



BSI Standards Publication

Common security requirements for radio equipment

Part 2: radio equipment processing data, namely Internet connected radio equipment, childcare radio equipment, toys radio equipment and wearable radio equipment

National foreword

This British Standard is the UK implementation of EN 18031-2:2024.

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 28364 8

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
2: radio equipment processing data, namely Internet
connected radio equipment, childcare radio equipment,
toys radio equipment and wearable radio equipment**

Exigences de sécurité communes applicables aux équipements radioélectriques - Partie 2 : Équipements radioélectriques qui traitent des données, à savoir les équipements radioélectriques connectés à l'internet, les équipements radioélectriques destinés à la garde d'enfants, les jouets dotés d'équipements radioélectriques et les équipements radioélectriques portables

Gemeinsame Sicherheitsanforderungen für datenverarbeitende Funkanlagen, namentlich mit dem Internet verbundene Funkanlagen, in der Kinderbetreuung eingesetzte Funkanlagen, in Spielzeug eingesetzte Funkanlagen sowie an einem Teil des menschlichen Körpers oder an Kleidungsstücken getragene Funkanlagen

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.



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
6.1.3 [ACM-3] Default access control for children in toys.....	26
6.1.4 [ACM-4] Default access control to children's privacy assets for toys and childcare equipment	30
6.1.5 [ACM-5] Parental/Guardian access controls for children in toys	36
6.1.6 [ACM-6] Parental/Guardian access controls for other entities' access to managed children's privacy assets in toys.....	40
6.2 [AUM] Authentication mechanism.....	45
6.2.1 [AUM-1] Applicability of authentication mechanisms	45
6.2.2 [AUM-2] Appropriate authentication mechanisms	55
6.2.3 [AUM-3] Authenticator validation	61
6.2.4 [AUM-4] Changing authenticators.....	65
6.2.5 [AUM-5] Password strength.....	68
6.2.6 [AUM-6] Brute force protection.....	76
6.3 [SUM] Secure update mechanism.....	80
6.3.1 [SUM-1] Applicability of update mechanisms.....	80
6.3.2 [SUM-2] Secure updates.....	83
6.3.3 [SUM-3] Automated updates.....	88
6.4 [SSM] Secure storage mechanism	91
6.4.1 [SSM-1] Applicability of secure storage mechanisms	91
6.4.2 [SSM-2] Appropriate integrity protection for secure storage mechanisms	96
6.4.3 [SSM-3] Appropriate confidentiality protection for secure storage mechanisms ...	101
6.5 [SCM] Secure communication mechanism.....	106
6.5.1 [SCM-1] Applicability of secure communication mechanisms	106
6.5.2 [SCM-2] Appropriate integrity and authenticity protection for secure communication mechanisms	112
6.5.3 [SCM-3] Appropriate confidentiality protection for secure communication mechanisms	118
6.5.4 [SCM-4] Appropriate replay protection for secure communication mechanisms ...	123
6.6 [LGM] Logging mechanism	128
6.6.1 [LGM-1] Applicability of logging mechanisms.....	128
6.6.2 [LGM-2] Persistent storage of log data.....	131
6.6.3 [LGM-3] Minimum number of persistently stored events.....	134
6.6.4 [LGM-4] Time-related information of persistently stored log data.....	137

6.7	[DLM] Deletion mechanism.....	140
6.7.1	[DLM-1] Applicability of deletion mechanisms	140
6.8	[UNM] User notification mechanism.....	144
6.8.1	[UNM-1] Applicability of user notification mechanisms	144
6.8.2	[UNM-2] Appropriate user notification content.....	148
6.9	[CCK] Confidential cryptographic keys.....	150
6.9.1	[CCK-1] Appropriate CCKs	150
6.9.2	[CCK-2] CCK generation mechanisms.....	154
6.9.3	[CCK-3] Preventing static default values for preinstalled CCKs	159
6.10	[GEC] General equipment capabilities	163
6.10.1	[GEC-1] Up-to-date software and hardware with no publicly known exploitable vulnerabilities.....	163
6.10.2	[GEC-2] Limit exposure of services via related network interfaces	168
6.10.3	[GEC-3] Configuration of optional services and the related exposed network interfaces.....	172
6.10.4	[GEC-4] Documentation of exposed network interfaces and exposed services via network interfaces.....	175
6.10.5	[GEC-5] No unnecessary external interfaces.....	178
6.10.6	[GEC-6] Input validation.....	181
6.10.7	[GEC-7] Documentation of external sensing capabilities.....	186
6.11	[CRY] Cryptography	188
6.11.1	[CRY-1] Best practice cryptography.....	188
	Annex A (informative) Rationale	194
A.1	General	194
A.2	Rationale.....	194
A.2.1	Family of standards	194
A.2.2	Security by design.....	194
A.2.3	Threat modelling and security risk assessment	195
A.2.4	Functional sufficiency assessment	196
A.2.5	Implementation categories.....	196
A.2.6	Assets	197
A.2.7	Mechanisms	199
A.2.8	Assessment criteria	199
A.2.9	Interfaces.....	202
	Annex B (informative) Mapping with EN IEC 62443-4-2: 2019.....	205
B.1	General	205
B.2	Mapping.....	205
	Annex C (informative) Mapping with ETSI EN 303 645 (Cyber Security for Consumer Internet of Things: Baseline Requirements)	208
C.1	General	208
C.2	Mapping.....	208
	Annex D (informative) Mapping with Security Evaluation Standard for IoT Platforms (SESIP)	214
D.1	General	214
D.2	Mapping.....	214

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 217

Bibliography 218

European foreword

This document (EN 18031-2:2024) 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 [36] 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 privacy 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 radio equipment [36] processing personal data [40] or traffic data [41] or location data [41] for either internet connected radio equipment [37], radio equipment designed or intended exclusively for childcare [37]; toys [39] and wearable radio equipment [37] (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/>

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 [29]]

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 personal information

personal information whose disclosure can compromise the user's or subscriber's privacy

3.11

confidential privacy function configuration

privacy function configuration whose disclosure can compromise the user's or subscriber's privacy

3.12

confidential security parameter

security parameter whose disclosure can compromise the user's or subscriber's privacy

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 [30]] 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

Note 1 to entry: Machine, network, and user interfaces are specific types of external interfaces.

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 can include security updates, installed after the equipment being placed on the market.

3.19 hard-coded

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

3.20 initialization

process that configures the network connectivity of the equipment for operation

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

3.21 interface

shared boundary across which *entities* exchange information

3.22 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 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.

3.23 log data

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

3.24

logging mechanism

equipment functionality to log internal activities

3.25

machine interface

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

3.26

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.

3.27

operational state

state in which the equipment is functioning normally according to the intended equipment functionality [38] and within its intended operational environment of use

3.28

optional service

service which is not necessary to setup the equipment, and which is not part of the basic functionality but is still relevant for the intended equipment functionality [38] and is 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.

3.29

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.

3.30

personal information

personal data [40], traffic data [41] or location data [41]

3.31

personal information of special categories

personal information that is genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation or that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership

[SOURCE: based on Article 9(1) of Regulation (EU) 2016/679 of the European parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [31]]

3.32

privacy asset

sensitive personal information or *confidential personal information* or *sensitive privacy function configuration* or *confidential privacy function configuration* or *privacy functions*

3.33**privacy function**

equipment's functionality that processes *personal information*

3.34**privacy function configuration**

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

3.35**public security parameter**

sensitive security parameter that is not confidential

3.36**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 [32]]

3.37**resource**

functional unit or data item needed to perform required operations

[SOURCE: IEC [33]]

3.38**risk**

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

[SOURCE: ISO/IEC Guide 51:2014 [34]]

3.39**security asset**

sensitive security parameter or confidential security parameter or security function

3.40**security function**

measure on the equipment that ensures that the personal data and the privacy of the user and of the subscriber are protected

3.41**security parameter**

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

3.42**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.

