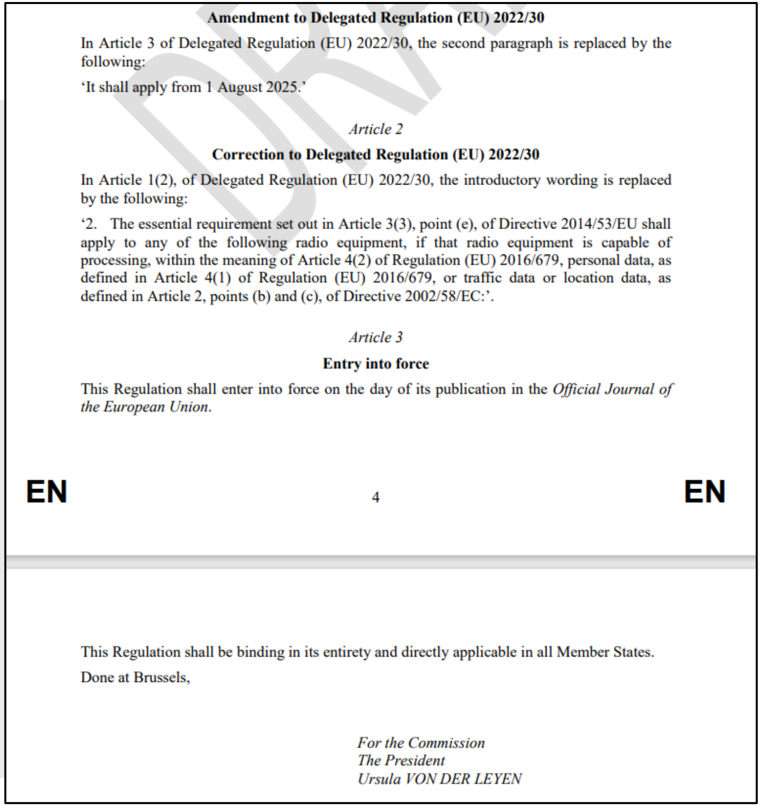
Infotag Licht
Cybersecurity Anforderungen in der RED 3.(3) d,e,f: Aktueller Status und Ausblick

Dr. Stephan Kloska

Alexander Matheus

Current Status RED 3.3

- Amendment to delegated regulation
  - New date „shall apply“ -> 01st August 2025
  - Not published in the official Journal of the EU yet.
  - New date for Standards -> 30th June 2024
    - Harmonization (publishing in official Journey)



Amendment to Delegated Regulation (EU) 2022/30

In Article 3 of Delegated Regulation (EU) 2022/30, the second paragraph is replaced by the following:

‘It shall apply from 1 August 2025.’

Article 2

Correction to Delegated Regulation (EU) 2022/30

In Article 1(2), of Delegated Regulation (EU) 2022/30, the introductory wording is replaced by the following:

‘2. The essential requirement set out in Article 3(3), point (e), of Directive 2014/53/EU shall apply to any of the following radio equipment, if that radio equipment is capable of processing, within the meaning of Article 4(2) of Regulation (EU) 2016/679, personal data, as defined in Article 4(1) of Regulation (EU) 2016/679, or traffic data or location data, as defined in Article 2, points (b) and (c), of Directive 2002/58/EC:’.

Article 3

Entry into force

This Regulation shall enter into force on the day of its publication in the *Official Journal of the European Union*.

EN 4 EN

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels,

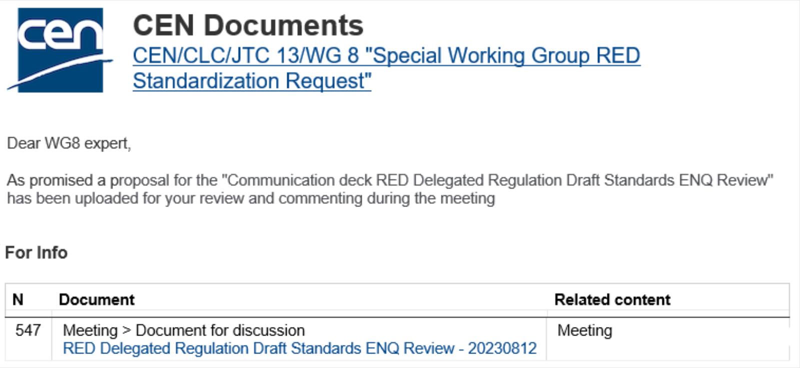
For the Commission
The President
Ursula VON DER LEYEN

VDE INSTITUTE

Actual status standards for RED 3.3 (d), (e), (f)

