Harmonised standards for cyber security certification under the radio equipment directive (RED)

Dr. Samim Ahmadi - member of CEN/CLC JTC 13 WG 8
umlaut communications GmbH (part of Accenture)

22.03.2023

public

Motivation

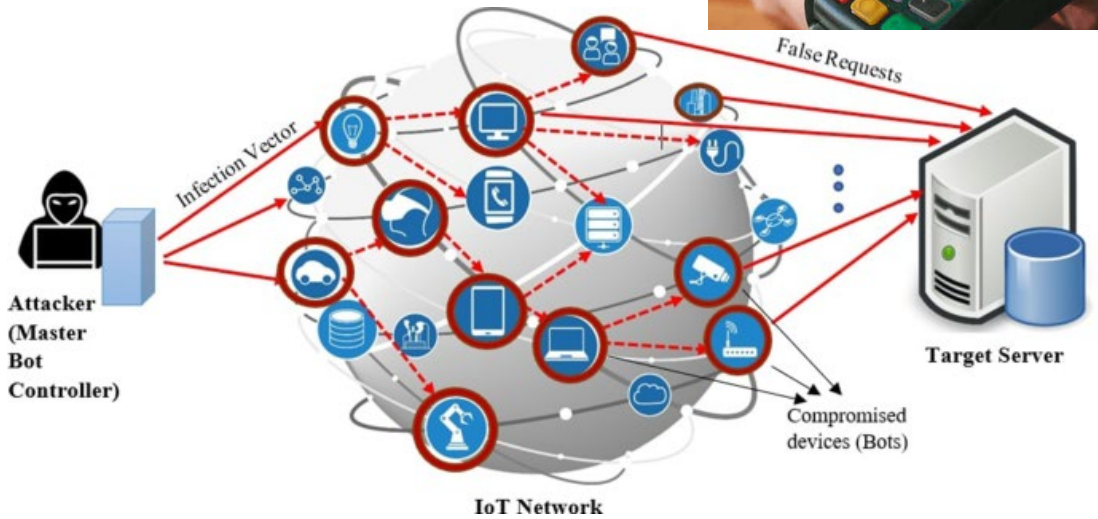
- lots of devices unsecured such as the smart toy „Cayla“

- such devices
  - communicate over radio waves
  - use sensitive personal data
  - are often not noticed of being hacked (by parents)

- similar IoT devices can also be used
  - as part of a botnet to launch DDoS attacks
  - to perform fraud with financial data

Market entry shall be forbidden
for such unsecure products

=> solution: Radio Equipment Directive



Agendachärt.

01 _____ Cybersecurity fundamentals in RED

02 _____ Conformity assessment under RED

03 _____ Standardisation Request under M585

04 _____ Creation of harmonised standards in CEN/CLC JTC 13 WG 8

Agendachärt.

01 _____ Cybersecurity fundamentals in RED

02 _____ Conformity assessment under RED

03 _____ Standardisation Request under M585

04 _____ Creation of harmonised standards in CEN/CLC JTC 13 WG 8

3. Radio equipment within certain categories or classes shall be so constructed that it complies with the following essential requirements:

(a) radio equipment interworks with accessories, in particular with common chargers;

(b) radio equipment interworks via networks with other radio equipment;

(c) radio equipment can be connected to interfaces of the appropriate type throughout the Union;

(d) radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service;

(e) radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected;

(f) radio equipment supports certain features ensuring protection from fraud;

(g) radio equipment supports certain features ensuring access to emergency services;

(h) radio equipment supports certain features in order to facilitate its use by users with a disability;

(i) radio equipment supports certain features in order to ensure that software can only be loaded into the radio equipment where the compliance of the combination of the radio equipment and software has been demonstrated.

The Commission shall be empowered to adopt delegated acts in accordance with Article 44 specifying which categories or classes of radio equipment are concerned by each of the requirements set out in points (a) to (i) of the first subparagraph of this paragraph.

