Nye standarder under radioudstyrsdirektivet styrker cybersikkerhed

Webinar 5. september 2024

Dagens program

10:00 **Velkommen**

10:05 **Indblik i de nye krav om cybersikkerhed i radioudstyrsdirektivet samt introduktion til de tre standarder; EN 18031-1, EN 18031-2 og EN 18031-3**

Torben Markussen, Kamstrup – aktiv ekspert i udarbejdelsen af de tre standarder under radioudstyrsdirektivet

10:45 **Spørgsmål og afrunding**

11:00 **Tak for i dag**

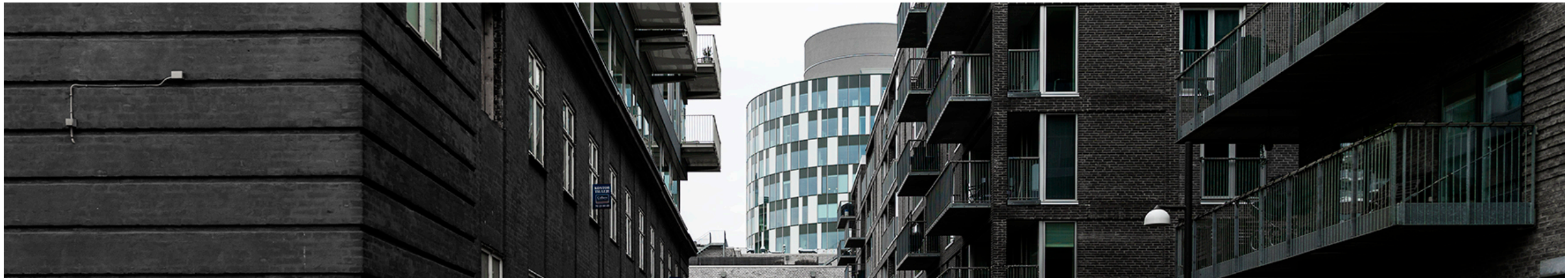
Om Dansk Standard

Hvem er Dansk Standard

- Danmarks officielle standardiseringsorganisation
- Erhvervsdrivende fond, grundlagt i 1926
- Ca. 200 medarbejdere
- Erhvervspolitisk partnerskab med Erhvervsministeriet

Vi er medlem af:

En stærk platform af solide brands:



Dansk Standards udvalg for cyber- og informationssikkerhed er med til at skrive fremtidens standarder

DANSK STANDARD

Udvalget består af 55+ medlemmer fra store danske virksomheder, smv'er, konsulenthuse, offentlige myndigheder, NGO'er, brancheorganisationer mm.

- Åbent for alle interesserede
- Beslutter den danske holdning
- Sikrer, at de danske interesser bliver varetaget på den internationale bane
- Bidrager til at definere fremtidens markedskrav

Aktuelle temaer

- Holde øje med udviklingen og implementeringen af relevant lovgivning på cyberområdet; fx Cyber Resilience Act, Cyber Security Act, Radioudstyrsdirektivet og NIS2.
- Følge aktivt med i udviklingen af de standarder, der skal udarbejdes i relation til EU lovgivning, herunder standarder under Cyber Resilience Act og Radioudstyrsdirektivet.
- Eventuelle revisioner af ISO/IEC 27000 serien
- Udbrede kendskabet til standarder for cyber- og informationssikkerhed gennem egne arrangementer, indlæg på eksterne arrangementer, via artikler mm.

Læs mere om udvalget på ds.dk/s-441

Three new standards to support Product Security Requirements under the Radio Equipment Directive

Dansk Standard – Webinar, September 5th 2024

Torben Markussen
Wireless Solution Architect
RF Communication, Kamstrup A/S

Agenda

- Recap (short)
  - Radio Equipment Directive (RED)
  - Delegated Regulation (2022/30)
  - Standardisation Request (M/585)
- Three new EN 18031 standards
  - Availability and status
  - Next steps
- Working with the standards
  - Scope considerations
  - Reading guide
  - Reservations

Radio Equipment Directive

When does Radio Equipment Directive apply to a product?

- Radio equipment into the EU market
- Radio function within the product
  - Transmitters
  - Receivers
  - Transceivers
- Frequency range of up to 3000 GHz

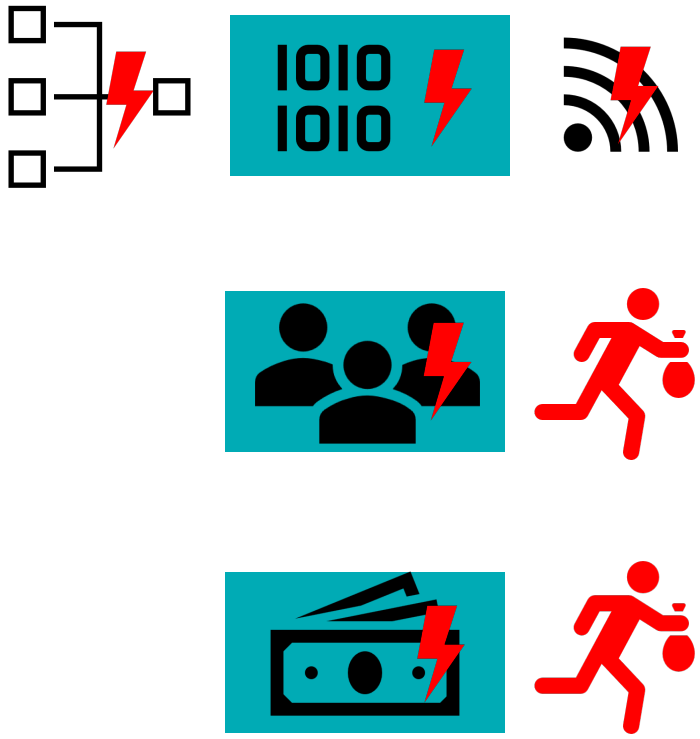
Essential requirements scope

Product Safety Article 3.1.a	EMC Performance Article 3.1.b	Radio Performance Article 3.2	Other categories Article 3.3