3.43**sensitive personal information**

personal information whose manipulation can compromise the user's or subscriber's privacy

3.44

sensitive privacy function configuration

privacy function configuration whose manipulation can compromise the user's or subscriber's privacy

3.45

sensitive security parameter

security parameter whose manipulation can compromise the user's or subscriber's privacy

3.46

security update

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

3.47

software

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

Note 1 to entry: Software also includes firmware.

3.48

storage mechanism

equipment functionality that allows to store information

3.49

update mechanism

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

3.50

user interface

external interface between the equipment and a user

3.51

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") [35]]

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
DHCP	dynamic host configuration protocol
DLM	deletion mechanism
DN	decision node
DoS	denial of service
DT	decision tree
E	evidence

E.Info	evidence.information
E.Just	evidence.justification
GEC	general equipment capabilities
IC	implementation category
ICMP	Internet control message protocol
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
UNM	user notification 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	

Clause #	Title		Description on how to apply the document
6.x.1.4.4		Conceptual assessment	
6.x.1.4.5		Functional completeness assessment	
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 privacy assets, except for access to security assets or privacy 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 assets and privacy 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 privacy assets that are in principle covered, but where the intended equipment functionality 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.

In general, full public accessibility to privacy assets cannot be considered as a reasonable intended equipment functionality, especially concerning children's privacy and childcare. However, specific scenarios involving public accessibility to privacy assets may be considered as intended equipment functionality if part of clearly advertised functionality or is communicated (to non-child users) via UNM.

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 privacy 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 security assets or privacy assets (for example, the WPS button on a home router);
- the equipment's functionality only provides information (on security assets or privacy assets) that is intended to be publicly accessible (for instance broadcasting short-range wireless technology 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.PrivacyAsset]: Description of each privacy asset that is accessible by entities, including:

- [E.Info.ACM-1.PrivacyAsset.Access]: possible entities' accesses to the privacy asset on the equipment; and
- (if access control by the equipment is absent for public accessibility of the privacy asset is the equipment's intended functionality) [E.Info.ACM-1.PrivacyAsset.PublicAccess]: Description of the equipment's intended functionality concerning the public accessibility of the privacy 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.PrivacyAsset.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.PrivacyAsset.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 privacy asset) [E.Info.ACM-1.PrivacyAsset.ACM]: Description of each access control mechanism that manages entities' access to the privacy asset.

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

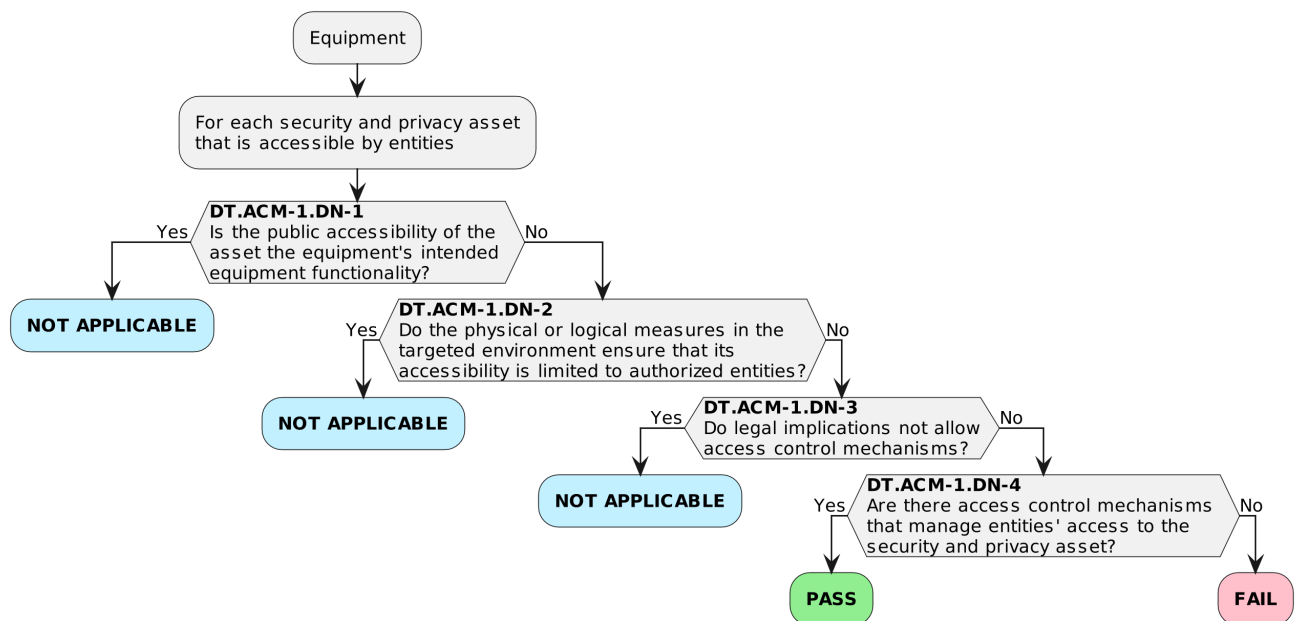


Figure 1 — Decision Tree for requirement ACM-1

For each security asset documented in [E.Info.ACM-1.SecurityAsset] and each privacy asset documented in [E.Info.ACM-1.PrivacyAsset], 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:

- all 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 the functional assessment is to verify that all the security assets and privacy assets that are accessible by entities, are documented in [E.Info.ACM-1.PrivacyAsset] 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.PrivacyAsset], 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 that are found are documented in [E.Info.ACM-1.SecurityAsset] and all privacy assets found are documented in [E.Info.ACM-1.PrivacyAsset].

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

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.PrivacyAsset] functionally confirm the existence of access control mechanisms according to [E.Info.ACM-1.SecurityAsset.ACM] and [E.Info.ACM-1.PrivacyAsset.ACM] by accessing the assets following [E.Info.ACM-1.PrivacyAsset.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.PrivacyAsset.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.PrivacyAsset.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 privacy assets.

6.1.2.2 Rationale

Security assets and privacy assets might 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 and privacy 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 privacy asset, such as changing security configuration; or
- a member of specific authorized groups can after authentication access a security asset or privacy asset; or
- an entity, authorized by another entity authorized to do so, can access a specific security asset or privacy asset.

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

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

For determining children's access rights to privacy assets or, other entities' access rights to children's privacy assets, the needs and capabilities of children are important aspects to be taken into account.

Moreover, in the case of the usage of potentially privacy compromising access rights, the equipment might depend on its capabilities and the intended equipment functionality, provide functionality to make the user aware of the execution of such access rights (for instance a symbol is displayed on a screen when the equipment's voice recording or geolocation functionality is used by an application).

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.PrivacyAsset]: Description of each privacy asset for which ACM-1 requires access control mechanisms, including:

- [E.Info.ACM-2.PrivacyAsset.ACM]: Description of the access control mechanisms required per ACM-1 that manages entities' access to the privacy asset and of how the mechanisms ensure that only authorized entities have access to the privacy 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 privacy asset documented in [E.Info.ACM-2.PrivacyAsset].