RED Delegated Regulation (2022/30) activates RED requirements 3.3.d/e/f

3.3.d “radio equipment **does not harm the network** or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service”

3.3.e “radio equipment incorporates safeguards to ensure that the **personal data and privacy** of the user and of the subscriber are protected”

3.3.f “radio equipment supports certain features ensuring **protection from fraud**”

RED Delegated Regulation (2022/30) scope for RED requirements 3.3.d/e/f

L 7/6 EN Official Journal of the European Union 12.1.2022

COMMISSION DELEGATED REGULATION (EU) 2022/30

of 29 October 2021

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

(Text with EEA relevance)

RED Article 3.3(d) – to **ensure network protection** – applies to:

- radio equipment that can communicate itself over the internet, whether it communicates directly or via any other equipment ('internet-connected radio equipment')

RED Article 3.3(e) – to ensure safeguards for the **protection of personal data and privacy** – applies to the following equipment when capable of processing personal data or traffic data and location data:

a) internet-connected radio equipment other than referred to in points b), c) or d);

b) radio equipment designed or intended exclusively for **childcare**;

c) radio equipment falling under the **Toys** Directive (2009/48/EC);

d) radio equipment designed or intended, whether exclusively or not exclusively, to be worn on, strapped to, or hung from the body or clothing **worn by human beings**

RED Article 3.3(f) – to ensure **protection from fraud** – applies to:

- internet-connected radio equipment, if that equipment enables the holder or user to transfer **money, monetary value or virtual currency**.

RED Delegated Regulation (2022/30) exemptions for 3.3.d/e/f

The following radio equipment is fully exempted from RED Articles 3.3(d), 3.3(e) and 3.3(f):

- Medical devices under Regulation (EU) 2017/745 and (EU) 2017/746

The following radio equipment is exempted from RED Articles 3.3(e) and 3.3(f), but article 3.3(d) still applies:

- Radio equipment under Regulation (EU) 2018/1139 (civil aviation)
- Radio equipment under Regulation (EU) 2019/2144 (motor vehicles)
- Radio equipment under Directive (EU) 2019/520 (road toll systems)

Agendachärt.

01 _____ Cybersecurity fundamentals in RED

02 _____ Conformity assessment under RED

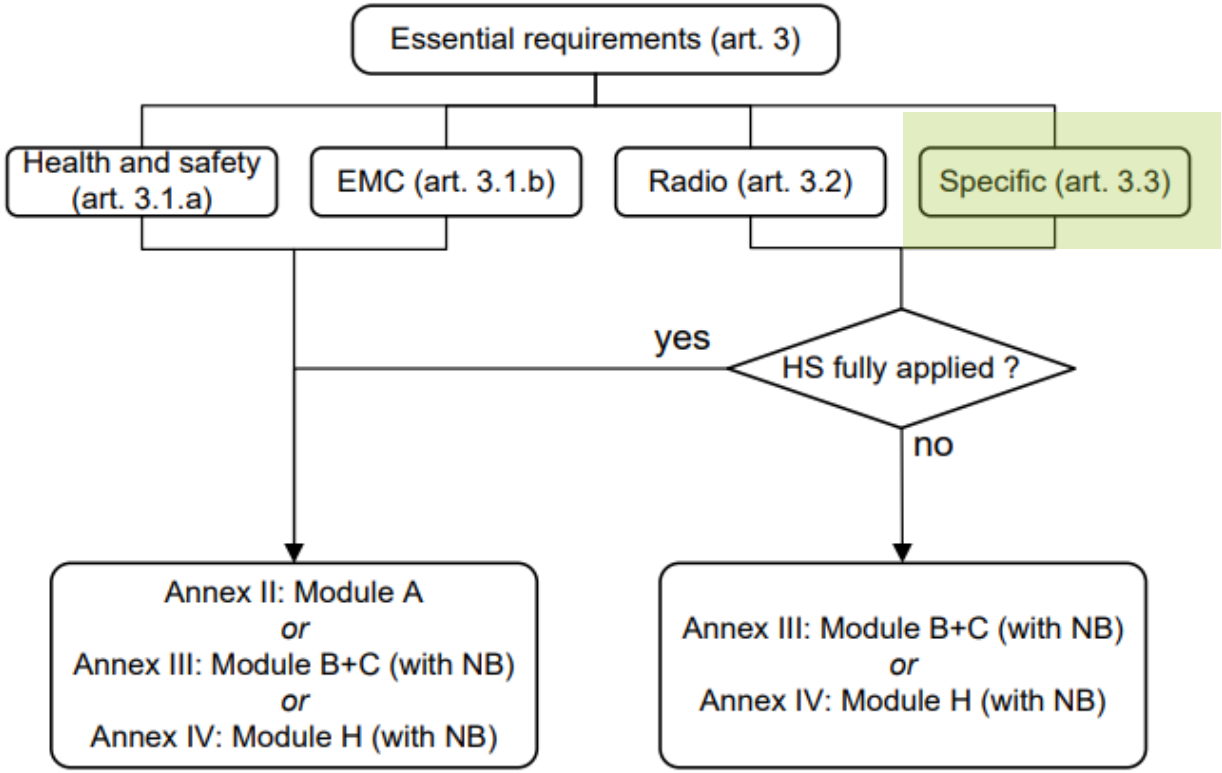
03 _____ Standardisation Request under M585