- ENQ Status -> until 16. November 2023

- Review and commenting of national bodies
  - until 16. November 2023



CEN Documents

CEN/CLC/JTC 13/WG 8 "Special Working Group RED Standardization Request"

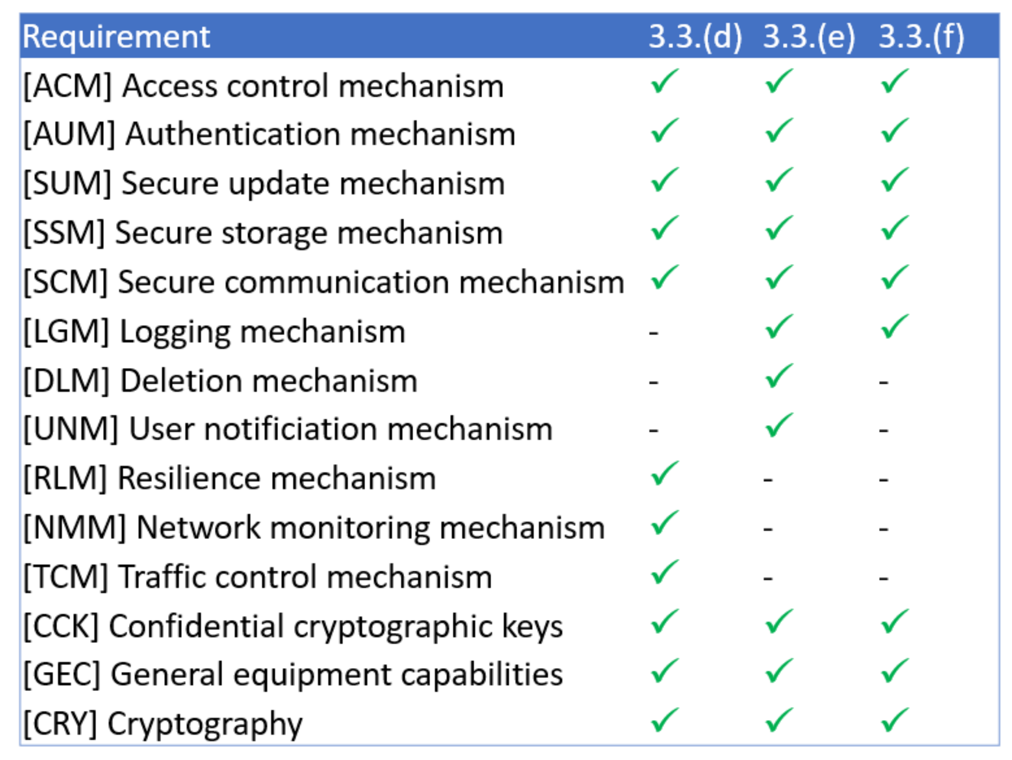
Dear WG8 expert,

As promised a proposal for the "Communication deck RED Delegated Regulation Draft Standards ENQ Review" has been uploaded for your review and commenting during the meeting

For Info

N	Document	Related content
547	Meeting > Document for discussion RED Delegated Regulation Draft Standards ENQ Review - 20230812	Meeting

Structure of new standards



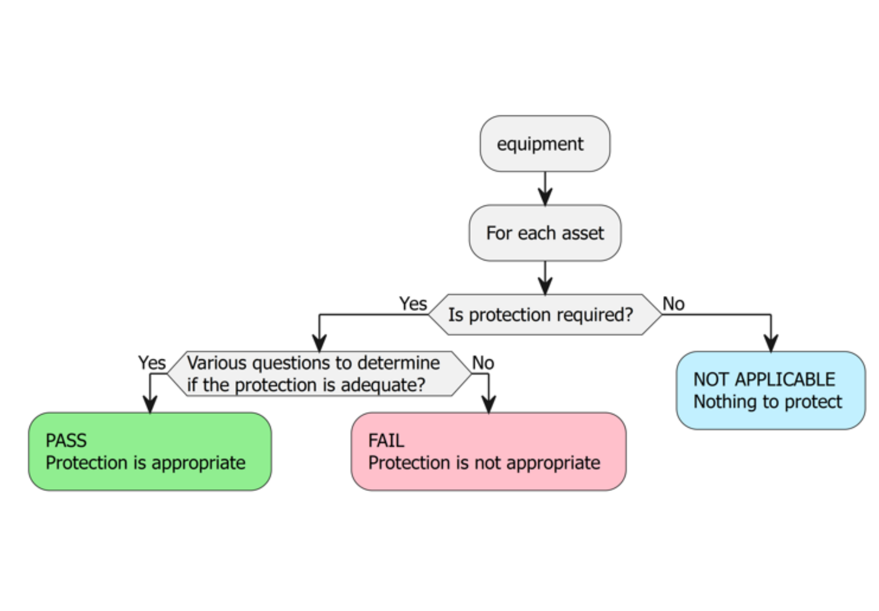
Requirement	3.3.(d)	3.3.(e)	3.3.(f)
[ACM] Access control mechanism	✓	✓	✓
[AUM] Authentication mechanism	✓	✓	✓
[SUM] Secure update mechanism	✓	✓	✓
[SSM] Secure storage mechanism	✓	✓	✓
[SCM] Secure communication mechanism	✓	✓	✓
[LGM] Logging mechanism	-	✓	✓
[DLM] Deletion mechanism	-	✓	-
[UNM] User notificiation mechanism	-	✓	-
[RLM] Resilience mechanism	✓	-	-
[NMM] Network monitoring mechanism	✓	-	-
[TCM] Traffic control mechanism	✓	-	-
[CCK] Confidential cryptographic keys	✓	✓	✓
[GEC] General equipment capabilities	✓	✓	✓
[CRY] Cryptography	✓	✓	✓

