Cybersecurity

Current status regarding regulation

Alexander Matheus

VDE INSTITUT

Introduction: VDE Test and Certification instituite

- Founded 1920, worldwide activities
- More than 100.000 tests per year
- The department „Smart Technologies“ was founded 2012:
  - Information security
  - Functional safety

- Assessments of information security on Smart Home Systems, IoT-Systems, Medical technology and Industry 4.0 Systems
- Conformity-tests and penetration-tests in the laboratory in Offenbach
- DAkkS accreditation as testing lab according to ISO/IEC 17025
  - Since 2020 accreditation as testing lab for IEC 62443-4-2

Impulse : More than 100years of Safety – and now?

Quiz:

What is shown here?

1. A device to increase the security for a building or home?
2. A safe device (as a CE label is attached)?
3. One of the biggest threat for the economy?

Answer:

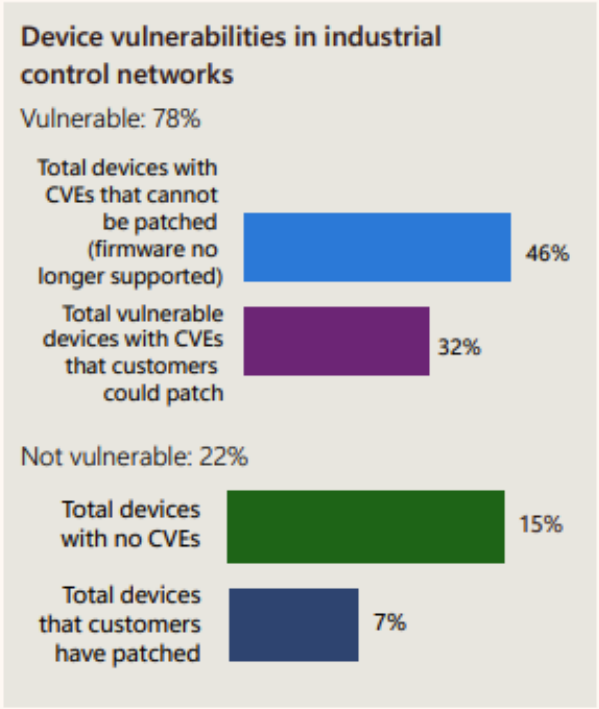
1+2+3 as IP Cameras could be and were hacked and misused for cybercrime:

- Become part of a Bot-Net
- Entry-point for trojans
- Spying device….

Is the threat real?

- The EU estimates an „estimated global annual cost of cybercrime of EUR 5.5 trillion by 2021”
  („Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020” - CRA)
- “Wannacry” attack in 2017 resulted in 230.000 infected computers and damages of 4 billion US $
- Ransomware trojans are a very successful business model which are organised in company-like structures

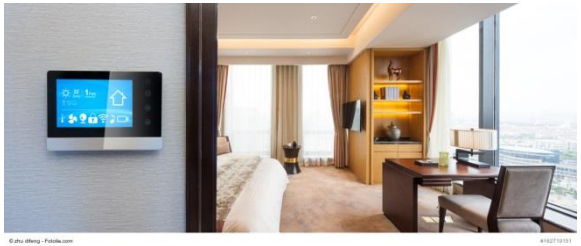
➢ Safe but insecure IoT Devices are a major threat for the economy as they are potential gateways for trojans.



Source: Microsoft Defender for IoT sensors

Cyber Security: a cross-sectional topic

Testing of devices and systems since 2012 (> 60 active certificates, >250 projects)
ISO27001 certified, TISAX