Changes in Cybersecurity Legislation in EU

RED Delegated Regulation (2022/30) activates (other categories) Articles 3.3.(d)(e)(f)

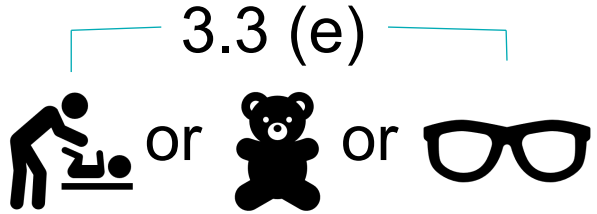
- 3.3 (d) “radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service”
- 3.3 (e) “radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected”
- 3.3 (f) “radio equipment supports certain features ensuring protection from fraud”



Scope of Regulation 2022/30

- Internet connected

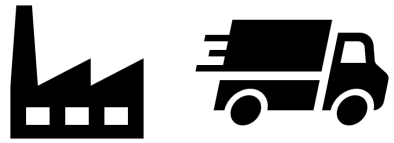
- OR childcare, toys or wearables



Applicability date

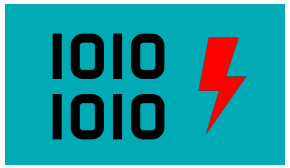
- Enters into force 1st August 2025

- All products “placed on the market” after this date must comply



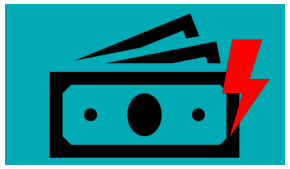
Standardization Request (M/585)

- Write three generic (product and technology agnostic) **harmonised standards**



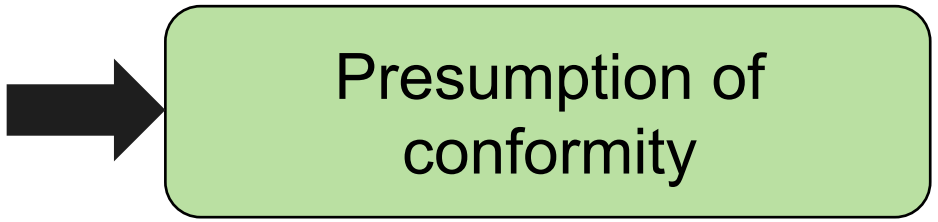
3.3 (d)

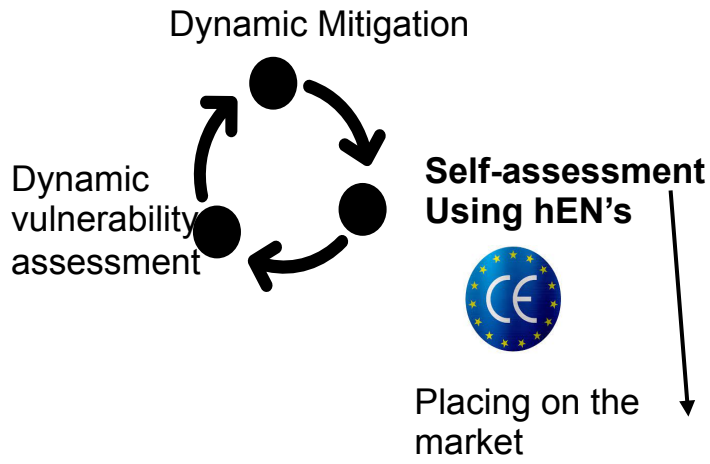
3.3 (e)



3.3 (f)

- Harmonised (cited in the OJEU) standards can be used under NLF in the EU



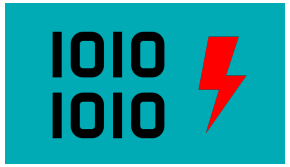


Three new cybersecurity standards

“Status”

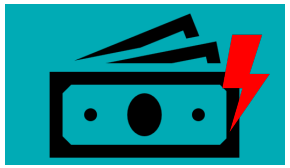
Status of the standards

- Three standards have been developed in CEN/CLC JTC13 WG8:



EN 18031-1

EN 18031-2



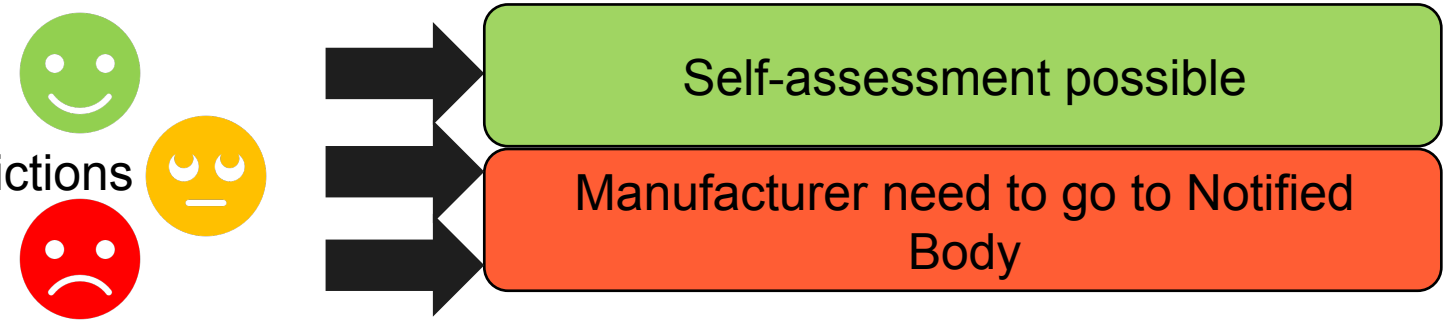
EN 18031-3

- Formal vote during spring resulted in 100% support from the member states
- In parallel, the standards have been scrutinized by HAS Consultants
- CEN/CENELEC decided to **publish** the three standards on August 14th 2024
- The outcome of the HASC evaluation was negative. They reported **severe problems** with the standards due to **legal uncertainty**