14 sections vs
9 sections in SR
(except special devices)

Standard concept for assessment

- Decision tree concept
  - Applicability
  - Appropriate

- Assessments
  - Conceptual
  - Functional
    - Complete
    - Adequate


equipment
For each asset
Yes
Is protection required?
No
Yes
Various questions to determine if the protection is adequate?
No
NOT APPLICABLE Nothing to protect
PASS Protection is appropriate
FAIL Protection is not appropriate

Security documentation

- Technical documentation:
  General:
  - information on the equipment’s intended use
  - information on the equipment’s expected operational environment of use
  - equipment’s technical information
  - declared state of the art and best practice
  - specific details such as a list of external interfaces
  - risk assessment

  - [E.Doc.DT.xxxxxx] Description
  - [E.Just.DT.xxxxxx] Justification

VDE-PB-0033

- Basis for security tests (documents, functional, pentests) -> Requirements from SR (Standaristaion request) of the delegated regulation
- EU-TEC (Type examination certificate):
  A method to prepare for the security requirements and to support development activities.
- EU-TEC valid for 2 years
- EU-TEC for modules and products possible

- Delta Analysis to ENQ drafts ongoing
- Once the new standards will be published, the VDE-PB-0033 will be adjusted (additional time for the harmonization needs to be considered)

CRA

Horizontal requirements on product security

- CRA Cyber Resilience Act
  - Draft was published on the 15.09.2022
    -> after signing 12/24 months transition period
  - Holistic cybersecurity for all connected hardware and software products
  - Complete life-cycle in scope
    (from development to sometime after bringing into the market)
  - Duties for manufacturers and importers
    -> included in the NLF (mandatory regulation -> CE label)
  - Conformity assessment according to harmonized standards
  - Information duties to governmental security agency
  - Penalties
  - Requirements from the RED 3.3 d,e,f will be included (delegated regulation will be repealed or amended)

heise online heise+

European Commission

CYBER RESILIENCE ACT

New EU cybersecurity rules ensure more secure hardware and software products

#DigitalEU #SecurityUnion #Cybersecurity

Quelle: https://www.heise.de/news/Cyberresilienz-EU-Kommission-sagt-Sicherheitsluecken-den-Kampf-an-7260034.html

CRA intention

Motivation: Yearly damage of 5.5 trillion € by 2021 caused by cyber crime

1. Conditions are to be established to develop secure products.
2. Users should be able to actively choose products in regards to cybersecurity for the individual needs.

Goals:

1. Manufacturers must ensure, that cybersecurity is enhanced during the whole life-cycle of the product (from the design phase up to decommissioning)
2. A cyber-security-framework should be established, which determines the conformity of hard- and software-products.
3. Enhancements of the transparency of the security measures of the products.
4. Companies and users should be enabled to use digital products securely.

CRA scope

Products with digital elements (examples)

- End devices, z.B.: laptops, smartphones, sensors and cameras; smart robots; smart cards; smart meters; mobile devices; smart speakers; routers; switches; industrial control systems
- Software: firmware; operating systems; mobile apps; desktop applications; video games
- Components (both hardware as well as software): computer processing units; video cards; software libraries.