Smart Home

Medical technology

IoT (Internet of things)/connected appliances

Automotive

Industry 4.0

IEC 62443-4-2 Accreditation

VDE INSTITUTE

EU Cyber Strategy - Steps

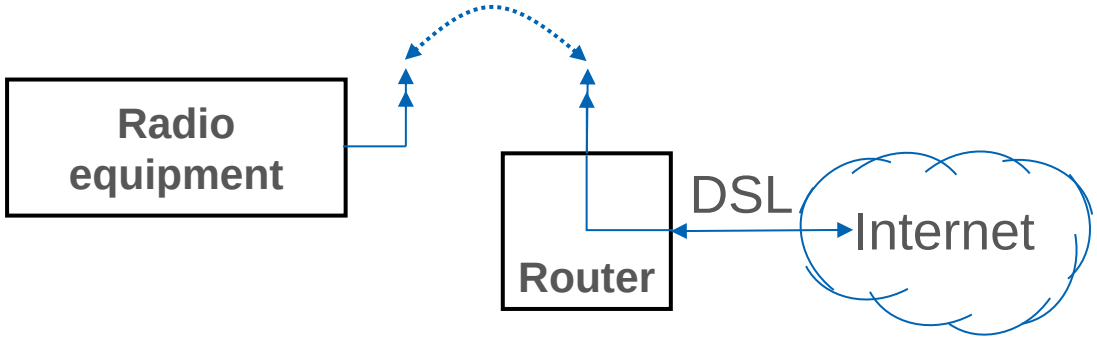
1. Voluntary label: Example BSI „IT-Sicherheitskennzeichen“ VDE listed on the BSI Web-side
2. RED 3.3 d,e,f -> comes into force 01.08.2025
   - -Existing regulation
   - -new standards EN 18031 (CEN/CENELEC)

   Formal vote 26th of June 2024 positive
   Published in August 2024
   No citation suggested by HAS consultant
3. CRA (Cyber Resilience Act) EU 2024/2847
   - -New Regulation
   - -Signed 10.10.2024, published 20.11.2024
   - -Transition time 36 months for products, 21 months for processes
   - -Existing standards (adjustments), new standards

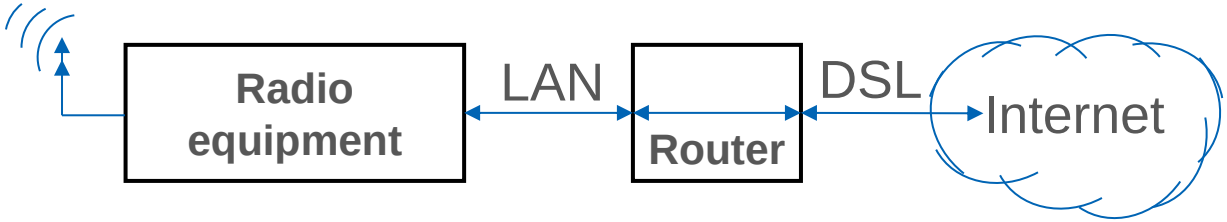
   Transition Time started
   -> 11-09-2026 Vulnerability reporting
   -> 11-12-2027 Products
4. (PSTI: UK Product Security and Telecommunications Infrastructure (Product Security) regime)
   - -29.April 2024

RED 3.3 d,e,f (2014/35/EU) Delegated regulation

Article 1, 1. “Internet connected radio equipment”