→ No presumption of conformity

Now what?

- The commission will decide on the way forward **early September 2024**
- Any amendment to the standards will take at least 9-12 months (+ translation)
- Options:
  - Full citation
  - Cited with restrictions
  - Not cited



- The published standards (even if not cited) WILL be used as guidance by
  - Manufacturers
  - Test houses
  - Notified Bodies

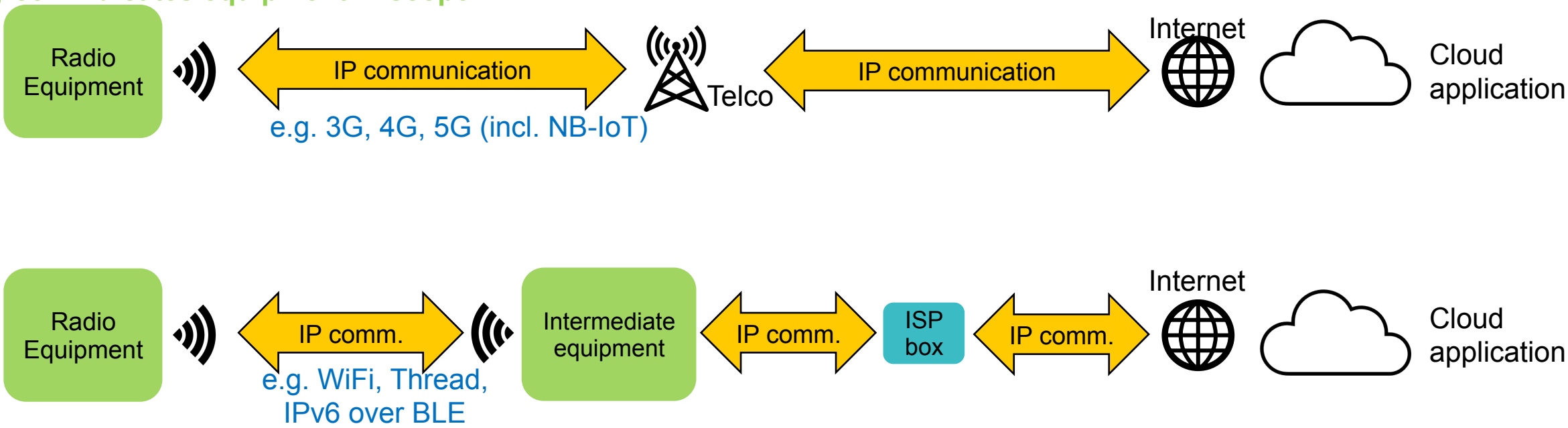
Three new cybersecurity standards

“Scope”

Scope (assumption)

The radio equipment **can** operate an **end-to-end** communication session with internet, **directly or via another equipment**

***green indicates equipment in scope**

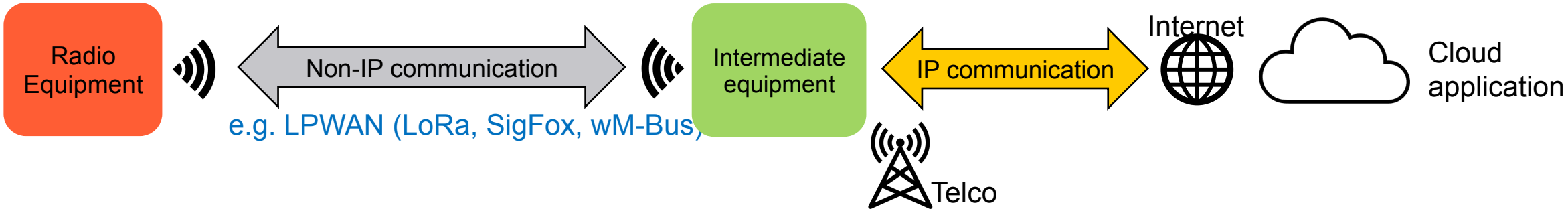


kamstrup

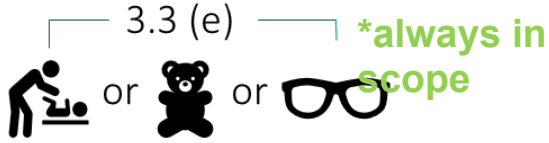
Scope (assumption)

The radio equipment **cannot** operate an **end-to-end** communication session with internet, **neither directly nor via another equipment**

***red indicates equipment out of scope**



Reservation
There are no official guidance
If in doubt: Consider assessmer



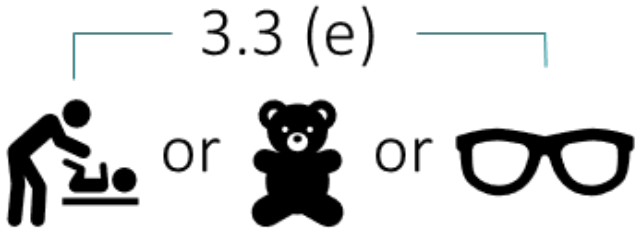
Three new cybersecurity standards

“Content”

