control mechanisms, including:

- [E.Info.ACM-2.SecurityAsset.ACM]: Description of the access control mechanisms required per ACM-1 that manages entities' access to the security asset and of how the mechanisms ensure that only authorized entities have access to the security asset based on the implementation category.

[E.Info.ACM-2.FinancialAsset]: Description of each financial asset for which ACM-1 requires access control mechanisms, including:

- [E.Info.ACM-2.FinancialAsset.ACM]: Description of the access control mechanisms required per ACM-1 that manages entities' access to the financial asset and of how the mechanisms ensure that only authorized entities have access to the financial asset based on the implementation category.

[E.Info.DT.ACM-2]: Description of the selected path through the decision tree in Figure 2 for each security asset documented in [E.Info.ACM-2.SecurityAsset] and financial asset documented in [E.Info.ACM-2.FinancialAsset].

[E.Just.DT.ACM-2]: Justification for each selected path through the decision tree documented in [E.Info.DT.ACM-2], with the following property:

- the justification for the decision [DT.ACM-2.DN-1] is based on [E.Info.ACM-2.FinancialAsset.ACM] or [E.Info.ACM-2.SecurityAsset.ACM].

NOTE A justification includes a description of the entities, their access rights on the respective security asset or financial asset and means how the access control mechanisms ensure that only authorised access to the respective asset is granted.

6.1.2.4.4 Conceptual assessment

6.1.2.4.4.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether the access control mechanisms that are required per ACM-1 are implemented as required per ACM-2.

6.1.2.4.4.2 Preconditions

None.

6.1.2.4.4.3 Assessment units

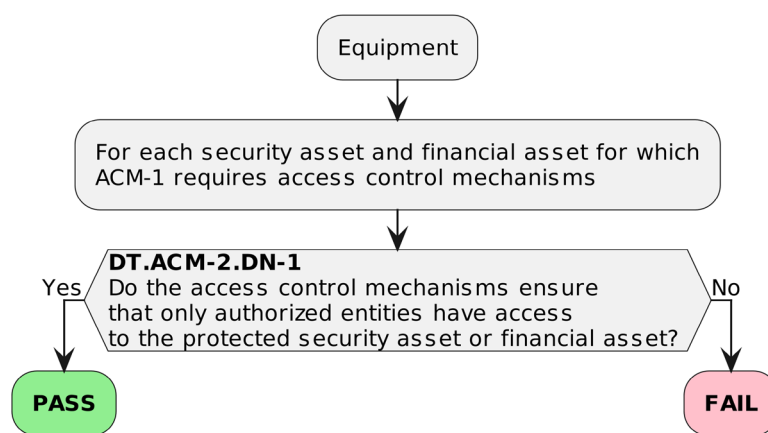


Figure 2 — Decision Tree for requirement ACM-2

For each security asset documented in [E.Info.ACM-2.SecurityAsset] and each financial asset documented in [E.Info.ACM-2.FinancialAsset], check whether the path through the decision tree documented in [E.Info.DT.ACM-2] ends with “PASS”.

For each path through the decision tree documented in [E.Info.DT.ACM-2], examine its justification documented in [E.Just.DT.ACM-2].

6.1.2.4.4.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

- all paths through the decision tree documented in [E.Info.DT.ACM-2] end with “PASS”; and
- the information provided in [E.Just.DT.ACM-2] are correct justifications for all paths through the decision tree documented in [E.Info.DT.ACM-2].

The verdict FAIL for the assessment case is assigned if:

- a path through the decision tree documented in [E.Info.DT.ACM-2] ends with “FAIL”; or
- a justification provided in [E.Just.DT.ACM-2] is not correct or missing for a path through the decision tree documented in [E.Info.DT.ACM-2].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.1.2.4.5 Functional completeness assessment

The functional completeness assessment is covered by the functional sufficiency assessment of the access control mechanism’s applicability.

Therefore, this functional completeness assessment is not necessary.

6.1.2.4.6 Functional sufficiency assessment

6.1.2.4.6.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether the access control mechanisms are implemented as required per ACM-2.

6.1.2.4.6.2 Assessment units

For each security asset documented in [E.Info.ACM-2.SecurityAsset] and financial asset documented in [E.Info.ACM-2.FinancialAsset]:

[AU.ACM-2.RBAC]: If the access control mechanisms documented in [E.Info.ACM-2.SecurityAsset.ACM] or [E.Info.ACM-2.FinancialAsset.ACM] belong to [IC.ACM-2.RBAC], functionally confirm that:

- roles are assigned to each user with associated authorization; and
- least privileges are associated with the roles; and
- the security asset or financial asset is only accessible by authorized users given by their role; and
- changes in roles can only be performed by authorized users.

[AU.ACM-2.DAC]: If the access control mechanisms documented in [E.Info.ACM-2.SecurityAsset.ACM] or [E.Info.ACM-2.FinancialAsset.ACM] belong to [IC.ACM-2.DAC], functionally confirm that:

- identities are assigned to each user with associated authorization; and
- least privileges are associated with the identities; and
- the security asset or financial asset is only accessible by authorized users given by their identity; and

- changes in identities can only be performed by authorized users.

[AU.ACM-2.MAC]: If the access control mechanisms documented in [E.Info.ACM-2.SecurityAsset.ACM] or [E.Info.ACM-2.FinancialAsset.ACM] belong to [IC.ACM-2.MAC], functionally confirm that:

- the security asset or financial asset is only accessible by authorized users after clearance was issued by the operating system and/or system administrator; and
- the issuance of clearance is associated with the principle of least privileges; and
- changing the operating system and/or system administrator that is responsible for the issuance of clearance to the user can only be performed by the authorized system administrator.

[AU.ACM-2.Generic]: If the access control mechanisms documented in [E.Info.ACM-2.SecurityAsset.ACM] or [E.Info.ACM-2.FinancialAsset.ACM] belong to [IC.ACM-2.Generic], functionally confirm that:

- the security asset or financial asset is only accessible by authorized users; and
- the principle of least privileges for users is followed; and
- changing settings related to the access control mechanism or changes of privileges of users are only allowed to be performed by authorized users.

6.1.2.4.6.3 Assignment of verdict

The verdict PASS for the assessment case is assigned if for each security asset documented in [E.Info.ACM-2.SecurityAsset] and financial asset documented in [E.Info.ACM-2.FinancialAsset] the confirmations in the implementation category dependent assessment unit are successful.

The verdict FAIL for the assessment case is assigned if for any security asset documented in [E.Info.ACM-2.SecurityAsset] or financial asset documented in [E.Info.ACM-2.FinancialAsset] a confirmation in the implementation category dependent assessment unit is not successful.