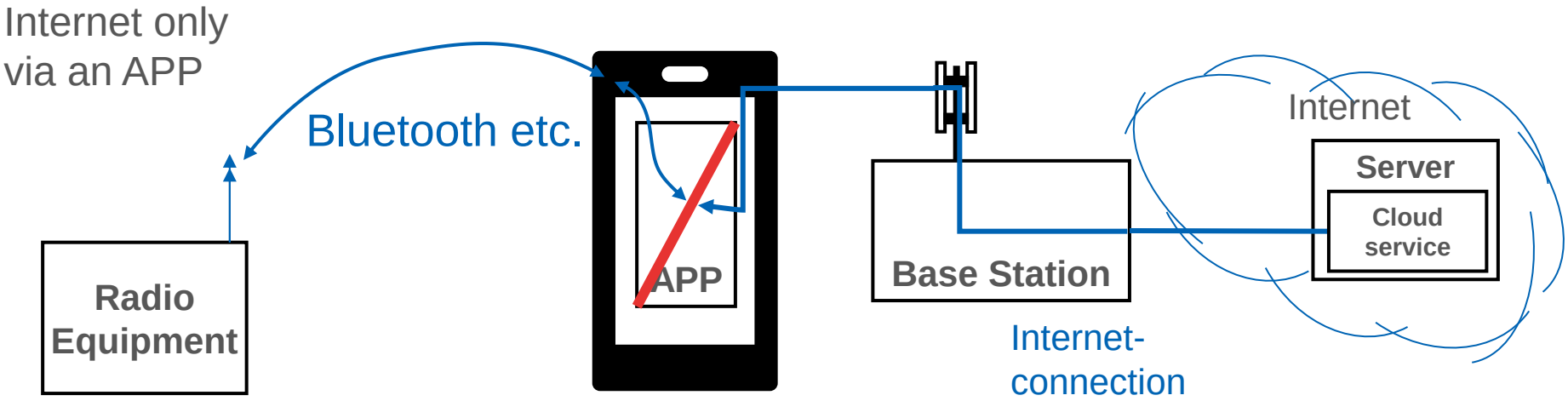
e.g. BT or RFID



Both scenarios are „internet connected radio equipment“ according 2022/30/EU

What is or is not in the scope of the delegated regulation?

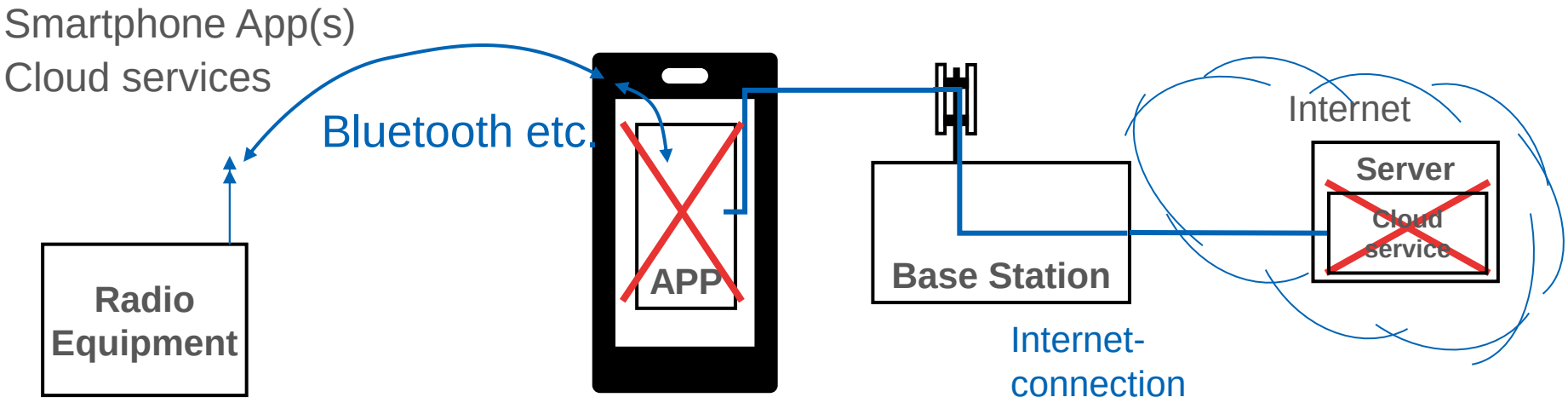
NOT in the scope



The Radio Equipment is not capable to connect itself to the internet!

What is or is not in the scope of the delegated regulation?