[E.Just.DT.ACM-2]: Justification for the 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.PrivacyAsset.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 privacy 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

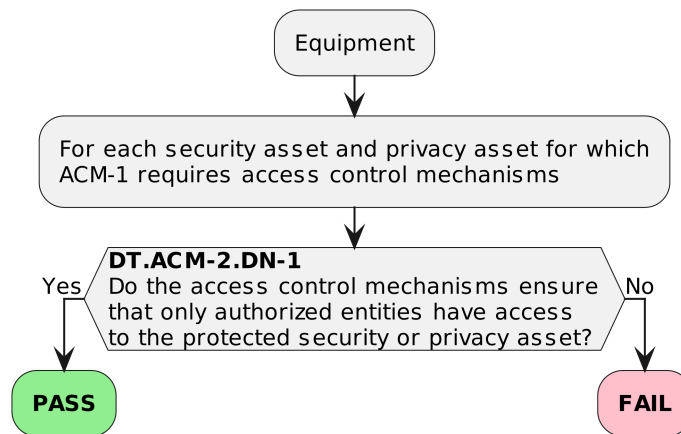


Figure 2 — Decision Tree for requirement ACM-2

For each security asset documented in [E.Info.ACM-2.SecurityAsset] and each privacy asset documented in [E.Info.ACM-2.PrivacyAsset], 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 privacy asset documented in [E.Info.ACM-2.PrivacyAsset]:

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

- the security asset or privacy 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.PrivacyAsset.ACM] belong to [IC.ACM-2.Generic], functionally confirm that:

- the security asset or privacy 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 privacy asset documented in [E.Info.ACM-2.PrivacyAsset] 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 privacy asset documented in [E.Info.ACM-2.PrivacyAsset] a confirmation in the implementation category dependent assessment unit is not successful.

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

6.1.3 [ACM-3] Default access control for children in toys

6.1.3.1 Requirement

If the equipment is a toy, for each privacy function where children can access external content and children's access is managed by access control mechanisms required per ACM-1, the access control mechanisms shall by default ensure that children's access to external content via the privacy function is restricted to content from authorized entities.

6.1.3.2 Rationale

Content from external sources that is accessed by children can be used for unauthorized communication, interaction or otherwise compromise the children's privacy. Restricting children's access by default to authorized entities only, supports avoiding related hazards.

6.1.3.3 Guidance

Privacy functions that allow children to access content can amongst others be:

- chat functions,
- voice or video call functions,
- functions that display content from external sources.

In order to ensure that children's default access to content from external sources is restricted to content from authorized entities, it is amongst others possible:

- to deny all children's access to external sources; or
- to deny all children's access to external sources, unless it is explicitly on a allow-list which is created after ensuring that it contains only access to content from authorized entities.

6.1.3.4 Assessment criteria

6.1.3.4.1 Assessment objective

The assessment addresses the requirement ACM-3.

6.1.3.4.2 Implementation categories

[IC.ACM-3.RBAC]: The methods to validate whether by default the access control mechanisms documented in [E.Info.ACM-3.ACM] solely rely on role-based access control and ensure that children's access to external content via the privacy function, is restricted to content from authorized entities.

[IC.ACM-3.DAC]: The methods to validate whether by default the access control mechanisms documented in [E.Info.ACM-3.ACM] solely rely on discretionary access control and ensure that children's access to external content via the privacy function, is restricted to content from authorized entities.

[IC.ACM-3.MAC]: The methods to validate whether by default the access control mechanisms documented in [E.Info.ACM-3.ACM] solely rely on mandatory access control and ensure that children's access to external content via the privacy function, is restricted to content from authorized entities.

[IC.ACM-3.Generic]: The methods to validate whether by default the access control mechanisms documented in [E.Info.ACM-3.ACM] do not solely rely on any of the methods described in ACM-3-RBAC, ACM-3-DAC or ACM-3-MAC and ensure that children's access to external content via the privacy function, is restricted to content from authorized entities.

6.1.3.4.3 Required information

[E.Info.ACM-3.PrivacyAsset]: Description of each privacy function where children can access external content, including:

- [E.Info.ACM-3.PrivacyAsset.TrustedSources]: List of authorized entities providing external content suitable for children.

[E.Info.ACM-3.ACM]: Description of each access control mechanism that is required per ACM-1 and that manages children's access for each privacy function documented in [E.Info.ACM-3.PrivacyAsset], including:

- Description on how the restriction of children's access to content from authorized entities only is implemented.

[E.Info.DT.ACM-3]: Description of the selected path through the decision tree in Figure 3 for each privacy function where children's access is managed by access control mechanisms documented in [E.Info.ACM-3.ACM].

[E.Just.DT.ACM-3]: Justification for each selected path through the decision tree for each privacy function where children's access is managed by access control mechanisms documented in [E.Info.DT.ACM-3] with the following property:

- the justification [DT.ACM-3.DN-2] is based on [E.Info.ACM-3.ACM] and [E.Info.ACM-3.PrivacyAsset.TrustedSources].

6.1.3.4.4 Conceptual assessment

6.1.3.4.4.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether the access control mechanisms for children's access on privacy functions are implemented as required per ACM-3.

6.1.3.4.4.2 Preconditions

None.

6.1.3.4.4.3 Assessment units

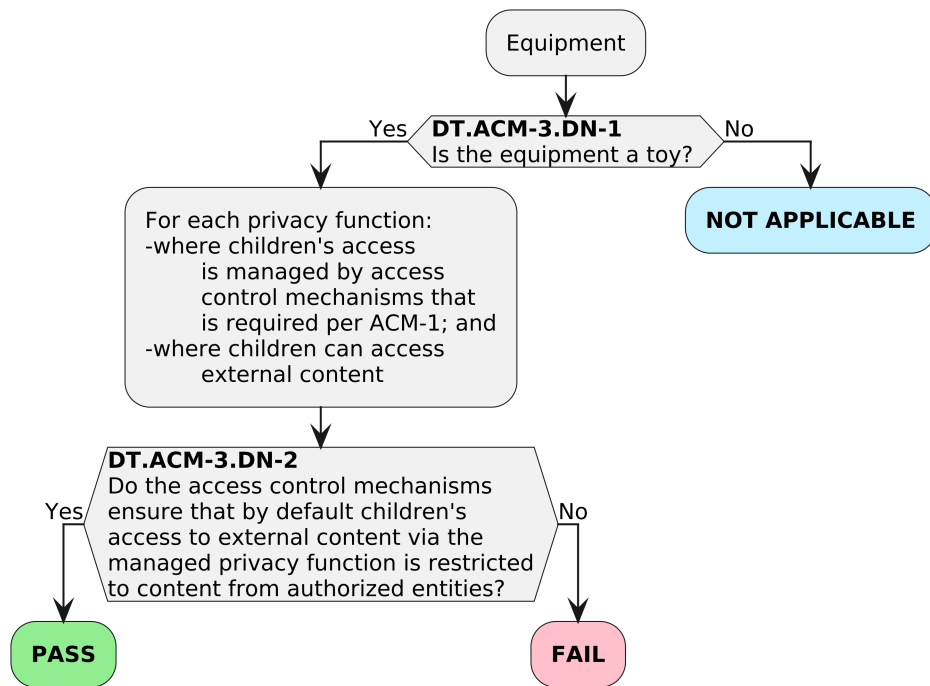


Figure 3 — Decision Tree for requirement ACM-3

For each privacy function where children can access external content as documented in [E.Info.ACM-3.PrivacyAsset] and where access is managed by access control mechanisms according to [E.Info.ACM-3.ACM], check whether the path through the decision tree documented in [E.Info.DT.ACM-3] ends with “PASS”.

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

6.1.3.4.4.4 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-3] ends with “PASS”; and
- no path through the decision tree documented in [E.Info.DT.ACM-3] ends with “FAIL”; and
- the information provided in [E.Just.DT.ACM-3] are correct justifications for all paths through the decision tree documented in [E.Info.DT.ACM-3].

The verdict FAIL for the assessment case is assigned if:

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

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

6.1.3.4.5 Functional completeness assessment

6.1.3.4.5.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether the documentation of privacy functions where children can access external content is complete.