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.2 [AUM] Authentication mechanism

6.2.1 [AUM-1] Applicability of authentication mechanisms

6.2.1.1 [AUM-1-1] Requirement network interface

Access control mechanisms required per ACM-1 shall use authentication mechanisms for managing entities' access via network interfaces that allow to:

- read confidential financial data, confidential financial function configuration or confidential security parameters; or
- modify sensitive financial data, sensitive financial function configuration or sensitive security parameters; or
- use financial functions or security functions.

6.2.1.2 [AUM-1-2] Requirement user interface

Access control mechanisms required per ACM-1 shall use authentication mechanisms for managing entities' access via user interfaces that allow to:

- read confidential financial data, confidential financial function configuration or confidential security parameters; or
- modify sensitive financial data, sensitive financial function configuration or sensitive security parameters; or
- use financial functions or security functions.

6.2.1.3 [AUM-1-3] Requirement machine interface

Access control mechanisms required per ACM-1 shall use authentication mechanisms for managing entities' access via machine interfaces that allow to:

- read confidential financial data, confidential financial function configuration or confidential security parameters; or
- modify sensitive financial data, sensitive financial function configuration or sensitive security parameters; or
- use financial functions or security functions.

6.2.1.4 Rationale

The equipment needs to provide an authentication mechanism such that the corresponding access control mechanism prevents unauthorized access to assets that can be used for fraud from entities which are not who or what they claim to be.

6.2.1.5 Guidance

Authentication mechanisms might use different layers (e.g., application or network layer) for verifying the validity of entities' claims. The management of associated access rights for entities are addressed by access control mechanisms.

There are different kinds of entities that can interact with the equipment, e.g.:

- a specific human, owner of a user account, device or service; or
- a member of specific groups such as an authorized group to access a specific equipment's resource; or
- authorised by another entity to access a specific equipment's resource.

Typically, the verification of an entity is based on examining evidence from one or more elements of the categories:

- knowledge (something you know); and
- possession (something you have); and
- inherence (something you are).

A trust relation to a network (e.g., an entity owns a shared secret like Wi-Fi credentials) could be used to authenticate an entity.

Authentication might not be needed for all accesses to security assets or financial assets.

Examples of access where authentication might not be mandatory are amongst others:

- reading information which is clearly advertised as publicly accessible information related to the intended equipment functionality; or
- reading a public key.

6.2.1.6 Assessment criteria network interface

6.2.1.6.1 Assessment objective

The assessment addresses the requirement AUM-1-1.

6.2.1.6.2 Implementation categories

Not applicable.

6.2.1.6.3 Required information

[E.Info.AUM-1-1.ACM]: Description of each access control mechanism required per ACM-1 for managing entities' access over network interfaces that allow to read confidential financial information, confidential financial function configuration or confidential security parameters; or modify sensitive financial information, sensitive financial function configuration or sensitive security parameters; or use financial functions or security functions, including:

- [E.Info.AUM-1-1.ACM.NetworkInterface]: Description of the network interfaces for the managed access; and
- [E.Info.AUM-1-1.ACM.ManagedAccessFinancialAsset]: Description of the managed access to financial assets via network interfaces; and
- [E.Info.AUM-1-1.ACM.ManagedAccessSecurityAsset]: Description of the managed access to security assets via network interfaces; and
- [E.Info.AUM-1-1.ACM.AuthenticationMechanism]: Description of the implemented authentication mechanisms.

[E.Info.DT.AUM-1-1]: Description of the selected path through the decision tree in Figure 3 for each access control mechanism documented in [E.Info.AUM-1-1.ACM].

[E.Just.DT.AUM-1-1]: Justification for the selected path through the decision tree documented in [E.Info.DT.AUM-1-1] with the following property:

- the justification for the decision [DT.AUM-1-1.DN-1] is based on [E.Info.AUM-1-1.ACM].

6.2.1.6.4 Conceptual assessment

6.2.1.6.4.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether an authentication mechanism is implemented when it is required per AUM-1-1.

6.2.1.6.4.2 Preconditions

None.

6.2.1.6.4.3 Assessment units

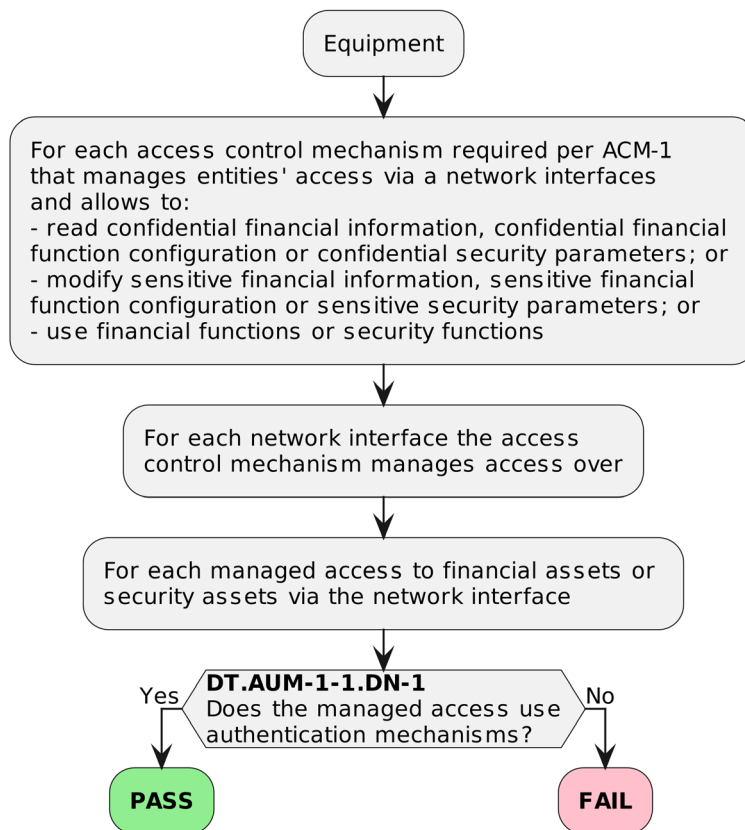


Figure 3 — Decision Tree for requirement AUM-1-1

For each access control mechanism documented in [E.Info.AUM-1-1.ACM], check whether the path through the decision tree documented in [E.Info.DT.AUM-1-1] ends with “NOT APPLICABLE” or “PASS”.

For each path through the decision tree documented in [E.Info.DT.AUM-1-1], examine its justification documented in [E.Just.DT.AUM-1-1].

6.2.1.6.4.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

- all paths through the decision tree documented in [E.Info.DT.AUM-1-1] ends with “PASS”; and
- the information provided in [E.Just.DT.AUM-1-1] are correct justifications for all paths through the decision tree documented in [E.Info.DT.AUM-1-1].