NOT in the scope



Constraints of the RED regulation

- Existing scope definitions of the existing regulation have to be adapted;
  - Only radio equipment (i.e. 5G, WLAN, BLE… included)
  - Only devices – no smartphone apps, no cloud applications
  - No Security processes (i.e. no development processes, no vulnerability handling processes)

  - Additional scope restrictions for the sections :
    d-> Internet connection
    e-> Privacy data or location data in the device + Internet connection or Toys/Childcare/Wearables
    f-> monetary value processing in the device

➢ Many devices will not be in the scope of the RED 3.3 d,e,f regulation

➢ **Limited scope and no complete view on security,**
but an important start for cyber-security for products

RED 3.3 d,e,f: Development of harmonised standards (EN)

- CEN/CLC/JTC 13 WG8 - Cybersecurity and data protection (Joint committee CEN and CENELEC)
- Three standards were developed for each Article 3, 3. (d), (e) and (f):

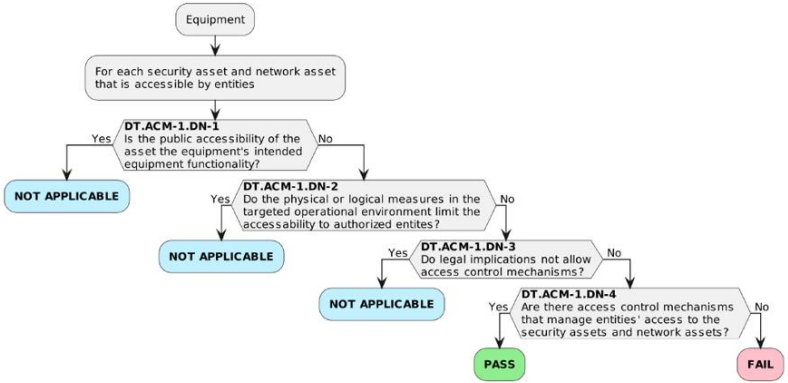
d-> Internet connection	EN 18031-1
e-> Privacy data or location data in the device	EN 18031-2
f-> monetary value processing in the device	EN 18031-3

- Formal vote of the European commitees June 2024 was positive
  -> harmonized standards
- Published August 2024
- But no HAS Consultant recommendation for a citation in the official journal
  -> no possibility for a self-declaration with a conformity assumption
  -> Current solution: EU type examination certificate by a notified body

EU-commission:
-Cite in full
-Cite with restrictions
-No citation

Details of the EN 18031-1/-2/-3 standard

- Published on the 14th August 2024
- 11 Requirement topics
- 31 Sub-Requirements
- Asset based approach:
  - Security assets
  - 1: Network assets
  - 2: Privacy assets
  - 3: Financial assets
- Decision tree for every requirement
- Specific requirements for the documentations (mandatory + conditional).



FprEN18031 Documentation requirements

- E.Info information for all requirements
- Security assets
- Network assets (-1)
- Privacy assets (-2)
- Financial assets (-3)
- E.info and E.just for Decision trees

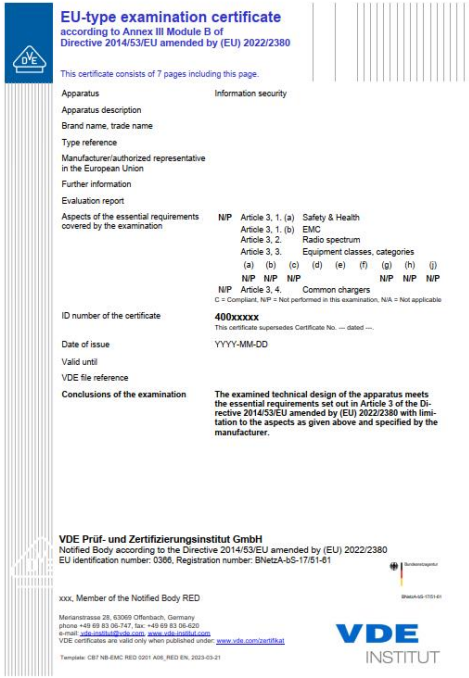
Documentation Checklist	#	Requirement	Required information	Mandatory/Condition
	6.1.1	[ACM-1] Applicability of access control mechanisms	E.Info.ACM-1.SecurityAsset	M
			E.Info.ACM-1.SecurityAsset.Access	M
			E.Info.ACM-1.SecurityAsset.PublicAccess	C
			E.Info.ACM-1.SecurityAsset.Environment	C
			E.Info.ACM-1.SecurityAsset.Legal	C
			E.Info.ACM-1.SecurityAsset.ACM	C
			E.Info.ACM-1.NetworkAsset	M
			E.Info.ACM-1.NetworkAsset.Access	M
			E.Info.ACM-1.NetworkAsset.PublicAccess	C
			E.Info.ACM-1.NetworkAsset.Environment	C
			E.Info.ACM-1.NetworkAsset.Legal	C
			E.Info.ACM-1.NetworkAsset.ACM	C
			E.Info.DT.ACM-1	M
			E.Just.DT.ACM-1	M
	6.1.2	[ACM-2] Appropriate access control mechanisms	E.Info.ACM-2.SecurityAsset	M
			E.Info.ACM-2.SecurityAsset.ACM	M
			E.Info.ACM-2.NetworkAsset	M
			E.Info.ACM-2.NetworkAsset.ACM	M
			E.Info.DT.ACM-2	M
			E.Just.DT.ACM-2	M