FprEN 18031-1	FprEN 18031-2	FprEN 18031-3
[ACM-1] Applicability of access control mechanisms [ACM-2] Appropriate access control mechanisms	[ACM-1] Applicability of access control mechanisms [ACM-2] Appropriate access control mechanisms [ACM-3] Default access control for children in toys [ACM-4] Default access control to children's privacy assets for toys and childcare equipment [ACM-5] Parental/Guardian access controls for children in toys [ACM-6] Parental/Guardian access controls for other entities' access to managed children's privacy assets in toys	[ACM-1] Applicability of access control mechanisms [ACM-2] Appropriate access control mechanisms
[AUM-1] Applicability of authentication mechanisms [AUM-2] Appropriate authentication mechanisms [AUM-3] Authenticator validation [AUM-4] Changing authenticators [AUM-5] Password strength [AUM-6] Brute force protection	[AUM-1] Applicability of authentication mechanisms [AUM-2] Appropriate authentication mechanisms [AUM-3] Authenticator validation [AUM-4] Changing authenticators [AUM-5] Password strength [AUM-6] Brute force protection	[AUM-1] Applicability of authentication mechanisms [AUM-2] Appropriate authentication mechanisms [AUM-3] Authenticator validation [AUM-4] Changing authenticators [AUM-5] Password strength [AUM-6] Brute force protection
[SUM-1] Applicability of update mechanisms [SUM-2] Secure updates [SUM-3] Automated updates	[SUM-1] Applicability of update mechanisms [SUM-2] Secure updates [SUM-3] Automated updates	[SUM-1] Applicability of update mechanisms [SUM-2] Secure updates [SUM-3] Automated updates
[SSM-1] Applicability of secure storage mechanisms [SSM-2] Appropriate integrity protection for secure storage mechanisms [SSM-3] Appropriate confidentiality protection for secure storage mechanisms	[SSM-1] Applicability of secure storage mechanisms [SSM-2] Appropriate integrity protection for secure storage mechanisms [SSM-3] Appropriate confidentiality protection for secure storage mechanisms	[SSM-1] Applicability of secure storage mechanisms [SSM-2] Appropriate integrity protection for secure storage mechanisms [SSM-3] Appropriate confidentiality protection for secure storage mechanisms
[SCM-1] Applicability of secure communication mechanisms [SCM-2] Appropriate integrity and authenticity protection for secure communication mechanisms [SCM-3] Appropriate confidentiality protection for secure communication mechanisms [SCM-4] Appropriate replay protection for secure communication mechanisms	[SCM-1] Applicability of secure communication mechanisms [SCM-2] Appropriate integrity and authenticity protection for secure communication mechanisms [SCM-3] Appropriate confidentiality protection for secure communication mechanisms [SCM-4] Appropriate replay protection for secure communication mechanisms	[SCM-1] Applicability of secure communication mechanisms [SCM-2] Appropriate integrity and authenticity protection for secure communication mechanisms [SCM-3] Appropriate confidentiality protection for secure communication mechanisms [SCM-4] Appropriate replay protection for secure communication mechanisms
[RLM-1] Applicability and appropriateness of resilience mechanisms	[LGM-1] Applicability of logging mechanisms	[LGM-1] Applicability of logging mechanisms
[NMM-1] Applicability and appropriateness of network monitoring mechanisms	[LGM-2] Persistent storage of log data	[LGM-2] Persistent storage of log data
[TCM-1] Applicability of and appropriate traffic control mechanisms	[LGM-3] Minimum number of persistently stored events [LGM-4] Time-related information of persistently stored dog data [DLM-1] Applicability of deletion mechanisms [UNM-1] Applicability of user notification mechanisms [UNM-2] Appropriate user notification content	[LGM-3] Minimum number of persistently stored events [LGM-4] Time-related information of persistently stored dog data
[CCK-1] Appropriate CCKs [CCK-2] CCK generation mechanisms [CCK-3] Preventing static default values for preinstalled CCKs	[CCK-1] Appropriate CCKs [CCK-2] CCK generation mechanisms [CCK-3] Preventing static default values for preinstalled CCKs	[CCK-1] Appropriate CCKs [CCK-2] CCK generation mechanisms [CCK-3] Preventing static default values for preinstalled CCKs
[GEC-1] Up-to-date software and hardware with no publicly known exploitable vulnerabilities [GEC-2] Limit exposure of services via related network interfaces [GEC-3] Configuration of optional services and the related exposed network interfaces [GEC-4] Documentation of exposed network interfaces and exposed services via network interfaces [GEC-5] No unnecessary external interfaces [GEC-6] Input validation	[GEC-1] Up-to-date software and hardware with no publicly known exploitable vulnerabilities [GEC-2] Limit exposure of services via related network interfaces [GEC-3] Configuration of optional services and the related exposed network interfaces [GEC-4] Documentation of exposed network interfaces and exposed services via network interfaces [GEC-5] No unnecessary external interfaces [GEC-6] Input validation [GEC-7] Documentation of external sensing capabilities	[GEC-1] Up-to-date software and hardware with no publicly known exploitable vulnerabilities [GEC-2] Limit exposure of services via related network interfaces [GEC-3] Configuration of optional services and the related exposed network interfaces [GEC-4] Documentation of exposed network interfaces and exposed services via network interfaces [GEC-5] No unnecessary external interfaces [GEC-6] Input validation [GEC-8] Equipment Integrity
[CRY-1] Best practice cryptography	[CRY-1] Best practice cryptography	[CRY-1] Best practice cryptography