The verdict FAIL for the assessment case is assigned if:

- a path through the decision tree documented in [E.Info.DT.AUM-1-1] ends with “FAIL”; or
- a justification provided in [E.Just.DT.AUM-1-1] is not correct or missing for a path through the decision tree documented in [E.Info.DT.AUM-1-1].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.2.1.6.5 Functional completeness assessment

6.2.1.6.5.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether there are access control mechanisms on the equipment for managing entities' access over network interfaces that allow to read confidential financial information, confidential financial function configuration or confidential security parameters; or modify sensitive financial information, sensitive financial function configuration or sensitive security parameters; or use financial functions or security functions that are not described in [E.Info.AUM-1-1.ACM].

6.2.1.6.5.2 Preconditions

The equipment is in an operational state.

6.2.1.6.5.3 Assessment units

Functionally assess whether there are access control mechanisms required per ACM-1 for managing entities' access over network interfaces that allow to read confidential financial information, confidential financial function configuration or confidential security parameters; or modify sensitive financial information, sensitive financial function configuration or sensitive security parameters; or use financial functions or security functions that are not described in [E.Info.AUM-1-1.ACM].

6.2.1.6.5.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if there is no evidence that an access control mechanism required per ACM-1 for managing entities' access over network interfaces that allow to read confidential financial information, confidential financial function configuration or confidential security parameters; or modify sensitive financial information, sensitive financial function configuration or sensitive security parameters; or use financial functions or security functions, is found that is not documented in [E.Info.AUM-1-1.ACM].

The verdict FAIL for the assessment case is assigned if there is evidence that an access control mechanism required per ACM-1 for managing entities' access over network interfaces that allow to read confidential financial information, confidential financial function configuration or confidential security parameters; or modify sensitive financial information, sensitive financial function configuration or sensitive security parameters; or use financial functions or security functions, is found that is not documented in [E.Info.AUM-1-1.ACM].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.2.1.6.6 Functional sufficiency assessment

6.2.1.6.6.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether the documented authentication mechanisms required per AUM-1-1 are implemented.

6.2.1.6.6.2 Preconditions

The equipment is in an operational state.

6.2.1.6.6.3 Assessment units

For each access control mechanisms documented in [E.Info.AUM-1-1.ACM], each managed access via network interfaces to financial assets documented in [E.Info.AUM-1-

1.ACM.ManagedAccessFinancialAsset] and each managed access via network interfaces to security assets documented in [E.Info.AUM-1-1.ACM.ManagedAccessSecurityAsset], access the corresponding assets and check whether the authentication mechanism is implemented.

6.2.1.6.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if there is no evidence that an authentication mechanism documented in [E.Info.AUM-1-1.ACM.AuthenticationMechanism] is not implemented.

The verdict FAIL for the assessment case is assigned if there is evidence that an authentication mechanism documented in [E.Info.AUM-1-1.ACM.AuthenticationMechanism] is not implemented.

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.2.1.7 Assessment criteria user interface

6.2.1.7.1 Assessment objective

The assessment addresses the requirement AUM-1-2.

6.2.1.7.2 Implementation categories

Not applicable.

6.2.1.7.3 Required information

[E.Info.AUM-1-2.ACM]: Description of each access control mechanism required per ACM-1 for managing entities' access over user interfaces that allow to read confidential financial information, confidential financial function configuration or confidential security parameters; or modify sensitive financial information, sensitive financial function configuration or sensitive security parameters; or use financial functions or security functions, including:

- [E.Info.AUM-1-2.ACM.UserInterfaces]: A description of the user interfaces for the managed access; and
- [E.Info.AUM-1-2.ACM.ManagedAccessFinancialAsset]: Description of the managed access to financial assets via user interfaces; and
- [E.Info.AUM-1-2.ACM.ManagedAccessSecurityAsset]: Description of the managed access to security assets via user interfaces; and
- [E.Info.AUM-1-2.ACM.AuthenticationMechanism]: Description of the implemented authentication mechanisms.

[E.Info.DT.AUM-1-2]: Description of the selected path through the decision tree in Figure 4 for each access control mechanism documented in [E.Info.AUM-1-2.ACM].

[E.Just.DT.AUM-1-2]: Justification for the path through the decision tree documented in [E.Info.DTAUM-1-2] with the following property:

- the justification for the decision [DT.AUM-1-2.DN-1] is based on [E.Info.AUM-1-2.ACM].

6.2.1.7.4 Conceptual assessment

6.2.1.7.4.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether an authentication mechanism is implemented when it is required per AUM-1-2.

6.2.1.7.4.2 Preconditions

None.

6.2.1.7.4.3 Assessment units

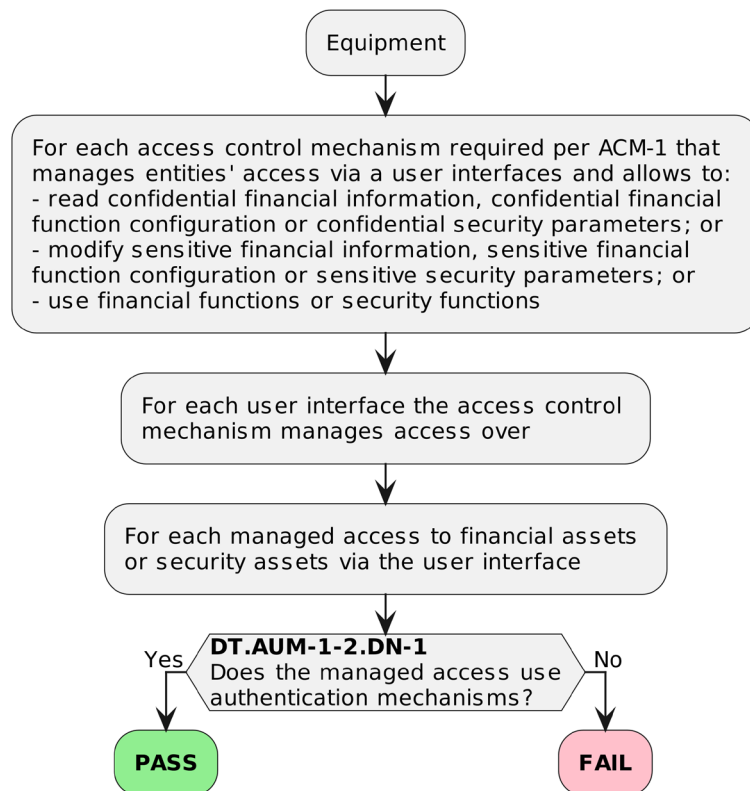


Figure 4 — Decision Tree for requirement AUM-1-2

For each access control mechanism documented in [E.Info.AUM-1-2.ACM], check whether the path through the decision tree documented in [E.Info.DT.AUM-1-2] ends with “NOT APPLICABLE” or “PASS”.

For each path through the decision tree documented in [E.Info.DT.AUM-1-2], examine its justification documented in [E.Just.DT.AUM-1-2].