VDE services offers RED 3.3 d,e,f

- Workshops
  - Requirement workshops for the accordant devices/systems
  - Risk analysis workshops

- Check up test:
  - Determine actual status of device/system in view of RED 3.(3) d), e) and/or f) requirements
  - Result: Gap analysis and list of missing information/documents

- EU-Type examination certificate
  - Assessment according to the internal VDE requirements or other standards:
    - EN18031-1/-2/-3 or ETSI EN 303 645 (VDE-PB-0033)
      or IEC 62443-4-2 (plus Deltas)
  - Certificate to state the fulfillment of the requirements of RED 3.(3) d), e) and/or f)
    -> Valid test report for the regulation



EU-type examination certificate
according to Annex III Module B of
Directive 2014/53/EU amended by (EU) 2022/2380

This certificate consists of 7 pages including this page.

Apparatus
Apparatus description
Brand name, trade name
Type reference
Manufacturer/authorized representative in the European Union
Further information
Evaluation report

Information security

Aspects of the essential requirements covered by the examination

N/P Article 3, 1. (a) Safety & Health
Article 3, 1. (b) EMC
Article 3, 2. Radio spectrum
Article 3, 3. Equipment classes, categories
(a) (b) (c) (d) (e) (f) (g) (h) (j)
N/P N/P N/P N/P N/P N/P N/P
N/P Article 3, 4. Common chargers
C = Compliant, N/P = Not performed in this examination, N/A = Not applicable

ID number of the certificate: **400xxxxx**
This certificate supersedes Certificate No. --- dated ----.

Date of issue: YYYY-MM-DD
Valid until
VDE file reference

Conclusions of the examination

The examined technical design of the apparatus meets the essential requirements set out in Article 3 of the Directive 2014/53/EU amended by (EU) 2022/2380 with limitation to the aspects as given above and specified by the manufacturer.

VDE Prüf- und Zertifizierungsinstitut GmbH
Notified Body according to the Directive 2014/53/EU amended by (EU) 2022/2380
EU identification number: 0366, Registration number: BNetzA-bS-17/51-61

xxx, Member of the Notified Body RED

Merianstrasse 28, 63069 Offenbach, Germany
phone +49 69 83 06-747, fax: +49 69 83 06-620
e-mail: vde-institut@vde.com, www.vde-institut.com
VDE certificates are valid only when published under: www.vde.com/zertifikat