- Not in Scope :
  - medical devices ((EU)2017/745)
  - in vitro diagnostic ((EU)2017/746)
  - civil aviation (2018/1139)
  - motor vehicles ((EU) 2019/2144)
  - Not mentioned: digitale services

Classes:

Uncritical

-> Self declaration

Critical Products I + II

-> Self declaration,
Conformity assessment 3rd party

CRA Annex 1 : ESSENTIAL CYBERSECURITY REQUIREMENTS

1 SECURITY REQUIREMENTS RELATING TO THE PROPERTIES OF PRODUCTS WITH DIGITAL ELEMENTS

1. Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks;
2. Products with digital elements shall be delivered without any known exploitable vulnerabilities;
3. On the basis of the risk assessment referred to in Article 10(2) and where applicable, products with digital elements shall:
   secure by default configuration, protection from unauthorised access protect the confidentiality of data (confidentiality, integrity, availability), minimisation of data, Verfügbarkeit, mimimizing of the attack vector, monitoring, security updates

-> Development and risk-analysis
   (Security-by-design)
-> Process to research vulnerabilities

-> Main principles of cybersecurity:
   Confidentiality, Integrity, Availablility (CIA)
-> product standards

VDE INSTITUTE

CRA Annex 1 : ESSENTIAL CYBERSECURITY REQUIREMENTS

2 VULNERABILITY HANDLING REQUIREMENTS

Manufacturers of the products with digital elements shall:

1. identify and document
2. remediate vulnerabilities without delay
3. apply effective and regular tests
4. publically disclose information about fixed vulnerabilities
5. vulnerability disclosure;
6. sharing of information about potential vulnerabilities in their product with digital elements
7. securely distribute updates for products with digital elements
8. disseminate security patches without delay and free of charge

Processes for vulnerability handling must be established

CERT (CERT@VDE)

JTC13 WG9

- JTC13 WG 9 was established on the 3rd of July 2023
- Standardization Request was received in July
- Establishment of SRAHG
- Approach: Making usage of already existing standards, add additional ones if required
- Demanding Timeline
- Horizontal (generic) and vertical (product) standards
  - 31.05.2025 (generic) SR -> EiF in Q3 2024 -> Q3 2026 (COM), Q3 2027 (Parliament and Council)
  - 31.05.2026 (product) SR -> EiF in Q3 2024 -> Q3 2026 (COM), Q3 2027 (Parliament and Council)

- Reporting 31.05.2025 SR -> EiF in Q3 2024 -> Q3 2025 (COM), Q3 2026 (Parliament), Q3 2026 (Council)

EIF (Entry into force)

VDE INSTITUTE

UK Requirements (PSTI)

The UK Product Security and Telecommunications Infrastructure (Product Security) regime

The UK's consumer connectable product security regime will come into effect on **29 April 2024.**

From that date, the law will require manufacturers of UK consumer connectable products to comply with minimum security requirements.

These minimum security requirements are based on the UK's Code of Practice for Consumer IoT security, the leading global standard for consumer IoT security ETSI EN 303 645, and on advice from the UK's technical authority for cyber threats, the National Cyber Security Centre.

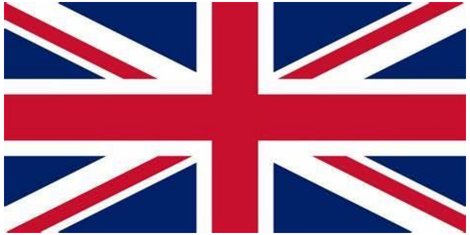
The regime comprises two pieces of legislation:

Part 1 of the Product Security and Telecommunications Infrastructure (PSTI) Act 2022;

The Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations, subject to parliamentary approval.

Requirements:

- Requirements for Passwords
- Requirement to report security issues (vulnerabilities, incidents)
- Requirements to inform the customer about the support of security patches



ETSI EN 303 645

ISO/IEC 29147

VDE INSTITUTE

Conclusion

- VDE can offer you from now on testing services and EU-Type Examination Certificate for article 3, 3. (d), (e) and (f)
- Notified Body under the RED is mandatory until harmonised standards are published and cited
- Early action is recommended especially for new developments, since the 2025-08-01 is not that far away!
- In the future Cyber Resilience Act CRA might replace the (new) requirements in the RED.
- Requirements for the UK will get active already in 2024.

VDE-Institute is your reliable partner for testing radio equipment for Safety, EMC, Spectrum and network protection, cybersecurity and privacy and to act as Notified Body under the RED.

Thank you
for your attention!

We are building the e-dialistic future.
Please join us.

Your contact:
Testing: Alexander Matheus

Phone +49 69 8306-499
alexander.matheus@vde.com

NB-RED: Dr. Stephan Kloska

Phone +49 69 8306-747
stephan.kloska@vde.com

VDE INSTITUTE