6.2.1.7.4.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

- all paths through the decision tree documented in [E.Info.DT.AUM-1-2] end with “PASS”; and
- the information provided in [E.Just.DT.AUM-1-2] are correct justifications for all paths through the decision tree documented in [E.Info.DT.AUM-1-2].

The verdict FAIL for the assessment case is assigned if:

- a path through the decision tree documented in [E.Info.DT.AUM-1-2] ends with “FAIL”; or
- a justification provided in [E.Just.DT.AUM-1-2] is not correct or missing for a path through the decision tree documented in [E.Info.DT.AUM-1-2].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.2.1.7.5 Functional completeness assessment

6.2.1.7.5.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether there are access control mechanisms on the equipment for managing entities’ access over user interfaces that allow to read confidential financial information, confidential financial function configuration or confidential security parameters; or modify sensitive financial information, sensitive financial function configuration or sensitive security parameters; or use financial functions or security functions that are not described in [E.Info.AUM-1-2.ACM].

6.2.1.7.5.2 Preconditions

The equipment is in an operational state.

6.2.1.7.5.3 Assessment units

Functionally assess whether there are access control mechanisms required per ACM-1 for managing entities’ access over user interfaces that allow to read confidential financial information, confidential financial function configuration or confidential security parameters; or modify sensitive financial information, sensitive financial function configuration or sensitive security parameters; or use financial functions or security functions that are not described in [E.Info.AUM-1-2.ACM].

6.2.1.7.5.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if there is no evidence that an access control mechanism required per ACM-1 for managing entities’ access over user interfaces that allow to read confidential financial information, confidential financial function configuration or confidential security parameters; or modify sensitive financial information, sensitive financial function configuration or sensitive security parameters; or use financial functions or security functions, is found that is not documented in [E.Info.AUM-1-2.ACM].

The verdict FAIL for the assessment case is assigned if there is evidence that an access control mechanism required per ACM-1 for managing entities’ access over user interfaces that allow to read confidential financial information, confidential financial function configuration or confidential security parameters; or modify sensitive financial information, sensitive financial function configuration or sensitive security parameters; or use financial functions or security functions, is found that is not documented in [E.Info.AUM-1-2.ACM].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.2.1.7.6 Functional sufficiency assessment

6.2.1.7.6.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether the documented authentication mechanisms required per AUM-1-2 are implemented.

6.2.1.7.6.2 Preconditions

The equipment is in an operational state.

6.2.1.7.6.3 Assessment units

For each access control mechanism documented in [E.Info.AUM-1-2.ACM], each managed access via user interfaces to financial assets documented in [E.Info.AUM-1-2.ACM.ManagedAccessFinancialAsset] and each managed access via user interfaces to security assets documented in [E.Info.AUM-1-2.ACM.ManagedAccessSecurityAsset], access the corresponding security assets and financial assets and check whether the authentication mechanism is implemented.

6.2.1.7.6.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if there is no evidence that an authentication mechanism documented in [E.Info.AUM-1-2.ACM.AuthenticationMechanism] is not implemented.

The verdict FAIL for the assessment case is assigned if there is evidence that an authentication mechanism documented in [E.Info.AUM-1-2.ACM.AuthenticationMechanism] is not implemented.

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.2.1.8 Assessment criteria machine interface

6.2.1.8.1 Assessment objective

The assessment addresses the requirement AUM-1-3.

6.2.1.8.2 Implementation categories

Not applicable.

6.2.1.8.3 Required information

[E.Info.AUM-1-3.ACM]: Description of each access control mechanism required per ACM-1 for managing entities' access over machine interfaces that allow to read confidential financial information, confidential financial function configuration or confidential security parameters; or modify sensitive financial information, sensitive financial function configuration or sensitive security parameters; or use financial functions or security functions, including:

- [E.Info.AUM-1-3.ACM.MachineInterfaces]: A description of the machine interfaces for the managed access; and
- [E.Info.AUM-1-3.ACM.ManagedAccessFinancialAsset]: Description of the managed access to financial assets via machine interfaces; and
- [E.Info.AUM-1-3.ACM.ManagedAccessSecurityAsset]: Description of the managed access to security assets via machine interfaces; and
- [E.Info.AUM-1-3.ACM.AuthenticationMechanism]: Description of the implemented authentication mechanisms.

[E.Info.DT.AUM-1-3]: Description of the selected path through the decision tree in Figure 5 for each access control mechanism documented in [E.Info.AUM-1-3.ACM].

[E.Just.DT.AUM-1-3]: Justification for the path through the decision tree documented in [E.Info.DT.AUM-1-2] with the following property:

- the justification for the decision [DT.AUM-1-3.DN-1] is based on [E.Info.AUM-1-3.ACM].

6.2.1.8.4 Conceptual assessment

6.2.1.8.4.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether an authentication mechanism is implemented when it is required per AUM-1-3.

6.2.1.8.4.2 Preconditions

None.

6.2.1.8.4.3 Assessment units

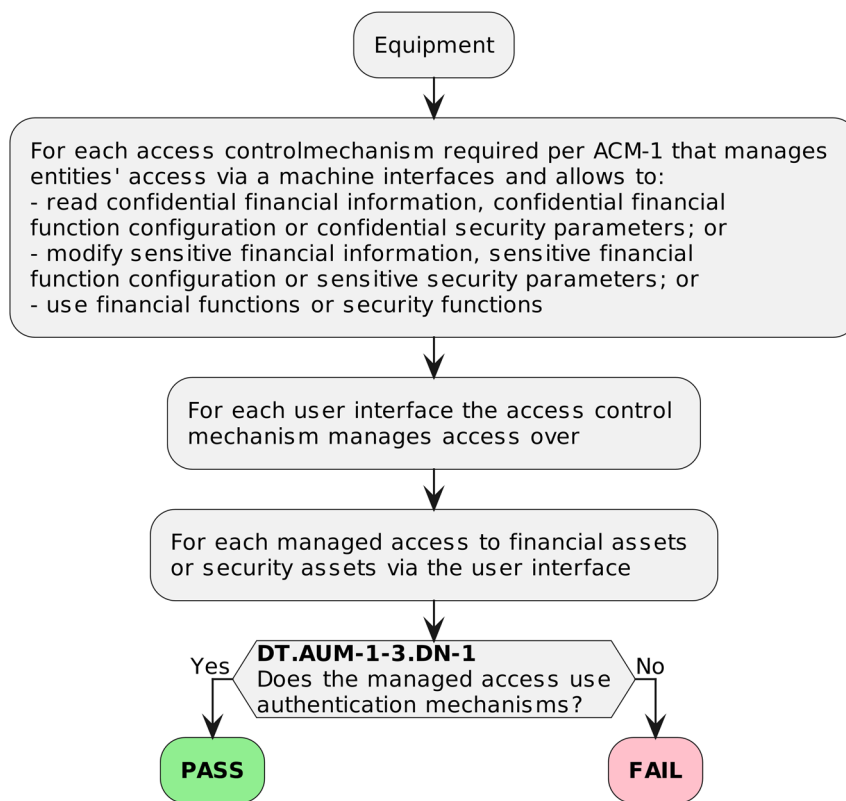


Figure 5 — Decision Tree for requirement AUM-1-3

For each access control mechanism documented in [E.Info.AUM-1-3.ACM], check whether the path through the decision tree documented in [E.Info.DT.AUM-1-3] ends with “NOT APPLICABLE” or “PASS”.