04 _____ Creation of harmonised standards in CEN/CLC JTC 13 WG 8

Conformity assessment under RED

- Module A: „Self Assessment“ requiring mainly
  - Technical Documentation containing details to compliance with Article 3
  - CE marking to be affixed
  - EU Declaration of Conformity

- Module B+C as well as Module H include notified body (NB)



=> If no Harmonised Standard (HS), NB is a must!

Agendachärt.

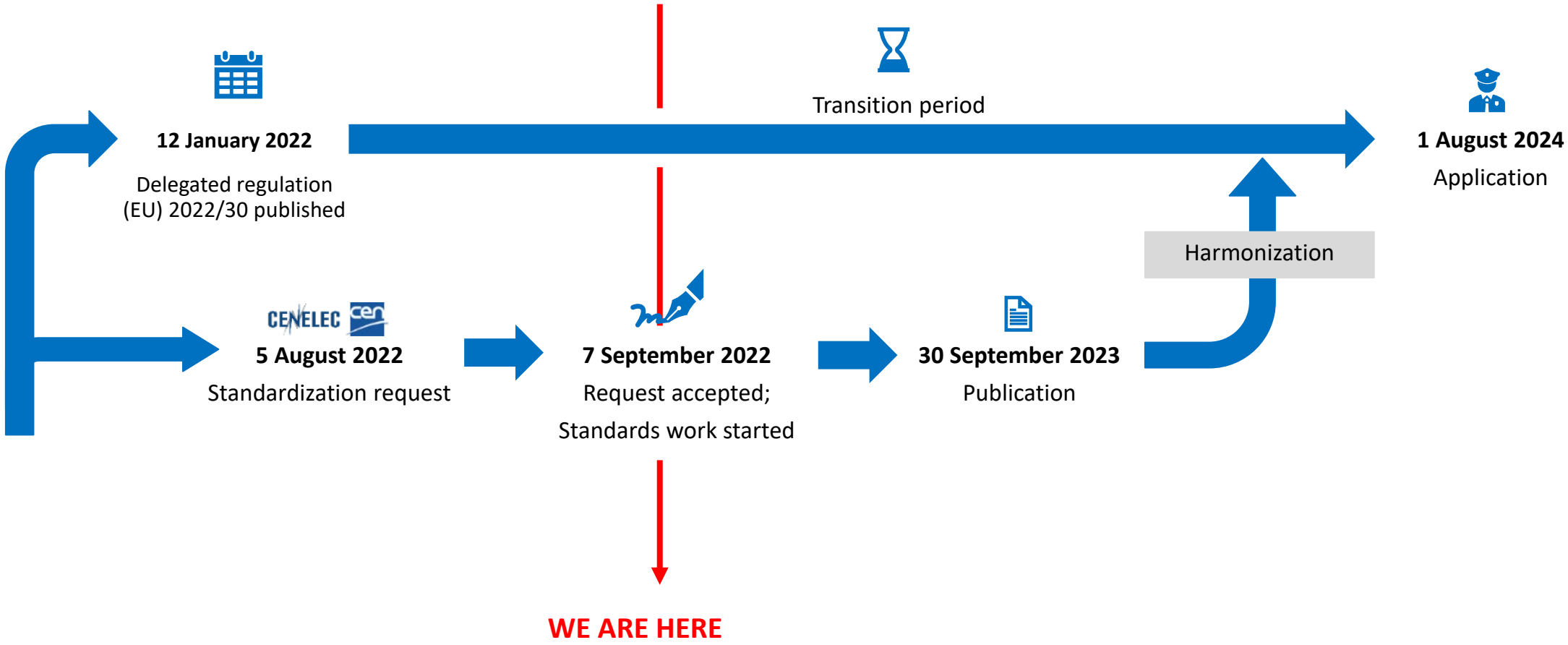
01 _____ Cybersecurity fundamentals in RED