Template: CB7 NB-EMC RED 0201 A06_RED EN, 2023-03-21

VDE INSTITUT

CRA Cyber Resiliance Act

CRA Cyber Resilience Act EU 2024/2847

- Regulation signed 10.10.2024, published 20.11.2024
  Will become active in September 2026 for vulnerability notification and in December 2027 for products
- Scope: “Products with digital elements”
- Holistic approach cybersecurity for all connected hardware and software products (i.e. Smartphone-Apps, Cloud application)
- Vulnerability Handling is an essential part (Security processes)
- Complete life-cycle in scope:
  From development (“Security-by-design”) to after-market support
- Duties for manufacturers and importers
  -> included in the NLF (mandatory regulation -> CE label)
- Conformity assessment according to harmonized standards
  Product classes: Critical products will need a 3rd party certification
- Information duties to governmental security agency
- Penalties are already planned
- Requirements from the RED 3.3 d,e,f will be included (delegated regulation will be repealed or amended)

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

Important Products I + II
Critical Products
-> Self declaration,
Conformity assessment 3rd party

(Notified Body: BSI probably notifying body)

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 unauthorized access protect the confidentiality of data (confidentiality, integrity, availability), minimization of data, availability, minimizing 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 (horizontal and vertical)
-> SBOM (Software Bill of Material)

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)

CRA Anhang 3:
IMPORTANT PRODUCTS WITH DIGITAL ELEMENTS: Class I

Class I

1. Identity management systems and privileged access management software and hardware, including authentication and

access control readers, including biometric readers

2. Standalone and embedded browsers

3. Password managers

4. Software that searches for, removes, or quarantines malicious software

5. Products with digital elements with the function of virtual private network (VPN)

6. Network management systems

7. Security information and event management (SIEM) systems

8. Boot managers

9. Public key infrastructure and digital certificate issuance software

10. Physical and virtual network interfaces

11. Operating systems

12. Routers, modems intended for the connection to the internet, and switches

13. Microprocessors with security-related functionalities

14. Microcontrollers with security-related functionalities

15. Application specific integrated circuits (ASIC) and field-programmable gate arrays (FPGA) with security-related

functionalities

16. Smart home general purpose virtual assistants

17. Smart home products with security functionalities, including smart door locks, security cameras, baby monitoring

systems and alarm systems

18. Internet connected toys covered by Directive 2009/48/EC of the European Parliament and of the Council (1) that have

social interactive features (e.g. speaking or filming) or that have location tracking features

19. Personal wearable products to be worn or placed on a human body that have a health monitoring (such as tracking)

purpose and to which Regulation (EU) 2017/745 or (EU) No 2017/746 do not apply, or personal wearable products

that are intended for the use by and for children

CRA Annex 3:
IMPORTANT PRODUCTS WITH DIGITAL ELEMENTS: Class II

Class II

1. Hypervisors and container runtime environments
2. Firewalls, intrusion detection and prevention
3. Tamper-resistant microprocessors
4. Tamper-resistant microcontrollers

CRA Annex 4
CRITICAL PRODUCTS WITH DIGITAL ELEMENTS

1. Hardware Devices with Security Boxes
2. Smart meter gateways within smart metering systems as defined in Article 2, point (23) of Directive (EU) 2019/944 of the European Parliament and of the Council (1) and other devices for advanced security purposes, including for secure cryptoprocessing
3. Smartcards or similar devices, including secure elements

CRA Anhang 4
EU-KONFORMITÄTSERKLÄRUNG

Die EU-Konformitätserklärung gemäß Artikel 20 enthält alle folgenden Angaben:

1. den Namen und den Typ sowie alle zusätzlichen Informationen, die eine eindeutige Identifizierung des Produkts mit digitalen Elementen ermöglichen;
2. den Namen und die Anschrift des Herstellers oder seines Bevollmächtigten;
3. eine Erklärung darüber, dass der Anbieter die alleinige Verantwortung für die Ausstellung der EU-Konformitätserklärung trägt;
4. den Gegenstand der Erklärung (Bezeichnung des Produkts zwecks Rückverfolgbarkeit, gegebenenfalls mit Foto);
5. eine Erklärung, dass der oben beschriebene Gegenstand der Erklärung den einschlägigen Harmonisierungsrechtsvorschriften der Union entspricht;
6. Verweise auf die verwendeten einschlägigen harmonisierten Normen oder sonstigen gemeinsamen Spezifikationen oder die Cybersicherheitszertifizierung, für die die Konformität erklärt wird;
7. gegebenenfalls den Namen und die Kennnummer der notifizierten Stelle, eine Beschreibung des durchgeführten Konformitätsbewertungsverfahrens und die Kennnummer der ausgestellten Bescheinigung;
8. weitere Angaben: Unterschrift, Ort, Datum