For each path through the decision tree documented in [E.Info.DT.AUM-1-3], examine its justification documented in [E.Just.DT.AUM-1-3].

6.2.1.8.4.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

- all paths through the decision tree documented in [E.Info.DT.AUM-1-3] end with “PASS”; and

- the information provided in [E.Just.DT.AUM-1-3] are correct justifications for all paths through the decision tree documented in [E.Info.DT.AUM-1-3].

The verdict FAIL for the assessment case is assigned if:

- a path through the decision tree documented in [E.Info.DT.AUM-1-3] ends with “FAIL”; or
- a justification provided in [E.Just.DT.AUM-1-3] is not correct or missing for a path through the decision tree documented in [E.Info.DT.AUM-1-3].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.2.1.8.5 Functional completeness assessment

6.2.1.8.5.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether there are access control mechanisms on the equipment for managing entities’ access over user interfaces that allow to read confidential financial information, confidential financial function configuration or confidential security parameters; or modify sensitive financial information, sensitive financial function configuration or sensitive security parameters; or use financial functions or security functions that are not described in [E.Info.AUM-1-2.ACM].

6.2.1.8.5.2 Preconditions

The equipment is in an operational state.

6.2.1.8.5.3 Assessment units

Functionally assess whether there are access control mechanisms required per ACM-1 for managing entities’ access over machine interfaces that allow to read confidential financial information, confidential financial function configuration or confidential security parameters; or modify sensitive financial information, sensitive financial function configuration or sensitive security parameters; or use financial functions or security functions that are not described in [E.Info.AUM-1-3.ACM].

6.2.1.8.5.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if there is no evidence that an access control mechanism required per ACM-1 for managing entities’ access over machine interfaces that allow to read confidential financial information, confidential financial function configuration or confidential security parameters; or modify sensitive financial information, sensitive financial function configuration or sensitive security parameters; or use financial functions or security functions, is found that is not documented in [E.Info.AUM-1-3.ACM].

The verdict FAIL for the assessment case is assigned if there is evidence that an access control mechanism required per ACM-1 for managing entities’ access over machine interfaces that allow to read confidential financial information, confidential financial function configuration or confidential security parameters; or modify sensitive financial information, sensitive financial function configuration or sensitive security parameters; or use financial functions or security functions, is found that is not documented in [E.Info.AUM-1-3.ACM].

6.2.1.8.6 Functional sufficiency assessment

6.2.1.8.6.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether the documented authentication mechanisms required per AUM-1-3 are implemented.

6.2.1.8.6.2 Preconditions

The equipment is in an operational state.

6.2.1.8.6.3 Assessment units

For each access control mechanisms documented in [E.Info.AUM-1-3.ACM] and each managed access via machine interfaces to financial assets documented in [E.Info.AUM-1-3.ACM.ManagedAccessFinancialAsset] and each managed access via machine interfaces to security assets documented in [E.Info.AUM-1-3.ACM.ManagedAccessSecurityAsset], access the corresponding assets and check whether the authentication mechanism is implemented.

6.2.1.8.6.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if there is no evidence that an authentication mechanism documented in [E.Info.AUM-1-3.ACM.AuthenticationMechanism] is not implemented.

The verdict FAIL for the assessment case is assigned if there is evidence that an authentication mechanism documented in [E.Info.AUM-1-3.ACM.AuthenticationMechanism] is not implemented.

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.2.2 [AUM-2] Appropriate authentication mechanisms

6.2.2.1 [AUM-2-1] Requirement one factor authentication

Authentication mechanisms that are required per AUM-1-1 (network interface), AUM-1-2 (user interface) or AUM-1-3 (machine interface) shall verify an entity's claim based on evidence derived from at least one element of the categories knowledge, possession and inherence (one factor authentication).

6.2.2.2 [AUM-2-2] Requirement two factor authentication

Authentication mechanisms that are required per AUM-1-1 (network interface) or AUM-1-2 (user interface) for access to financial functions via user interfaces over network interface that transfer money, monetary assets or virtual currencies shall verify an entity's claim based on evidence derived from at least two different elements of the categories knowledge, possession and inherence (two factor authentication).

6.2.2.3 Rationale

One factor authentication is suitable to prevent unauthorized access to security assets or financial assets that can be used for fraud from entities which are not who or what they claim to be. The management of associated access rights for entities is addressed by access control mechanisms.

The ability to perform financial transactions over a network needs strong user authentication to deny fraudulent transactions over the network e.g., based on weak user passwords. Therefore at least two factor authentication is required in this case.

6.2.2.4 Guidance

Examples for a verification of an entity's claim based on examining evidence from one element of the categories, knowledge, possession and inference, are:

- PIN-Code used for user interface
- 1-Factor (e.g., password based) of each incoming connection on a user or network interface
- fingerprint biometrics or face recognition for a user interface
- verifying the possession of a private key that matches to a trusted certificate
- trust relation to a network (e.g., based on a common secret) established at on-boarding.

Examples for a verification of an entity's claim based on evidence derived from at least two different elements of the categories, knowledge, possession and inference, are:

- Password + OTP
- PIN + Smartcard
- Password + Token

If a user is accessing the equipment through a software application running on another device, such as a maintenance application running on a server or laptop, this can, depending on the architecture, be considered a software process accessing the equipment. Hence, the authentication for software processes can apply. Strong authentication, including possibly multi-factor authentication, can be used for the user to authenticate to the external software application. It is also possible to use cryptographic measures to create a trust relationship between the equipment and another device such that the possession of the other device can be considered as one authentication factor. The two-factor authentication to access the equipment might be ensured through another device in the operational environment of the equipment.

Considering possible constraints of human users with disabilities is an important aspect for implementing appropriate authentication mechanisms. Examples of considerations when selecting authentication mechanisms include:

- transferring the authentication information to and from a relevant assistive technology,
- enabling a dual or shared use when the equipment is in use by a user and a support worker (and/or parent and child),
- offering alternative authentication mechanisms so that they are useable by a user with specific learning impairments (including dyslexia) and do not trigger negative feelings (e.g., by avoiding specifying family or personal information which may be distressing or not relevant for the end user).