6.1.3.4.5.2 Preconditions

The equipment is in an operational state.

6.1.3.4.5.3 Assessment units

Functionally assess whether there are privacy functions that allow children to access external content, which are not listed in [E.Info.ACM-3.PrivacyAsset] by performing the following steps:

- 1) List all equipment's privacy functions where children can access external content, e.g., by inspecting all parts of the software such as checking the internet browser settings, examining the app store access, inspect installed apps, investigate built-in or installed parental controls.
- 2) Compare the list from step 1 of functionally identified privacy functions with the list of privacy functions given by [E.Info.ACM-3.PrivacyAsset] and highlight any mismatch.

6.1.3.4.5.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if all discovered privacy functions, where children can access external content, are documented in [E.Info.ACM-3.PrivacyAsset].

The verdict FAIL for the assessment case is assigned if one discovered privacy function, where children can access external content, is not documented in [E.Info.ACM-3.PrivacyAsset].

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

6.1.3.4.6 Functional sufficiency assessment

6.1.3.4.6.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether by default the access control mechanisms ensure that children's access to external content via the privacy function, is restricted to content from authorized entities.

6.1.3.4.6.2 Preconditions

The equipment is in an operational state.

6.1.3.4.6.3 Assessment units

[AU.ACM-3.RBAC]: If the access control mechanisms documented in [E.Info.ACM-3.ACM] belong to [IC.ACM-3.RBAC]), functionally confirm that:

- children are assigned to associated roles that only allow to access content from authorized entities via the privacy function that allows access to external content; and
- least privileges are associated with the children's role; and
- changes in roles can only be performed by authorized users.

[AU.ACM-3.DAC]: If the access control mechanisms documented in [E.Info.ACM-3.ACM] belong to [IC.ACM-3.DAC]), functionally confirm that:

- children are assigned to associated identities that only allow to access content from authorized entities via the privacy function that allows access to external content; and
- least privileges are associated with the children's identity; and
- changes in identities can only be performed by authorized users.

[AU.ACM-3.MAC]: If the access control mechanisms documented in [E.Info.ACM-3.ACM] belong to [IC.ACM-3.MAC]), functionally confirm that:

- children are only issued with clearance by the operating system and/or system administrator when trying to access content from authorized entities via the privacy function that allows access to external content; 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-3.Generic]: If the access control mechanisms documented in [E.Info.ACM-3.ACM] belong to [IC.ACM-3.Generic]), functionally confirm that:

- children can only access content from authorized entities via the privacy function that allows access to external content; and
- the principle of least privileges for children is followed; and
- changing settings related to the access control mechanism or changes of privileges of children are only allowed to be performed by authorized users.

6.1.3.4.6.4 Assignment of verdict

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

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

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

6.1.4 [ACM-4] Default access control to children's privacy assets for toys and childcare equipment

6.1.4.1 Requirement

If the equipment is a toy or childcare equipment, any children's privacy function and personal information access control mechanisms required per ACM-1 shall by default restrict, apart from the child's or their parental/guardians, any third-party access to the children's privacy function and personal information processed by the equipment, except for authorised accesses which are required for the equipment's intended functionality.

6.1.4.2 Rationale

Exposing privacy functions or personal information to third parties by default can compromise children's privacy, even when consent is given. Restricting third parties' default access rights to children's privacy function and personal information to that are necessary for the operation of the equipment, supports privacy protection.

6.1.4.3 Guidance

If privacy assets are protected by several access control mechanisms, the default configuration of all these access control mechanisms can contribute to the privacy assets' default accessibility.

It might be necessary for external entities such as cloud services in control of the equipment's manufacturer to access children's personal information, for the equipment's intended functionality. An example is a child watch where parents can track the location history of the watch which is recorded on a cloud service independent of the watches current network connectivity status.

With children being vulnerable to cyber-crime, designers of default settings are strongly advised to consider the best interests of children.

6.1.4.4 Assessment criteria

6.1.4.4.1 Assessment objective

The assessment addresses the requirement ACM-4.

6.1.4.4.2 Implementation categories

[IC.ACM-4.RBAC]: The methods to validate whether by default the access control mechanisms documented in [E.Info.ACM-4.ACM] solely rely on role-based access control and ensure that other entities' third-parties' access to the children's privacy function and personal information processed by the equipment privacy assets is restricted to the necessary for the operation of the equipment.

[IC.ACM-4.DAC]: The methods to validate whether by default the access control mechanisms documented in [E.Info.ACM-4.ACM] solely rely on discretionary access control and ensure that other entities' third-parties' access to the children's privacy function and personal information processed by the equipment privacy assets is restricted to the necessary for the operation of the equipment.

[IC.ACM-4.MAC]: The methods to validate whether by default the access control mechanisms documented in [E.Info.ACM-4.ACM] solely rely on mandatory access control and ensure that other entities' third-parties' access to the children's privacy function and personal information processed by the equipment privacy assets is restricted to the necessary for the operation of the equipment.

[IC.ACM-4.Generic]: The methods to validate whether by default the access control mechanisms documented in [E.Info.ACM-4.ACM] do not solely rely on any of the methods described in ACM-4-RBAC, ACM-4-DAC or ACM-4-MAC and ensure that other entities' third-parties' access to the children's privacy function and personal information processed by the equipment privacy assets is restricted to the necessary for the operation of the equipment.

6.1.4.4.3 Required information

[E.Info.ACM-4.PrivacyAsset]: Description of each children's privacy function and personal information processed by the equipment which can be accessed by entities other than the children or their parents/guardians.

[E.Info.ACM-4.ACM]: Description of each access control mechanism that is required per ACM-1 and that manages third-parties other than the children or their parents'/guardians' access, for each children's privacy function and personal information processed by the equipment, including:

- description on how third-party accesses are managed in the default configuration; and
- description on how restrictions on third-party accesses are implemented; and

(if authorised accesses which are required for the equipment's intended functionality) [E.Info.ACM-4.AuthorisedAccess]: List of all authorised third-parties, including:

- List of all assets documented in [E.Info.ACM-4.PrivacyAsset] that can be accessed by the third party for each authorised third-party; and
- description on how the equipment's intended functionality depends on the authorised access of affected assets documented in [E.Info.ACM-4.PrivacyAsset] for each authorised third-party.

[E.Info.DT.ACM-4]: Description of the selected path through the decision tree in Figure 4 for each of the children's privacy function and personal information processed by the equipment documented in [E.Info.ACM-4.PrivacyAsset], where access for third-parties other than the children or their parents or guardians, is managed by access control mechanisms documented in [E.Info.ACM-4.ACM].

[E.Just.DT.ACM-4]: Justification for each selected path through the decision tree documented in [E.Info.DT.ACM-4] with the following properties:

- (if a decision from [DT.ACM-4.DN-2] results in "NOT APPLICABLE") the justification for the decision [DT.ACM-4.DN-2] is based on [E.Info.ACM-4.AuthorisedAccess]; and
- the justification for the decision [DT.ACM-4.DN-3] is based on [E.Info.ACM-4.ACM].

6.1.4.4.4 Conceptual assessment

6.1.4.4.4.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether the access control mechanisms are implemented as required per ACM-4.

6.1.4.4.4.2 Preconditions

None.