FprEN 18031-1	FprEN 18031-2	FprEN 18031-3
[ACM-1] Applicability of access control mechanisms [ACM-2] Appropriate access control mechanisms	[ACM-1] Applicability of access control mechanisms [ACM-2] Appropriate access control mechanisms [ACM-3] Default access control for children in toys [ACM-4] Default access control to children's privacy assets for toys and childcare equipment [ACM-5] Parental/Guardian access controls for children in toys	[ACM-1] Applicability of access control mechanisms [ACM-2] Appropriate access control mechanisms
[AUM-1] Applicability of authentication mechanisms [AUM-2] Appropriate authentication mechanisms [AUM-3] Authenticator validation [AUM-4] Changing authenticators [AUM-5] Password strength [AUM-6] Brute force protection [SUM-1] Applicability of update mechanisms [SUM-2] Secure updates [SUM-3] Automated updates [SSM-1] Applicability of secure storage mechanisms [SSM-2] Appropriate integrity protection for secure storage mechanisms [SSM-3] Appropriate confidentiality protection for secure storage mechanisms [SCM-1] Applicability of secure communication mechanisms [SCM-2] Appropriate integrity and authenticity protection for secure communication mechanisms [SCM-3] Appropriate confidentiality protection for secure communication mechanisms [SCM-4] Appropriate replay protection for secure communication mechanisms [RLM-1] Applicability and appropriateness of resilience mechanisms [NMM-1] Applicability and appropriateness of network monitoring mechanisms [TCM-1] Applicability of and appropriate traffic control mechanisms	[AUM-1] Applicability of authentication mechanisms [AUM-2] Appropriate authentication mechanisms [AUM-3] Authenticator validation [AUM-4] Changing authenticators [AUM-5] Password strength [AUM-6] Brute force protection [SUM-1] Applicability of update mechanisms [SUM-2] Secure updates [SUM-3] Automated updates [SSM-1] Applicability of secure storage mechanisms [SSM-2] Appropriate integrity protection for secure storage mechanisms [SSM-3] Appropriate confidentiality protection for secure storage mechanisms [SCM-1] Applicability of secure communication mechanisms [SCM-2] Appropriate integrity and authenticity protection for secure communication mechanisms [SCM-3] Appropriate confidentiality protection for secure communication mechanisms [SCM-4] Appropriate replay protection for secure communication mechanisms [LGM-1] Applicability of logging mechanisms [LGM-2] Persistent storage of log data [LGM-3] Minimum number of persistently stored events [LGM-4] Time-related information of persistently stored dog data	[AUM-1] Applicability of authentication mechanisms [AUM-2] Appropriate authentication mechanisms [AUM-3] Authenticator validation [AUM-4] Changing authenticators [AUM-5] Password strength [AUM-6] Brute force protection [SUM-1] Applicability of update mechanisms [SUM-2] Secure updates [SUM-3] Automated updates [SSM-1] Applicability of secure storage mechanisms [SSM-2] Appropriate integrity protection for secure storage mechanisms [SSM-3] Appropriate confidentiality protection for secure storage mechanisms [SCM-1] Applicability of secure communication mechanisms [SCM-2] Appropriate integrity and authenticity protection for secure communication mechanisms [SCM-3] Appropriate confidentiality protection for secure communication mechanisms [SCM-4] Appropriate replay protection for secure communication mechanisms [LGM-1] Applicability of logging mechanisms [LGM-2] Persistent storage of log data [LGM-3] Minimum number of persistently stored events [LGM-4] Time-related information of persistently stored dog data
[CCK-1] Appropriate CCKs [CCK-2] CCK generation mechanisms [CCK-3] Preventing static default values for preinstalled CCKs [GEC-1] Up-to-date software and hardware with no publicly known exploitable vulnerabilities [GEC-2] Limit exposure of services via related network interfaces [GEC-3] Configuration of optional services and the related exposed network interfaces [GEC-4] Documentation of exposed network interfaces and exposed services via network interfaces [GEC-5] No unnecessary external interfaces [GEC-6] Input validation	[CCK-1] Appropriate CCKs [CCK-2] CCK generation mechanisms [CCK-3] Preventing static default values for preinstalled CCKs [GEC-1] Up-to-date software and hardware with no publicly known exploitable vulnerabilities [GEC-2] Limit exposure of services via related network interfaces [GEC-3] Configuration of optional services and the related exposed network interfaces [GEC-4] Documentation of exposed network interfaces and exposed services via network interfaces [GEC-5] No unnecessary external interfaces [GEC-6] Input validation [GEC-7] Documentation of external sensing capabilities	[CCK-1] Appropriate CCKs [CCK-2] CCK generation mechanisms [CCK-3] Preventing static default values for preinstalled CCKs [GEC-1] Up-to-date software and hardware with no publicly known exploitable vulnerabilities [GEC-2] Limit exposure of services via related network interfaces [GEC-3] Configuration of optional services and the related exposed network interfaces [GEC-4] Documentation of exposed network interfaces and exposed services via network interfaces [GEC-5] No unnecessary external interfaces [GEC-6] Input validation [GEC-8] Equipment Integrity
[CRY-1] Best practice cryptography	[CRY-1] Best practice cryptography	[CRY-1] Best practice cryptography