At the time of publishing the present document long passwords like “WeihnachtsmarkTElephanT CarpeT2023@Bon(n)” are considered stronger passwords than short passwords like “P@ssw0rd!” and more guidance on current best practice on passwords can be found in NIST Special Publication 800-63B [10], ISO/IEC EN 27002:2022 [3], ISO/IEC EN 24760 [4], IEC EN 62443-4-2 [2] and ETSI EN 303 645 [6].

6.2.2.5 Assessment criteria one factor authentication

6.2.2.5.1 Assessment objective

The assessment addresses the requirement AUM-2-1.

6.2.2.5.2 Implementation categories

Not applicable.

6.2.2.5.3 Required information

[E.Info.AUM-2-1.AuthenticationMechanism]: Description of each authentication mechanism required per AUM-1-1 (network interface), AUM-1-2 (user interface) or AUM-1-3 (machine interface) including:

- [E.Info.AUM-2-1.AuthenticationMechanism.AuthFactor]: Description of the authenticators including their categories (knowledge, possession, and inherence).

[E.Info.DT.AUM-2-1]: Description of the selected path through the decision tree in Figure 6 for each authentication mechanism documented in [E.Info.AUM-2-1.AuthenticationMechanism].

[E.Just.DT.AUM-2-1]: Justification for the selected path through the decision tree documented in [E.Just.DT.AUM-2-1] with the following property:

- the justification for the decision [DT.AUM-2-1.DN-1] is based on [E.Info.AUM-2-1.AuthenticationMechanism.AuthFactor].

6.2.2.5.4 Conceptual assessment

6.2.2.5.4.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether the authentication mechanism that are required per AUM-1-1 (network interface), AUM-1-2 (user interface) or AUM-1-3 (machine interface) are implemented as required per AUM-2-1.

6.2.2.5.4.2 Preconditions

None.

6.2.2.5.4.3 Assessment units

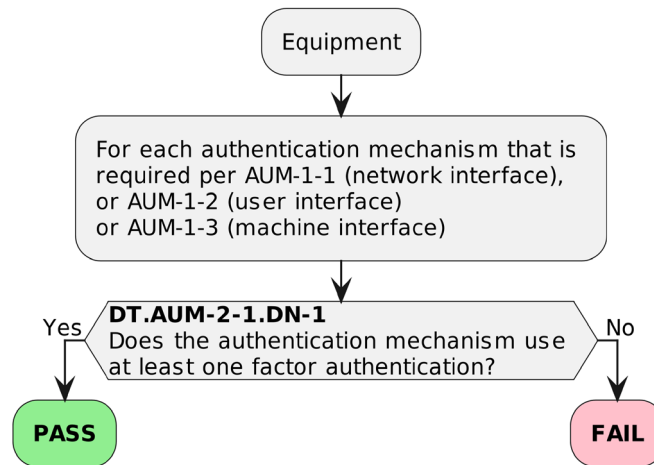


Figure 6 — Decision Tree for requirement AUM-2-1

For each authentication mechanism documented in [E.Info.AUM-2-1.AuthenticationMechanism], check whether the path through the decision tree documented in [E.Info.DT.AUM-2-1] ends with “PASS”.

For each path through the decision tree documented in [E.Info.DT.AUM-2-1], examine its justification documented in [E.Just.DT.AUM-2-1].

6.2.2.5.4.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

- all paths through the decision tree documented in [E.Info.DT.AUM-2-1] end with “PASS”; and
- the information provided in [E.Just.DT.AUM-2-1] are correct justifications for all paths through the decision tree documented in [E.Info.DT.AUM-2-1].

The verdict FAIL for the assessment case is assigned if:

- a path through the decision tree documented in [E.Info.DT.AUM-2-1] ends with “FAIL”; or
- a justification provided in [E.Just.DT.AUM-2-1] is not correct or missing for a path through the decision tree documented in [E.Info.DT.AUM-2-1].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.2.2.5.5 Functional completeness assessment

The functional completeness assessment is covered by the functional sufficiency assessment of the authentication mechanism’s applicability.

Therefore, this functional completeness assessment is not necessary.

6.2.2.5.6 Functional sufficiency assessment

6.2.2.5.6.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether the authentication mechanisms that are required per AUM-1-1 (network interface), AUM-1-2 (user interface) or AUM-1-3 (machine interface) are implemented as documented in [E.Info.AUM-2-1.AuthenticationMechanism.AuthFactor].

6.2.2.5.6.2 Preconditions

The equipment is in an operational state.

6.2.2.5.6.3 Assessment units

For each authentication mechanism that is required per AUM-1-1 (network interface), AUM-1-2 (user interface) or AUM-1-3 (machine interface) documented in [E.Info.AUM-2-1.AuthenticationMechanism], perform the authentication and check whether the authentication mechanism is implemented as documented.

6.2.2.5.6.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if there is no evidence that an authentication mechanism's implementation deviates from [E.Info.AUM-2-1.AuthenticationMechanism].

The verdict FAIL for the assessment case is assigned if there is evidence that an authentication mechanism's implementation deviates from [E.Info.AUM-2-1.AuthenticationMechanism].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.2.2.6 Assessment criteria two factor authentication

6.2.2.6.1 Assessment objective

The assessment addresses the requirement AUM-2-2.

6.2.2.6.2 Implementation categories

Not applicable.

6.2.2.6.3 Required information

[E.Info.AUM-2-2.AuthenticationMechanism]: Description of each authentication mechanism required per AUM-1-1 (network interface) or AUM-1-2 (user interface) and used for access to financial functions that transfer money, monetary assets or virtual currencies, via user interfaces over network interfaces including:

- [E.Info.AUM-2-2.AuthenticationMechanism.AuthFactor]: Description of each authenticator including categories (knowledge, possession, and inherence).

[E.Info.DT.AUM-2-2]: Description of the selected path through the decision tree in Figure 7 for each authentication mechanism documented in [E.Info.AUM-2-2.AuthenticationMechanism].

[E.Just.DT.AUM-2-2]: Justification for the selected path through the decision documented in [E.Info.DT.AUM-2-2] with the following property:

- The justification for the decision [DT.AUM-2-2.DN-1] is based on [E.Info.AUM-2-2.AuthenticationMechanism] and [E.Info.AUM-2-2.AuthenticationMechanism.AuthFactor].

6.2.2.6.4 Conceptual assessment

6.2.2.6.4.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether the authentication mechanism required per AUM-1-1 (network interface) or AUM-1-2 (user interface) are implemented as required per AUM-2-2.

6.2.2.6.4.2 Preconditions

None.