6.1.4.4.3 Assessment units

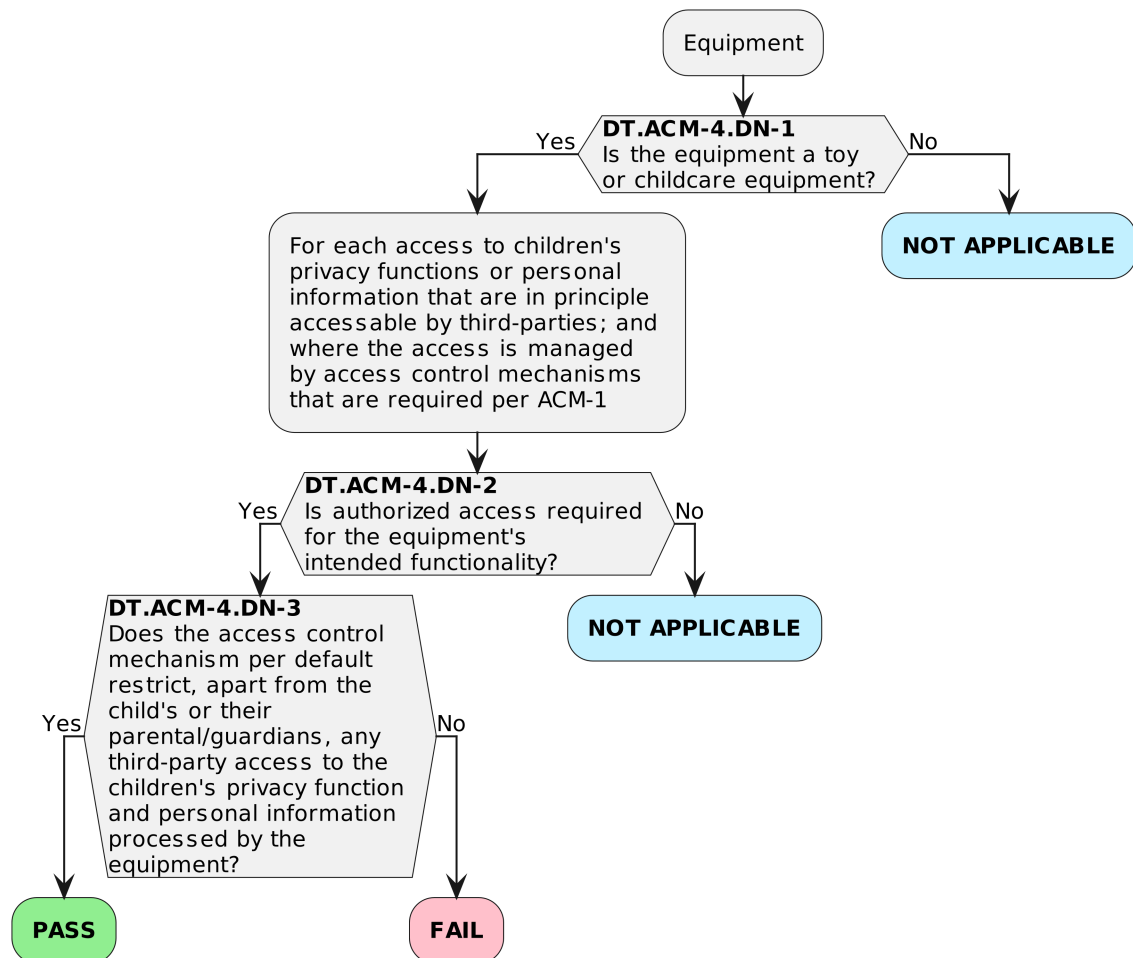


Figure 4 — Decision Tree for requirement ACM-4

For children’s privacy function and personal information processed by the equipment which can be accessed by third-parties, other than the children or their parents/guardians documented in [E.Info.ACM-4.PrivacyAsset] and where access is managed by access control mechanisms according to [E.Info.ACM-4.ACM], check whether the path through the decision tree documented in [E.Info.DT.ACM-4] ends with “NOT APPLICABLE” or “PASS”.

For each path through the decision tree documented in [E.Info.DT.ACM-4], examine its justification documented in [E.Just.DT.ACM-4].

6.1.4.4.4 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-4] ends with “PASS”; and
- no path through the decision tree documented in [E.Info.DT.ACM-4] ends with “FAIL”; and
- the information provided in [E.Just.DT.ACM-4] are correct justifications for all paths through the decision tree documented in [E.Info.DT.ACM-4].

The verdict FAIL for the assessment case is assigned if:

- a path through the decision tree documented in [E.Info.DT.ACM-4] ends with “FAIL”; or
- a justification provided in [E.Just.DT.ACM-4] is not correct or missing for a path through the decision tree documented in [E.Info.DT.ACM-4].

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

6.1.4.4.5 Functional completeness assessment

6.1.4.4.5.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether the documentation of children’s privacy function and personal information processed by the equipment which can be accessed by third-parties other than the children or their parents/guardians, is complete.

6.1.4.4.5.2 Preconditions

The equipment is in an operational state.

6.1.4.4.5.3 Assessment units

Functionally assess whether there are children’s privacy function and personal information on the equipment which can be accessed by third-parties other than the children or their parents/guardians, which are not listed in [E.Info.ACM-4.PrivacyAsset] by performing the following steps:

- 1) List all equipment’s children’s privacy functions and personal information on the equipment which can be accessed by third-parties other than the children or their parents/guardians, e.g. by inspecting all parts of the software such as checking the internet browser settings, examining the app store access, inspect installed apps, investigate built-in or installed parental controls.
- 2) Compare the list from step 1 with the list given by [E.Info.ACM-4.PrivacyAsset] and highlight any privacy function or personal information on the equipment that has been identified/found and that is not listed in [E.Info.ACM-4.PrivacyAsset].

6.1.4.4.5.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if all the children’s privacy function and personal information processed by the equipment which can be accessed by third-parties other than the children or their parents/ guardians, are documented in [E.Info.ACM-4.PrivacyAsset].

The verdict FAIL for the assessment case is assigned if a discovered children’s privacy function and personal information processed by the equipment which can be accessed by third-parties other than the children or their parents/ guardians, is not documented in [E.Info.ACM-4.PrivacyAsset].

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

6.1.4.4.6 Functional sufficiency assessment

6.1.4.4.6.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether by default the access control mechanisms ensure that other entities’ third-parties’ access to the children’s privacy function and personal information processed by the equipment privacy assets is restricted to the necessary for the operation of the equipment.

6.1.4.4.6.2 Assessment units

[AU.ACM-4.RBAC]: If the access control mechanisms documented in [E.Info.ACM-4.ACM] belong to [IC.ACM-4.RBAC]), functionally confirm that:

- other entities' third-parties' are assigned to associated roles that restrict access to the children's privacy function and personal information processed by the equipment's privacy assets to the necessary for the operation of the equipment; and
- least privileges are associated with the other entities' third-parties' role; and
- changes in roles can only be performed by authorized users.

[AU.ACM-4.DAC]: If the access control mechanisms documented in [E.Info.ACM-4.ACM] belong to [IC.ACM-4.DAC]), functionally confirm that:

- other entities' third-parties' are assigned to associated identities that restrict access to the children's privacy function and personal information processed by the equipment's privacy assets to the necessary for the operation of the equipment; and
- least privileges are associated with the other entities' third-parties' identity; and
- changes in identities can only be performed by authorized users.

[AU.ACM-4.MAC]: If the access control mechanisms documented in [E.Info.ACM-4.ACM] belong to [IC.ACM-4.MAC]), functionally confirm that:

- other entities' third-parties' that want to access to the children's privacy function and personal information processed by the equipment's privacy assets are only issued with clearance by the operating system and/or system administrator if necessary for the operation of the equipment; 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-4.Generic]: If the access control mechanisms documented in [E.Info.ACM-4.ACM] belong to [IC.ACM-4.Generic]), functionally confirm that:

- other entities' third-parties' can only access children's privacy function and personal information processed by the equipment's privacy assets if necessary for the operation of the equipment; and
- the principle of least privileges for other entities' third-parties is followed; and
- changing settings related to the access control mechanism or changes of privileges of other entities' third-parties' are only allowed to be performed by authorized users.