NB: Even if requirements seems to be identical across standards, they may differ



kamstrup

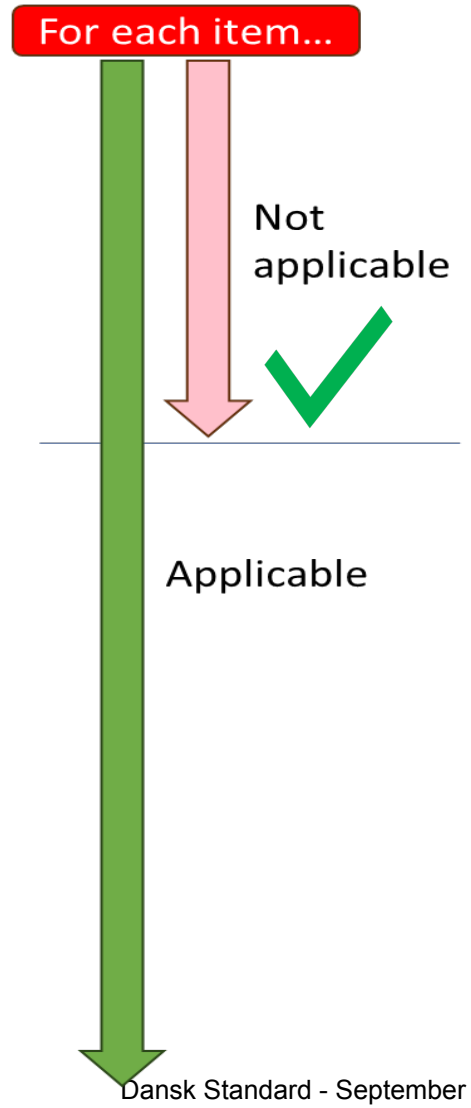
Three new cybersecurity standards

“How they are supposed to work”

Mechanism Structure

- To apply a harmonized standard for presumption of conformity with the essential requirements, the entire document shall be used.
- An applicable/non-applicable decision is taken for each of the items specified (f.ex. assets)
- If applicable it is followed by a pass/fail appropriateness decision for each of the items specified (e.g. independent interfaces)

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



Identify and document the Assets to protect

Standards are centred on the assets contained in the product

Document	Covers the essential requirements of	Addresses security assets and risks	Addresses network assets and risks	Addresses privacy assets and risks	Addresses financial assets and risks
EN 18031-1	3.3. (d)	✓	✓	✗	✗
EN 18031-2	3.3. (e)	✓	✗	✓	✗
EN 18031-3	3.3.(f)	✓	✗	✗	✓

Examples of **Network** Assets
- Server configurations
- Client configurations
- Network Configurations
- Protocol servers
- Web servers
- Network diagnostics

To protect

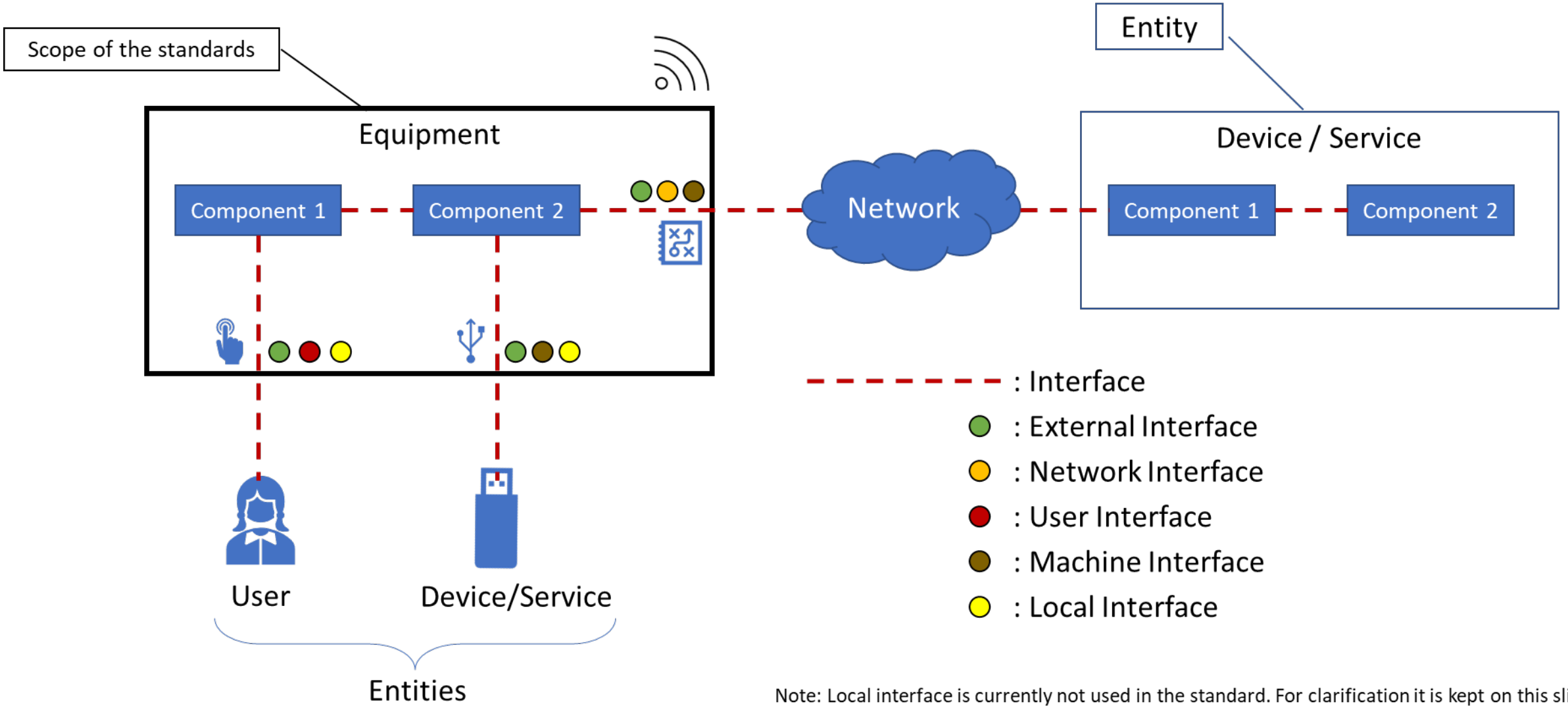
Examples of **Privacy** Assets
- Data loggers (disclosing habits)
- User data
- Behavioural or location data
- Address, gender, sexuality