6.2.2.6.4.3 Assessment units

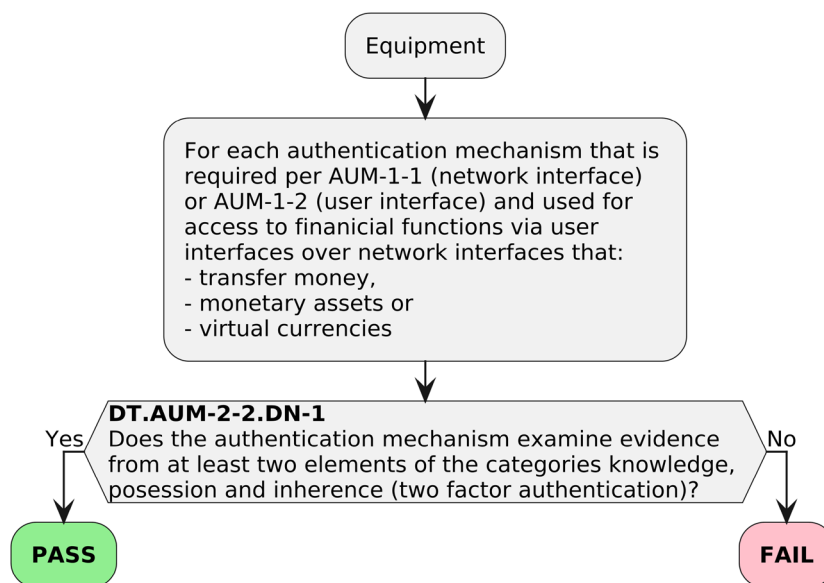


Figure 7 — Decision Tree for requirement AUM-2-2

For each authentication mechanism documented in [E.Info.AUM-2-2.AuthenticationMechanism], check whether the path through the decision tree documented in [E.Info.DT.AUM-2-2] ends with “PASS”.

For each path through the decision tree documented in [E.Info.DT.AUM-2-2], examine its justification documented in [E.Just.DT.AUM-2-2].

6.2.2.6.4.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

- all paths through the decision tree documented in [E.Info.DT.AUM-2-2] end with “PASS”; and
- the information provided in [E.Just.DT.AUM-2-2] are correct justifications for all paths through the decision tree documented in [E.Info.DT.AUM-2-2].

The verdict FAIL for the assessment case is assigned if:

- a path through the decision tree documented in [E.Info.DT.AUM-2-2] ends with “FAIL”; or

- a justification provided in [E.Just.DT.AUM-2-2] is not correct or missing for a path through the decision tree documented in [E.Info.DT.AUM-2-2].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.2.2.6.5 Functional completeness assessment

The functional completeness assessment is covered by the functional sufficiency assessment of the authentication mechanism's applicability.

Therefore, this functional completeness assessment is not necessary.

6.2.2.6.6 Functional sufficiency assessment

6.2.2.6.6.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether the authentication mechanisms that are required per AUM-1-1 (network interface) or AUM-1-2 (user interface) are implemented as documented in [E.Info.AUM-2-2.AuthenticationMechanism.AuthFactor].

6.2.2.6.6.2 Preconditions

The equipment is in an operational state.

6.2.2.6.6.3 Assessment units

For each authentication mechanism that is required per AUM-1-1 (network interface) or AUM-1-2 (user interface) documented in [E.Info.AUM-2-2.AuthenticationMechanism], perform the authentication and check whether the authentication mechanism is implemented as documented.

6.2.2.6.6.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if there is no evidence that an authentication mechanism's implementation deviates from [E.Info.AUM-2-2.AuthenticationMechanism].

The verdict FAIL for the assessment case is assigned if there is evidence that an authentication mechanism's implementation deviates from [E.Info.AUM-2-2.AuthenticationMechanism].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.2.3 [AUM-3] Authenticator validation

6.2.3.1 Requirement

Authentication mechanisms that are required per AUM-1-1 (network interface), AUM-1-2 (user interface) or AUM-1-3 (machine interface) shall validate all relevant properties of the used authenticators, dependent on the available information in the operational environment of use.

6.2.3.2 Rationale

Even when the equipment provides an authentication mechanism, the risk is given that an attacker uses typical design weaknesses to overcome it. The usage of forged or partially forged authenticators are often used for an attack against such a mechanism. Therefore, the security design of the mechanisms needs techniques to resist forged authenticators, for example manipulated PKI certificates.

6.2.3.3 Guidance

The authenticator and its attributes can vary depending on the authentication mechanism. For the validation of the authenticator, best practice ought to be applied for the corresponding authentication mechanism. This is necessary in order to detect and prevent the use of an authenticator that is invalid. For example, if the equipment only validates the common name of a PKI certificate without further validation of the complete certification information, then a correspondingly forged authenticator would be accepted. In this example, the relevant properties of the authenticator are the signatures and public keys of the trust chain, the revocation status and in many cases also the validity period of the certificate. The set of relevant properties can differ depending on whether the equipment is actually internet connected or not. For example, offline equipment probably does not have access to a reliable time source or to certificate revocation information.

Another example for insufficient validation of authenticators is, if only parts of the password is checked. This would weaken the strength of the password, facilitating brute force attacks on the corresponding authentication mechanism.

6.2.3.4 Assessment criteria

6.2.3.4.1 Assessment objective

The assessment addresses the requirement AUM-3.

6.2.3.4.2 Implementation categories

[IC.AUM-3.Password]: The authenticator is a password.

[IC.AUM-3.CertificatePrivateKey]: The authenticator is a private key associated to a certificate trusted by the equipment.

NOTE A certificate can be trusted by the equipment for example via a chain of trust to a preinstalled root certificate of a PKI or by certificate pinning.

[IC.AUM-3.Generic]: The authenticator is different from [IC.AUM-3.Password] or [IC.AUM-3.CertificatePrivateKey].

EXAMPLE Biometrics, Secure Shell (SSH) keys, symmetric keys

6.2.3.4.3 Required information

[E.Info.AUM-3.AUM]: Description of each authentication mechanism required per AUM-1-1 (network interface), AUM-1-2 (user interface) or AUM-1-3 (machine interface), including:

- [E.Info.AUM-3.AUM.AuthVal]: Description how the validation of the authenticator is performed including its implementation category and the relevant properties; and
- [E.Info.AUM-3.AUM.AuthEnv]: Description of the available information about the authenticator in the operational environment of use.

[E.Info.DT.AUM-3]: Description of the selected path through the decision tree in Figure 8 for each authentication mechanism that is documented in [E.Info.AUM-3.AUM].

[E.Just.DT.AUM-3]: Justification for the selected path through the decision tree documented in [E.Info.DT.AUM-3] with the following property:

- the justification for the decision [DT.AUM-3.DN-1] is based on [E.Info.AUM-3.AUM.AuthVal] and [E.Info.AUM-3.AUM.AuthEnv].