6.1.4.4.6.3 Assignment of verdict

The verdict PASS for the assessment case is assigned if for each access control mechanism documented in [E.Info.ACM-4.ACM] the confirmations in the implementation category dependent assessment unit are successful.

The verdict FAIL for the assessment case is assigned if for an access control mechanism documented in [E.Info.ACM-4.ACM] a confirmation in the implementation category dependent assessment unit is not successful.

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

6.1.5 [ACM-5] Parental/Guardian access controls for children in toys

6.1.5.1 Requirement

If the equipment is a toy, for each security and privacy asset that is accessible by children, any access control mechanism required per ACM-1 managing the children's access, shall be configurable by an authorized entity to restrict children's access to the protected security and privacy assets.

6.1.5.2 Rationale

Bearing in mind protection needs and evolving capacities of children, especially to judge the consequences of privacy and security configuration, it is necessary that parents or guardians can limit the possible access to security and privacy assets of their children, in order to avoid any hazard related to their privacy.

6.1.5.3 Guidance

The requirement demands that children's access to security and privacy assets can be restricted by an authorized entity typically represented by the children's parents or guardians.

For example, when the ability to pair a toy using a short-range wireless technology interface with a mobile phone can be controlled by a parent/guardian they can avoid that the children initiate a pairing with malicious intent. However, a parent/ guardians could give a child the permission to initiate a pairing with a mobile phone.

It is important that access control configuration by parents/guardians can be done easily.

6.1.5.4 Assessment criteria

6.1.5.4.1 Assessment objective

The assessment addresses the requirement ACM-5.

6.1.5.4.2 Implementation categories

[IC.ACM-5.RBAC]: The methods to validate whether by default the access control mechanisms documented in [E.Info.ACM-5.ACM] solely rely on role-based access control and are configurable by an authorized entity to restrict children's access to the security assets and privacy assets that are accessible by children.

[IC.ACM-5.DAC]: The methods to validate whether by default the access control mechanisms documented in [E.Info.ACM-5.ACM] solely rely on discretionary access control and are configurable by an authorized entity to restrict children's access to the security assets and privacy assets that are accessible by children.

[IC.ACM-5.MAC]: The methods to validate whether by default the access control mechanisms documented in [E.Info.ACM-5.ACM] solely rely on mandatory access control and are configurable by an authorized entity to restrict children's access to the security assets and privacy assets that are accessible by children.

[IC.ACM-5.Generic]: The methods to validate whether by default the access control mechanisms documented in [E.Info.ACM-5.ACM] do not solely rely on any of the methods described in ACM-5-RBAC, ACM-5-DAC or ACM-5-MAC and are configurable by an authorized entity to restrict children's access to the security assets and privacy assets that are accessible by children.

6.1.5.4.3 Required information

[E.Info.ACM-5.SecurityAsset]: Description of each security asset that is accessible by children.

[E.Info.ACM-5.PrivacyAsset]: Description of each privacy asset that is accessible by children.

[E.Info.ACM-5.ACM]: Description of each access control mechanism that is required per ACM-1 and that manages children's access for each security asset documented in [E.Info.ACM-5.SecurityAsset] and privacy asset documented in [E.Info.ACM-5.PrivacyAsset] processed by the equipment, including:

- Description on how an entity is authorized to restrict children's access to the protected security and privacy assets; and
- description on how these restrictions are implemented.

[E.Info.DT.ACM-5]: Description of the selected path through the decision tree in Figure 5 for each security asset and privacy asset where children's access is managed by access control mechanisms documented in [E.Info.ACM-5.ACM].

[E.Just.DT.ACM-5]: Justification for each selected path through the decision tree documented in [E.Info.DT.ACM-5] with the following property:

- the justification for the decision [DT.ACM-5.DN-2] is based on [E.Info.ACM-5.ACM].

6.1.5.4.4 Conceptual assessment

6.1.5.4.4.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether the access control mechanisms managing the children's access are configurable by an authorized entity to restrict children's access to the managed security assets and privacy assets.

6.1.5.4.4.2 Preconditions

None.

6.1.5.4.4.3 Assessment units

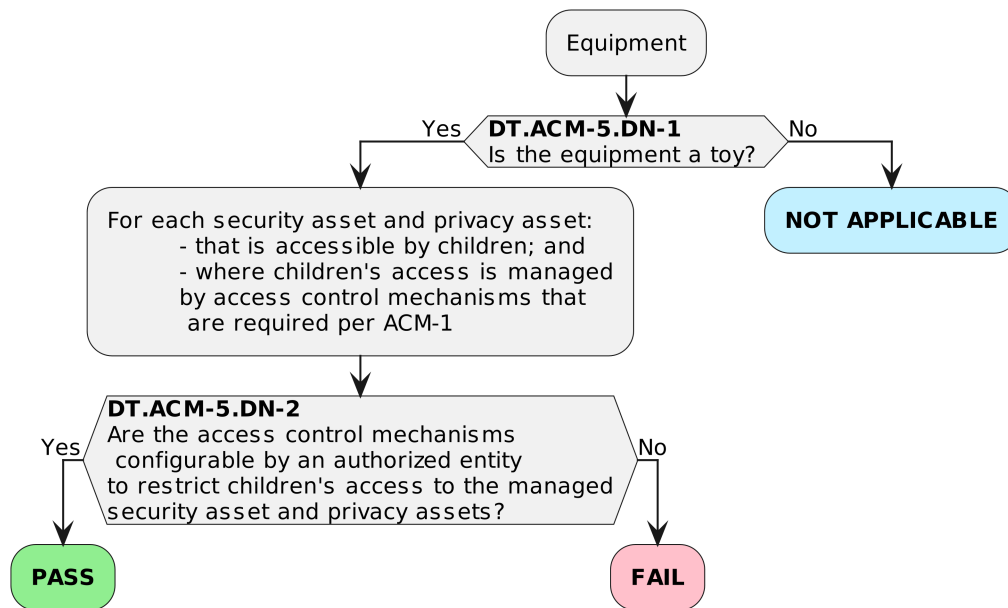


Figure 5 — Decision Tree for requirement ACM-5

For each security asset and privacy asset which can be accessed by children as documented in [E.Info.ACM-5.SecurityAsset] and [E.Info.ACM-5.PrivacyAsset] and where children's access is managed by access control mechanisms according to [E.Info.ACM-5.ACM] check whether the path through the decision tree documented in [E.Info.DT.ACM-5] ends with "NOT APPLICABLE" or "PASS".

For each path through the decision tree documented in [E.Info.DT.ACM-5], examine its justification documented in [E.Just.DT.ACM-5].

6.1.5.4.4.4 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-5] ends with "PASS"; and
- no path through the decision tree documented in [E.Info.DT.ACM-5] ends with "FAIL"; and
- the information provided in [E.Just.DT.ACM-5] are correct justifications for all paths through the decision tree documented in [E.Info.DT.ACM-5].

The verdict FAIL for the assessment case is assigned if:

- a path through the decision tree documented in [E.Info.DT.ACM-5] ends with "FAIL"; or
- a justification provided in [E.Just.DT.ACM-5] is not correct or missing for a path through the decision tree documented in [E.Info.DT.ACM-5].

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

6.1.5.4.5 Functional completeness assessment

6.1.5.4.5.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether the documentation of security asset and privacy assets that are accessible by children is complete.

6.1.5.4.5.2 Preconditions

The equipment is in an operational state.