02 _____ Conformity assessment under RED

03 _____ Standardisation Request under M585

04 _____ Creation of harmonised standards in CEN/CLC JTC 13 WG 8

The standardization request



The standardization request

Harmonised standards in support of the essential requirement set out in Article 3(3), point (d/e/f), of Directive 2014/53/EU for the categories and classes specified by Delegated Regulation (EU) 2022/30 shall contain technical specifications that ensure at least that those radio equipment, where applicable:

d 1. include elements to monitor and control network traffic, including the transmission of outgoing data;

d 2. is designed to mitigate the effects of ongoing denial of service attacks;

def 3. implement appropriate authentication and access control mechanisms;

def 4. are provided, on a risk basis, with up-to-date software and hardware at the moment of placing on the market that do not contain publicly known exploitable vulnerabilities as regards harm to the <d><e><f>;

def 5. are provided with automated and secure mechanisms for updating software or firmware that allow, when necessary, the mitigation of vulnerabilities that if exploited may lead to <d><e><f>;

6. protect the exposed attack surfaces and minimise the impact of successful attacks.

def 7. protect stored, transmitted or otherwise processed <e> <f> against accidental or unauthorised storage, ef processing, access, disclosure, unauthorised destruction, loss or alteration or lack of availability of <e> <f>;

8. include functionalities to inform the user of changes that may affect data protection and privacy;

e 9. log the internal activity that can have an impact on <e> <f>;

ef 10. allow users to easily delete their stored personal data, enabling the disposal or replacement of e equipment without the risk of exposing personal information;

<d> = network or its functioning or misuse of network resources, <e> = personal & location data protection and privacy, <f> = financial or monetary data

Agendachärt.

01 _____ Cybersecurity fundamentals in RED

02 _____ Conformity assessment under RED

03 _____ Standardisation Request under M585

04 _____ Creation of harmonised standards in CEN/CLC JTC 13 WG 8

CEN/CENELEC JTC 13/WG 8 “Special Working Group RED Standardization Request”

JTC 13/WG 8 was established on July 7, 2022, to address the RED Standardization Request.

JTC 13/WG 8 is on a very tough meeting schedule with many online and hybrid meetings.

WG 8 currently has 167 committee members representing:

- 18 National bodies
- CENELEC TC’s
- Liaisons:
  - ANEC
  - APPLIA
  - ESMIG
  - ETSI
  - EURALARM
  - EUROSMART

Convenor: Ben Kokx

Secretariat: NEN

RED Delegated Regulation hENs Updated Schedule			
Stage Code	**Stage**	**Target date**	**Duration**
10.99	Decision on WI Proposal	2022-10-14	
			+ 16 weeks
20.60	Circulation of 1st WD	2023-02-03	
			+ 27 weeks
30.99	Acceptance of ENQ draft	2023-08-11	
			+ 3 weeks
40.20	Submission to Enquiry	2023-09-01	
			+ 12 weeks
40.60	Closure of Enquiry	2023-11-24	
			+ 12 weeks
45.99	Acceptance of FV draft	2024-02-16	
			+ 3 weeks
50.20	Submission to Formal Vote	2024-03-08	
			+ 8 weeks
50.60	Closure of Formal Vote	2024-05-03	
			+ 4 weeks
60.55	DOR/Ratification	2024-05-31	
			+ 4 weeks
60.60	DAV/Definitive text available	2024-06-28	

CEN/CLC request for amendment of M/585

- CEN and CENELEC requested on December 13th for an amendment of the standardization request as the initial requested timelines, giving 13 months, are unachievable.
- In the best-case scenario the 31st of December 2023 is possible but is not likely to include 5G Networking equipment.
- If 5G Networking equipment should be included: postpone the deadline for the publication by the ESO's by 9 months to June 30, 2024.