6.2.3.4.4 Conceptual assessment

6.2.3.4.4.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether the authentication mechanisms validate all relevant properties of the authenticator as documented in [E.Info.AUM-3.AUM]. This assessment is conducted on each path to security assets and/or financial assets required by AUM-1-1, AUM-1-2 or AUM-1-3.

6.2.3.4.4.2 Preconditions

None.

6.2.3.4.4.3 Assessment units

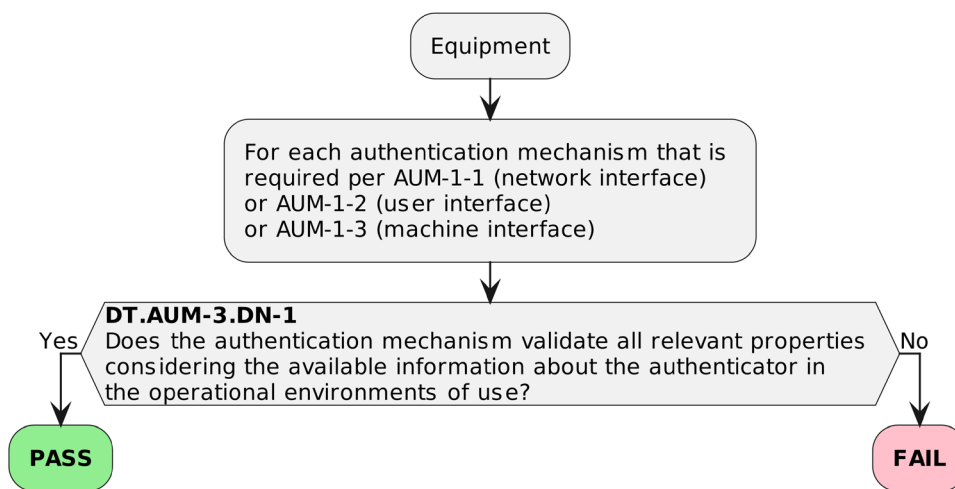


Figure 8 — Decision Tree for requirement AUM-3

For each authentication mechanism documented in [E.Info.AUM-3.AUM], check whether the path through the decision tree documented in [E.Info.DT.AUM-3] ends with “PASS”.

For each path through the decision tree documented in [E.Info.DT.AUM-3], examine its justification documented in [E.Just.DT.AUM-3].

6.2.3.4.4.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

- all paths through the decision tree documented in [E.Info.DT.AUM-3] end with “PASS”; and
- the information provided in [E.Just.DT.AUM-3] are correct justifications for all paths through the decision tree documented in [E.Info.DT.AUM-3].

The verdict FAIL for the assessment case is assigned if:

- a path through the decision tree documented in [E.Info.DT.AUM-3] ends with “FAIL”; or
- a justification provided in [E.Just.DT.AUM-3] is not correct or missing for a path through the decision tree documented in [E.Info.DT.AUM-3].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.2.3.4.5 Functional completeness assessment

The functional completeness assessment is covered by the functional sufficiency assessment of the authentication mechanism's applicability.

Therefore, this functional completeness assessment is not necessary.

6.2.3.4.6 Functional sufficiency assessment

6.2.3.4.6.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether the authentication mechanism required per AUM-1-1, AUM-1-2 or AUM-1-3 validates all required properties.

6.2.3.4.6.2 Preconditions

The equipment is in an operational state.

6.2.3.4.6.3 Assessment units

For each authentication mechanism documented in [E.Info.AUM-3.AUM]:

[AU.AUM-3.Password]: If the authenticator belongs to [IC.AUM-3.Password], functionally confirm the validation of the relevant properties of the authenticator documented in [E.Info.AUM-3.AUM.AuthVal] by examining whether:

- incorrect passwords can be used for successful authentication; and
- (if the confidentiality of the messages exchanged during authentication via network interfaces is not protected) a replay of a recorded successful authentication attempt can be used for successful authentication; and
- parts of the correct password can be used for authentication; and
- (if different user accounts exist or can be created) passwords of other entities can be used for authentication.

[AU.AUM-3.CertificatePrivateKey]: If the authenticator belongs to [IC.AUM-3.CertificatePrivateKey], functionally confirm the validation of the relevant properties of the authenticator documented in [E.Info.AUM-3.AUM.AuthVal] by examining whether:

- incorrect private keys to a trusted certificate can be used for successful authentication; and
- (if the confidentiality of the messages exchanged during authentication via network interfaces is not protected) a replay of a recorded successful authentication attempt can be used for successful authentication; and
- valid private keys to untrusted or invalid certificates can be used for successful authentication; and

NOTE untrusted or invalid certificates can be certificates revoked by the certificate authority, expired certificates, certificates with an invalid chain of trust e.g., generated by an untrusted entity containing an expected "Common Name" (CN) entry.

- (if different user accounts exist or can be created) private keys to a trusted certificate of other entities can be used for authentication.

[AU.AUM-3.Generic]: If the authenticator belongs to [IC.AUM-3.Generic], functionally confirm the validation of the relevant properties of the authenticator documented in [E.Info.AUM-3.AUM.AuthVal] by examining whether:

- incorrect authenticators can be used for successful authentication; and
- (if the confidentiality of the messages exchanged during authentication via network interfaces is not protected) a replay of a recorded successful authentication attempt can be used for successful authentication; and
- (if different user accounts exist or can be created) authenticators of other entities can be used for authentication.

6.2.3.4.6.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if for each authentication mechanism documented in [E.Info.AUM-3.AUM] the confirmations in the implementation category dependent assessment unit are successful.

The verdict FAIL for the assessment case is assigned if for an authentication mechanism documented in [E.Info.AUM-3.AUM] a confirmation in the implementation category dependent assessment unit is not successful.

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.2.4 [AUM-4] Changing authenticators

6.2.4.1 Requirement

Authentication mechanisms that are required per AUM-1-1, AUM-1-2 or AUM-1-3 shall allow for changing the authenticator except for authenticators where conflicting security goals do not allow for a change.

6.2.4.2 Rationale

Static authenticators can be a security risk for the equipment, e.g., increased vulnerability to brute force and eavesdropping attacks. Therefore, the support for changing authenticators on the equipment is needed as a countermeasure.

6.2.4.3 Guidance

An authorised entity needs the possibility to change the authenticator. The procedure can vary depending on the authentication mechanism used.

- The equipment provides a functionality to the authorised entity, e.g., user, to change the authenticator on the equipment.
- The authenticator, e.g., token, is renewed or changed by the manufacturer and the equipment accepts the changed authenticator because the trust chain is still valid.
- The authenticator is updated using a secure update mechanism.

In case of machine interfaces new pairing can be necessary. The integration of the change of the authenticator in the normal workflow simplifies the procedure for the user. This procedure depends on the selected authenticator (e.g., fingerprint, password or token)