-> Hinweis auf Cybersicherheit

CRA Anhang 5 + 6

- Anhang 5 INHALT DER TECHNISCHEN DOKUMENTATION
- Anhang 6 KONFORMITÄTSBEWERTUNGSVERFAHREN (Module A, B, C, H)

Konformitätsbewertungsverfahren auf der Grundlage einer internen Kontrolle (auf der Grundlage von Modul A)

EU-Baumusterprüfung (auf der Grundlage von Modul B)

Konformität mit dem Baumuster auf der Grundlage einer internen Fertigungskontrolle (auf der Grundlage von Modul C)

Konformität auf der Grundlage einer umfassenden Qualitätssicherung (auf der Grundlage von Modul H)

ANHANG V

INHALT DER TECHNISCHEN DOKUMENTATION

Die in Artikel 23 genannte technische Dokumentation muss mindestens die folgenden Informationen enthalten, soweit sie für das betreffende Produkt mit digitalen Elementen von Belang sind:

1. eine allgemeine Beschreibung des Produkts mit digitalen Elementen, einschließlich
   a) seiner Zweckbestimmung,
   b) Softwareversionen, die sich auf die Erfüllung der grundlegenden Anforderungen auswirken,
   c) wenn es sich bei dem Produkt mit digitalen Elementen um ein Hardwareprodukt handelt: Fotografien oder Abbildungen, aus denen äußere Merkmale, Kennzeichnungen und innerer Aufbau hervorgehen;
   d) Informationen und Anleitungen für die Nutzer gemäß Anhang II;
2. eine Beschreibung der Konzeption, Entwicklung und Herstellung des Produkts und der Verfahren zur Behandlung von Schwachstellen, einschließlich
   a) vollständiger Informationen über die Konzeption und Entwicklung des Produkts mit digitalen Elementen, gegebenenfalls mit Zeichnungen und Schemata und/oder einer Beschreibung der Systemarchitektur, aus der hervorgeht, wie Softwarekomponenten aufeinander aufbauen, miteinander zusammenwirken und sich in die Gesamtverarbeitung integrieren;

JTC13 WG9

- JTC13 WG 9 was established on the 3rd of July 2023

- Approach: Making usage of already existing standards, add additional ones if required (Horizontal/Vertical), coordination with Working groups:
  - Process hENs
  - hENs to cover ETSI EN 303 645
  - hENs to cover IEC 62443
  - hENs Annex III products (CRITICAL PRODUCTS WITH DIGITAL ELEMENTS)

- Project Team 1: General principles
- Project Team 2: Common security requirements
- Project Team 3: Security vulnerability handling

CRA: BSI - Information

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber_Resilience_Act/cyber_resilience_act_node.html

Federal Office for Information Security

Technical Guideline TR-03183:
Cyber Resilience Requirements for Manufacturers and Products

Conclusion

- The EU commission started to introduce mandatory product requirements for security.
- New delegated regulation 2022/30/EU is published for the Radio Equipment Directive.
- Notified Body under the RED is mandatory until harmonised standards are published and cited.
  - EU Technical examination certificate possible:
    - Documentation check (Requirements from the EN 18031 or VDE-PB-0033)
    - Vulnerability check on the device
- Early action for manufacturers is recommended, since the 2025-08-01 is less than a year!
- In the future Cyber Resilience Act CRA might replace the (new) requirements in the RED.
- CRA will become active for vulnerability notifications in September 2026 and for products in Dezember 2027

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