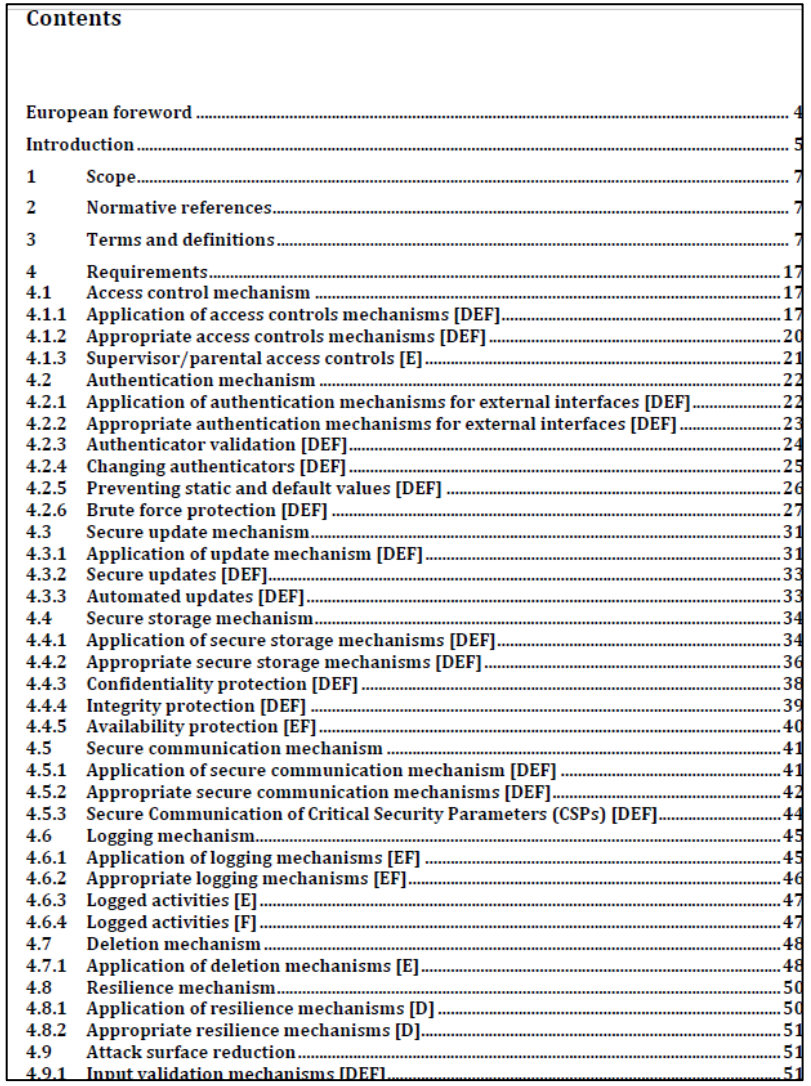
In order to provide the European market adequate time to ensure their products comply with the Harmonized standards, **CEN and CENELEC invite the European Commission to consider a postponement of the date of applicability of the Delegated Regulation**, in alignment with the SR

Current hEN draft in CEN/CLC JTC 13 WG 8

The current working draft has **17 main requirement** sections, each having one of more requirements. Each of these requirement has the requirement statement, rationale, guidance and will have assessment criteria (not available in the working draft).

Current requirement sections:

-Access control mechanism
-Authentication mechanism
-Secure update mechanism
-Secure storage mechanism
-Secure communication mechanism
-Logging mechanism
-Deletion mechanism
-Resilience mechanism
-Attack surface reduction
-Network monitoring mechanism
-Traffic control mechanism
-User notification mechanism
-CSP generation mechanism
-General equipment capabilities
-Cryptography
-Smart meters
-5G Network equipment



Contents

Current status within the work of CEN/CLC JTC 13 WG 8

- Received around 750 comments on the Working Draft without completion of assessment criteria
- EC wants us to revise the formulation of our requirements otherwise full presumption of conformity cannot be ensured
  - Requirements shall be more precise, avoid using words like „intended use“ and „intended operational environment of use“
  - Assessments are to be as reproducible as possible and requirements are to be objectively verifiable
- EC understands that security is a much more dynamic target than a physically measurable quantity
  => requirements shall be formulated as objectively as possible
- WG 8 appreciates EC‘s understanding and is optimistic to move forward with an adapted time schedule

Thank you for your attention!

Sources

Images (all accessed on 15.3.2023):

- https://www.theinternetpatrol.com/wp-content/uploads/my-friend-cayla-hackers.jpg
- https://media.springernature.com/lw685/springer-static/image/art%3A10.1007%2Fs11235-019-00599-z/MediaObjects/11235_2019_599_Fig2_HTML.png
- https://www.handelsblatt.com/vergleich/wp-content/uploads/2020/10/Kartenzahlung-Anbieter-2.jpeg

Other sources:

- Radio Equipment Directive 2014/53/EU
- Guide to the Radio Equipment Directive 2014/53/EU (”RED Guide”, 2018)
- Standardisation Request M/585 C(2022)5637
- Delegated Regulation (EU) 2022/30
- RED WG 8 Communication Deck on 1st Working Draft (access only to CEN/CLC JTC 13 and Liaisons)

www.umlaut.com

Disclaimer

Backup - Current hEN draft in CEN/CLC JTC 13 WG 8 Exemplary requirements – Logging mechanism

4.6 Logging mechanism

4.6.1 Application of logging mechanisms [EF]

4.6.1.1 Requirement [E]

The equipment shall provide appropriate mechanisms to log events of internal activities that can have an impact on the protection of privileged data, personal data, traffic data and location data, unless

— the "equipment's reasonably foreseeable and intended use" does not allow logging; or

— the "intended operational environment of use" does not allow logging; or

— legal obligations prohibit logging.

4.6.1.2 Requirement [F]

The equipment shall provide appropriate mechanisms to log events of internal activities that can have an impact on the protection of privileged data and data related to the transfer of money, monetary value or virtual currency, unless

— the "equipment's reasonably foreseeable and intended use" does not allow logging; or

— the "intended operational environment of use" does not allow logging; or

— legal obligations prohibit logging.

4.6.1.3 Rationale [E]

To provide information about events of the equipment related to the protection of privileged data, personal data, traffic data, location data the equipment must generate relevant logs. Such log information can be of support to help identify e.g., potential unusual equipment behaviour, security/data breaches.

4.6.1.4 Rationale [F]

To provide information about events of the equipment related to the protection of privileged data and data related to the transfer of money, monetary value or virtual currency the equipment must generate relevant logs. Such log information can be of support to help identify e.g., potential unusual equipment behaviour, security/data breaches.

4.6.1.5 Guidance

Recording of events that have security implications or forensic value can help to identify potential unusual equipment behaviour and security breaches.

4.6.1.6 Assessment criteria

tbd

4.6.2 Appropriate logging mechanisms [EF]

4.6.2.1 Requirement [E]

Each logging mechanism which are subject to 4.6.1 shall be appropriate:

— for the "equipment's reasonably foreseeable and intended use" to log events of internal activities that can have an impact on the protection of privileged functions, privileged data, personal data, traffic data, location data; and

— for the "intended operational environment of use"; and

— to legal constraints; and

— to satisfy data protection requirements; and

— to satisfy data retention and deletion requirements.

4.6.2.2 Requirement [F]

Each logging mechanism which are subject to 4.6.1 shall be appropriate:

— for the "equipment's reasonably foreseeable and intended use" to log events of internal activities that can have an impact on the protection of privileged functions, privileged data and the functions and data related to the transfer of money, monetary value or virtual currency; and

— for the "intended operational environment of use"; and

— to legal constraints; and

— to satisfy data protection requirements; and

— to satisfy data retention and deletion requirements.

4.6.2.3 Rationale [E]

To provide information about events of the equipment related to the protection of privileged data, personal data, traffic data, location data the equipment must generate relevant logs. Such log information can be of support to help identify e.g., potential unusual equipment behaviour, security/data breaches.

4.6.2.4 Rationale [F]

To provide information about events of the equipment related to the protection of privileged data and data related to the transfer of money, monetary value or virtual currency the equipment must generate relevant logs. Such log information can be of support to help identify e.g., potential unusual equipment behaviour, security/data breaches.

4.6.2.5 Guidance

Examples of best practices for a logging mechanism are:

— implement the option on the equipment to configure the logging activities;

— indicate to the user where the log data is stored;

— store an event only once;

4.6.4 Logged activities [F]

Logged activities which are subject to 4.6.1 shall be appropriate:

— for the "equipment's reasonably foreseeable and intended use"; and

— for the "intended operational environment of use"; and

— for the risks to the protection of privileged functions, privileged data and the functions and data related to the transfer of money, monetary value or virtual currency; and

— addressing legal obligations; and

— include security events.

4.6.4.1 Rationale [EF]

To create relevant log information, the respective events/triggers need to be identified. Logging is there to support analysing unintended and malicious use of the equipment. The investigation related to a bad actor who connects to a consumer IoT device such as a webcam or toy.

4.6.4.2 Guidance [E]

Logging is there to support analysing unintended and malicious use of the equipment, examples of logging events are:

— activities on the assets such as access, add, edit, remove/archive, delete;

— unauthorized access attempts;

— If the equipment has physical breach sensors any triggers should be logged.

See standards such as IEC 62443-4-2 and NIST SP 800-92