6.1.5.4.5.3 Assessment units

Functionally assess whether there are security assets that are accessible by children, which are not documented in [E.Info.ACM-5.SecurityAsset] and whether there are privacy assets that are accessible by children, which are not documented in [E.Info.ACM-5.PrivacyAsset] by performing the following steps:

- 1) List all security assets and privacy assets that are accessible by children, e.g., by examining installed apps, check internet and browser settings, inspect app store access, analyse parental control settings, assess data sharing and storage.
- 2) Compare the list from step 1 with the list given by [E.Info.ACM-5.SecurityAsset] and [E.Info.ACM-5.PrivacyAsset] and highlight any security asset or privacy asset on the equipment that has been identified/found and that is neither listed in [E.Info.ACM-5.PrivacyAsset] nor in [E.Info.ACM-5.SecurityAsset].

6.1.5.4.5.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if all discovered security assets that are accessible by children, are documented in [E.Info.ACM-5.SecurityAsset] and all discovered privacy assets that are accessible by children, are documented in [E.Info.ACM-5.PrivacyAsset].

The verdict FAIL for the assessment case is assigned if discovered security assets that are accessible by children, are not documented in [E.Info.ACM-5.SecurityAsset] or if discovered privacy assets that are accessible by children, are not documented in [E.Info.ACM-5.PrivacyAsset].

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

6.1.5.4.6 Functional sufficiency assessment

6.1.5.4.6.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether security assets and privacy asset that are accessible by children and where children's access is managed by access control mechanisms are configurable by an authorized entity to restrict children's access.

6.1.5.4.6.2 Assessment units

[AU.ACM-5.RBAC]: If the access control mechanisms documented in [E.Info.ACM-5.ACM] belong to [IC.ACM-5.RBAC]), functionally confirm that:

- all users are assigned to associated roles; and
- least privileges are associated with users' roles so that only an authorized entity is able to configure the role-based access control mechanisms to restrict children's access to the managed security assets and privacy assets, as justified in [E.Just.DT.ACM-5]; and

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

[AU.ACM-5.DAC]: If the access control mechanisms documented in [E.Info.ACM-5.ACM] belong to [IC.ACM-5.DAC]), functionally confirm that:

- all users are assigned to associated identities; and
- least privileges are associated with users' identities so that only an authorized entity is able to configure the discretionary access control mechanisms to restrict children's access to the managed security assets and privacy assets, as justified in [E.Just.DT.ACM-5]; and
- changes in identities can only be performed by authorized users.

[AU.ACM-5.MAC]: If the access control mechanisms documented in [E.Info.ACM-5.ACM] belong to [IC.ACM-5.MAC]), functionally confirm that:

- All users are only issued with clearance by the operating system and/or system administrator to configure the mandatory access control to restrict children's access to the managed security assets and privacy assets, as justified in [E.Just.DT.ACM-5], if this user is an authorized user; 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-5.Generic]: If the access control mechanisms documented in [E.Info.ACM-4.ACM] belong to [IC.ACM-4.RBAC]), functionally confirm that:

- users are only allowed to configure access control mechanisms to restrict children's access to the managed security assets and privacy assets if this user is an authorized user; and
- the principle of least privileges for all 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.

6.1.5.4.6.3 Assignment of verdict

The verdict PASS for the assessment case is assigned if for each access control mechanism documented in [E.Info.ACM-5.ACM] the confirmations in the implementation category dependent assessment unit are successful.

The verdict FAIL for the assessment case is assigned if for an access control mechanism documented in [E.Info.ACM-5.ACM] a confirmation in the implementation category dependent assessment unit is not successful.

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

6.1.6 [ACM-6] Parental/Guardian access controls for other entities' access to managed children's privacy assets in toys

6.1.6.1 Requirement

If the equipment is a toy, for each children's privacy asset that is accessible by entities, other than the children or their parents or guardians, and where those other entities' access is managed by access

control mechanisms required per ACM-1, the access control mechanisms shall be configurable by an authorized entity to restrict the other entities' access to the managed children's privacy assets.

6.1.6.2 Rationale

Bearing in mind the protection needs and evolving capacities of children, it is necessary that parents or guardians can limit entities' access to children's privacy assets, in order to avoid any hazard related to their privacy.

6.1.6.3 Guidance

The requirement demands that entities' access to children's privacy assets can be restricted by an authorized entity, who is typically represented by the children's parents or guardians.

For example, parents/guardians can limit the access of third parties and other potentially malicious actors, who could remotely access the equipment functionality, for observation, remote communication or control and other related hazards for children.

It is important that access control configuration by guardians can be done easily.

6.1.6.4 Assessment criteria

6.1.6.4.1 Assessment objective

The assessment addresses the requirement ACM-6.

6.1.6.4.2 Implementation categories

[IC.ACM-6.RBAC]: The methods to validate whether by default the access control mechanisms documented in [E.Info.ACM-6.ACM] solely rely on role-based access control and whether this underlying access control, that manages access to children's privacy assets that are accessible by entities other than the children or their parents or guardians, is configurable by an authorized entity.

[IC.ACM-6.DAC]: The methods to validate whether by default the access control mechanisms documented in [E.Info.ACM-6.ACM] solely rely on discretionary access control and whether this underlying access control, that manages access to children's privacy assets that are accessible by entities other than the children or their parents or guardians, is configurable by an authorized entity.

[IC.ACM-6.MAC]: The methods to validate whether by default the access control mechanisms documented in [E.Info.ACM-6.ACM] solely rely on mandatory access control and whether this underlying access control, that manages access to children's privacy assets that are accessible by entities other than the children or their parents or guardians, is configurable by an authorized entity.

[IC.ACM-6.Generic]: The methods to validate whether by default the access control mechanisms documented in [E.Info.ACM-6.ACM] do not solely rely on any of the methods described in ACM-6-RBAC, ACM-6-DAC or ACM-6-MAC and whether this underlying access control, that manages access to children's privacy assets that are accessible by entities other than the children or their parents or guardians, is configurable by an authorized entity.

6.1.6.4.3 Required information

[E.Info.ACM-6.PrivacyAsset]: Description of each children's privacy asset that is accessible by entities, other than the children or their parents or guardians.

[E.Info.ACM-6.ACM]: Description of each access control mechanism that is required per ACM-1 and that manages entities, other than the children or their parents or guardians, access to children's privacy assets documented in [E.Info.ACM-6.PrivacyAsset], including:

- Description on how entities are authorised to configure the access control mechanism to restrict other entities access to the managed children's privacy assets; and
- description on how the restrictions to access the managed children's privacy assets are implemented.

[E.Info.DT.ACM-6]: Description of the selected path through the decision tree in Figure 6 for each children's privacy asset that is accessible by entities, other than the children or their parents or guardians documented in [E.Info.ACM-6.PrivacyAsset] and where the other entities' access is managed by access control mechanisms documented in [E.Info.ACM-6.ACM].

[E.Just.DT.ACM-6]: Justification for each selected path through the decision tree documented in [E.Info.DT.ACM-6] with the following property:

- the justification for the decision [DT.ACM-6.DN-2] is based on [E.Info.ACM-6.ACM].

6.1.6.4.4 Conceptual assessment

6.1.6.4.4.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether the access control mechanisms are configurable by an authorized entity to restrict other entities' access to the managed children's privacy assets.

6.1.6.4.4.2 Preconditions

None.