Examples of **Security** Assets
- Symmetric keys
- Certificates
- Asymmetric private/public key
- Access control configuration
- Passwords
- SIM card eSIM/physical

Examples of **Financial** Assets
- Monetary representation
- Pre-payment, tariff
- Monetary transfer functions

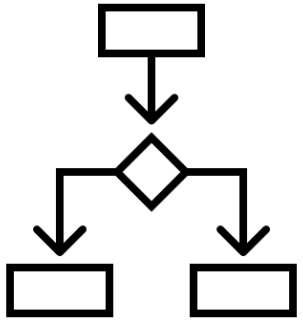
To protect

Identify and document Interfaces through which Assets can be accessed



Note: Local interface is currently not used in the standard. For clarification it is kept on this slide.

Applicability: Decision trees and exception statements



Mechanisms may include exceptions to the requirement if it can be justified security is implemented by other means.

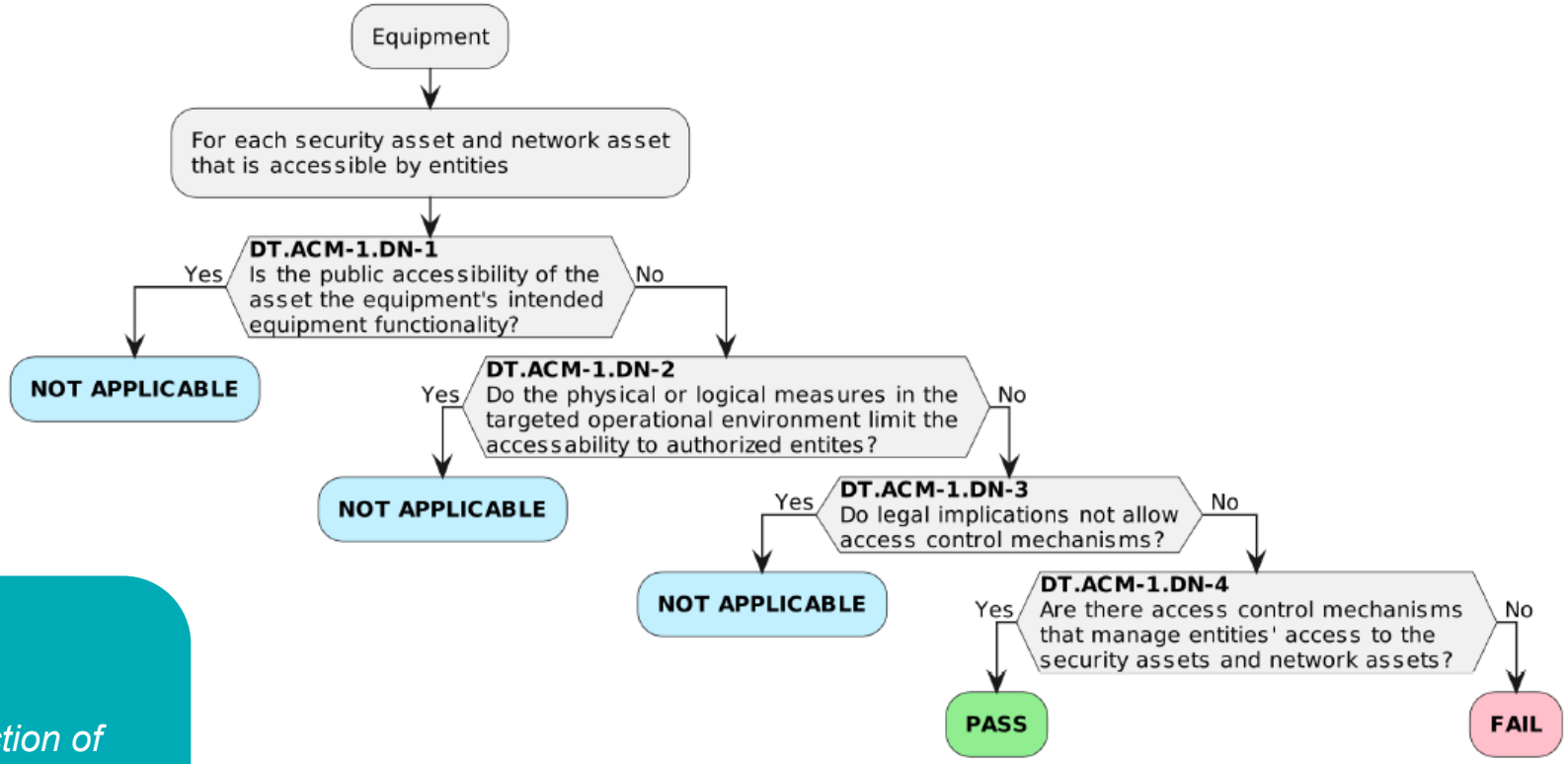


Figure 1 — Decision Tree for requirement ACM-1

Reservation
This is the major issue reported by HASC:
"Exception shifts the responsibility for the protection of the requirement beyond or beyond the control of the equipment and the manufacturer and is therefore unacceptable for this standard, which is limited to equipment and does not cover its installation."