6.1.6.4.4.3 Assessment units

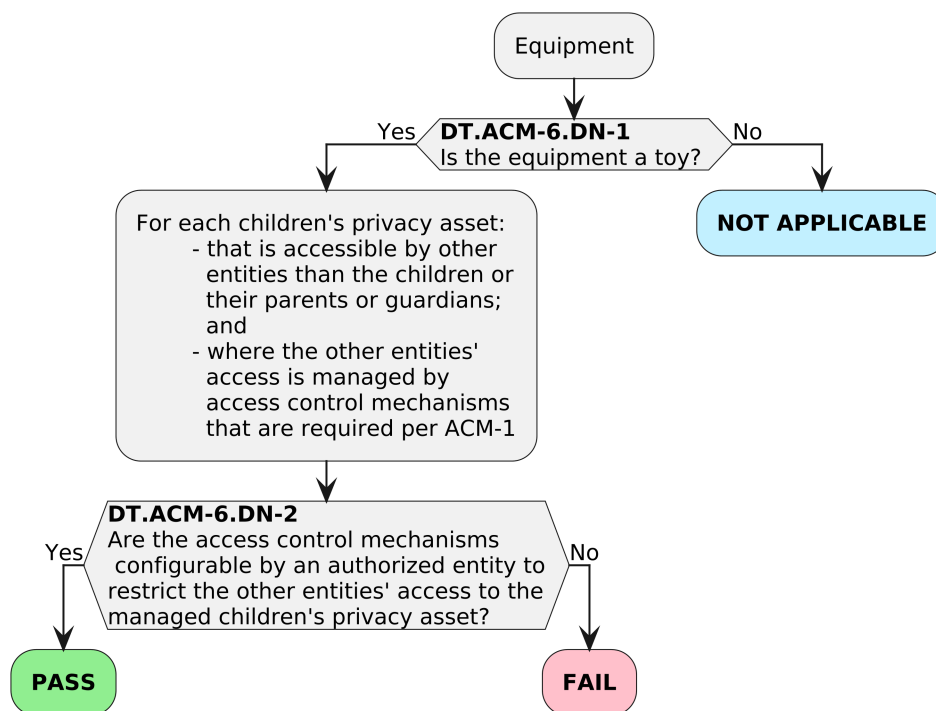


Figure 6 — Decision Tree for requirement ACM-6

For each children's privacy asset that is accessible by entities, other than the children or their parents or guardians, documented in [E.Info.ACM-6.PrivacyAsset] and where the other entities' access is managed by access control mechanisms according to [E.Info.ACM-6.ACM], check whether the path through the decision tree documented in [E.Info.DT.ACM-6] ends with "NOT APPLICABLE" or "PASS".

For each path through the decision tree documented in [E.Info.DT.ACM-6], examine its justification documented in [E.Just.DT.ACM-6].

6.1.6.4.4.4 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-6] ends with "PASS"; and
- no path through the decision tree documented in [E.Info.DT.ACM-6] ends with "FAIL"; and
- the information provided in [E.Just.DT.ACM-6] are correct justifications for all paths through the decision tree documented in [E.Info.DT.ACM-6].

The verdict FAIL for the assessment case is assigned if:

- a path through the decision tree documented in [E.Info.DT.ACM-6] ends with "FAIL"; or
- a justification provided in [E.Just.DT.ACM-6] is not correct or missing for a path through the decision tree documented in [E.Info.DT.ACM-6].

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

6.1.6.4.5 Functional completeness assessment

6.1.6.4.5.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether the documentation of children's privacy assets documented in [E.Info.ACM-6.PrivacyAsset] that are accessible by entities, other than the children or their parents or guardians, is complete.

6.1.6.4.5.2 Preconditions

The equipment is in an operational state.

6.1.6.4.5.3 Assessment units

Functionally assess whether there are children's privacy assets that are accessible by entities, other than the children or their parents or guardians, which are not documented in [E.Info.ACM-6.PrivacyAsset] by performing the following steps:

- 1) List all privacy assets that are accessible by entities, other than the children or their parents or guardians, e.g., by examining app permissions and their terms and privacy policies, review network and internet connections, inspect equipment settings, review web browser history and settings, check potential data access points such as photo libraries, location logs, communication and social media apps.
- 2) Compare the list from step 1 with the list given by [E.Info.ACM-6.PrivacyAsset] and highlight any privacy asset on the equipment that has been identified/found and that is not listed in [E.Info.ACM-6.PrivacyAsset].

6.1.6.4.5.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if all discovered children's privacy assets that are accessible by entities, other than the children or their parents or guardians, are documented in [E.Info.ACM-6.PrivacyAsset].

The verdict FAIL for the assessment case is assigned if a discovered children's privacy asset that is accessible by entities, other than the children or their parents or guardians, is not documented in [E.Info.ACM-6.PrivacyAsset].

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

6.1.6.4.6 Functional sufficiency assessment

6.1.6.4.6.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether children's privacy assets that are accessible by entities, other than the children or their parents or guardians, are managed by access control mechanisms that are configurable by an authorized entity to restrict other entities' access.

6.1.6.4.6.2 Assessment units

[AU.ACM-6.RBAC]: If the access control mechanisms documented in [E.Info.ACM-6.ACM] belong to [IC.ACM-6.RBAC]), functionally confirm that :

- all users are assigned to associated roles; and
- least privileges are associated with users' roles so that only an authorized entity is able to configure the role-based access control mechanisms to restrict the other entities' access to the managed children's privacy assets, as justified in [E.Just.DT.ACM-6]; and
- changes in roles can only be performed by authorized users.

[AU.ACM-6.DAC]: If the access control mechanisms documented in [E.Info.ACM-6.ACM] belong to [IC.ACM-6.DAC]), functionally confirm that:

- All users are assigned to associated identities; and
- least privileges are associated with users' identities so that only an authorized entity is able to configure the discretionary access control mechanisms to restrict access to the other entities' access to the managed children's privacy assets, as justified in [E.Just.DT.ACM-6]; and
- changes in identities can only be performed by authorized users.

[AU.ACM-6.MAC]: If the access control mechanisms documented in [E.Info.ACM-6.ACM] belong to [IC.ACM-6.MAC]), functionally confirm that:

- users are only issued with clearance by the operating system and/or system administrator to configure the mandatory access control to restrict other entities' access to the children's managed security and privacy assets, as justified in [E.Just.DT.ACM-6], if this user is an authorized user; 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-6.Generic]: If the access control mechanisms documented in [E.Info.ACM-6.ACM] belong to [IC.ACM-6.Generic]), functionally confirm that:

- users are only allowed to configure access control mechanisms to restrict other entities' access to the children's managed privacy assets if this user is an authorized user; and
- the principle of least privileges for all 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.

6.1.6.4.6.3 Assignment of verdict

The verdict PASS for the assessment case is assigned if for each access control mechanism documented in [E.Info.ACM-6.ACM] the confirmations in the implementation category dependent assessment unit are successful.

The verdict FAIL for the assessment case is assigned if for an access control mechanism documented in [E.Info.ACM-6.ACM] 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 personal information, confidential privacy function configuration or confidential security parameters; or
- modify sensitive personal information, sensitive privacy function configuration or sensitive security parameters; or
- use privacy functions or security functions,

except for access:

- to personal information, privacy functions or privacy function configuration where the absence of authentication is required for the intended equipment functionality; or
- via networks where physical or logical measures in the equipment's targeted operational environment limit accessibility to authorised entities.

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 personal information, confidential privacy function configuration or confidential security parameters; or

- modify sensitive personal information, sensitive privacy function configuration or sensitive security parameters; or
- use privacy functions or security functions,

except for access:

- where physical or logical measures in the equipment's targeted operational environment limit accessibility to authorized entities;

and except for read only access to personal information, privacy functions or privacy function configuration where access without authentication is needed:

- to enable the intended equipment functionality or
- because legal implications do not allow for authentication mechanisms.

6.2.1.3 Rationale

The equipment needs to provide an authentication mechanism such that the corresponding access control mechanism prevents unauthorized access to security and privacy assets that are relevant to user's privacy from entities which are not who or what they claim to be.

6.2.1.4 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 privacy 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.