Importance/reasoning for exceptions

- To apply a harmonized standard for presumption of conformity with the essential requirements, the entire document shall be used (self-assessment)

- Exceptions are introduced to ensure the sharing of responsibility between manufacturers and others Otherwise:

  - Existing security solutions will seem to fail or be incompatible, even though sufficient advanced security is implemented -> **NB**
  - Different protection environment (locked boxes, housings, locked premises) as protecting environment may not be sufficient -> **NB**
  - Standards may be un-fit for some manufacturers -> **NB**
  - Some industries will not be able to turn their architectures within decades -> **NB**
  - Incompatibility with investments in prominent security standards as EN 303645 (consumer IoT) IEC 62443 (industry) -> **NB**

- It is normal within harmonized standards (under NLF) to share the responsibility between manufacturer and user by declaring the use case and environment of use (e.g. temperature range, voltage range)

Documentation

- Document relevant Assets
- Document relevant Interfaces
- Document justification on the selected path(s) through the decision trees
- Document the security mechanisms implemented (if applicable)
- E.Info.xxx can point to part of a sample document (or another standard)

7.2.1.5.3 Required information

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

- [E.Info.AUM-1-1.ACM.NetworkInterfaces]: A description of the network interfaces for the managed access; and
- [E.Info.AUM-1-1.ACM.ManagedAccessNetworkAsset]: A description of the managed access to network assets via network interfaces; and
- [E.Info.AUM-1-1.ACM.ManagedAccessSecurityAsset]: A description of the managed access to security assets via network interfaces; and
- (if absence of authentication for access to network functions or network functions configuration via network interfaces is required for the equipment's intended functionality) [E.Info.AUM-1-1.ACM.IntendedFunctionality]: A description of the
  - unauthenticated accessible network functions or network functions configuration and
  - the equipment's intended functionality and
  - its properties that require the absence of authentication for access to the network functions or network functions configuration; and
- (if authentication is absent for access via networks where access is limited to authorised entities) [E.Info.AUM-1-1.ACM.TrustedNetwork]: A description the networks and the physical or logical measures in the equipment's targeted operational environment that limit access to authorized entities; and
- (if authentication is required per AUM-1-1) [E.Info.AUM-1-1.ACM.AuthenticationMechanism]: A description of the implemented authentication mechanisms.

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

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

- (if a decision from [DT.AUM-1-1.DN-1] results in "NOT APPLICABLE") the justification for the decision [DT.AUM-1-1.DN-1] is based on [E.Info.AUM-1-1.ACM.IntendedFunctionality]: and
- (if a decision from [DT.AUM-1-1.DN-2] results in "NOT APPLICABLE") the justification for the decision [DT.AUM-1-1.DN-2] is based on [E.Info.AUM-1-1.ACM.TrustedNetwork].

Determine sufficient protection

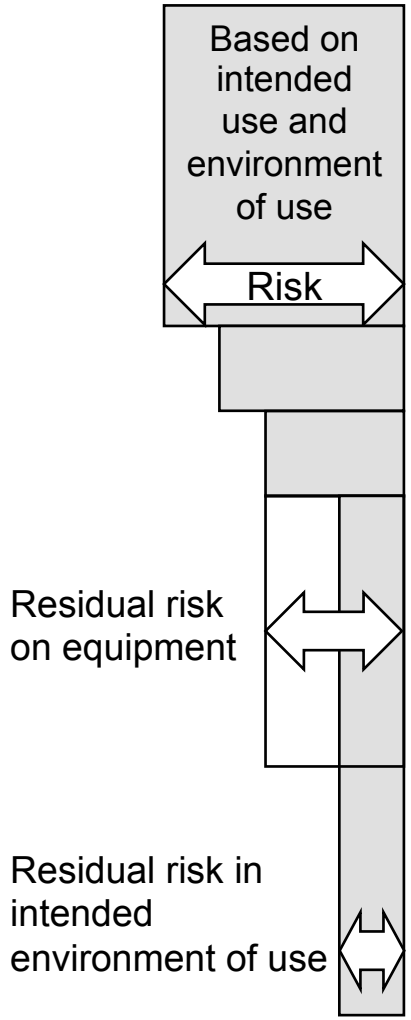
Reservations
- Zero-trust has been mentioned in early HASC evaluation comments
  - ➢ But “no risk” can never be claimed in cyber security

From the Risk assessment

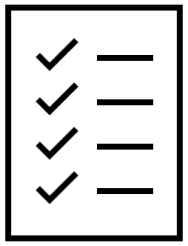
- Identify threats and calculate the risk:

$$Risk = f(P(successfull\ attack), impact\ of\ attack)$$

- Mitigate risks (iterative)
- Document the accepted residual risk



Assessment of appropriateness



Perform Assessment

- Select the implementation category used (if available)
- Perform conceptual and functional assessments

For each update mechanism documented in [E.Info.SUM-2.SUM]:

- [AU.SUM-2.Sign]: When the implementation is based on [IC.SUM-2.AuthIntVal.Sign], functionally confirm that:
  - it is implemented using best practice cryptography according to CRY-1; and
  - an unsigned software update is not installed; and
  - a software update with a modified signature is not installed; and
  - a modified software update with a valid signature for the unmodified software update is not installed; and
  - a software update with a signature from an unauthorized entity is not installed.
- [AU.SUM-2.SecChan]: When the implementation is based on [IC.SUM-2.AuthIntVal.SecChan], functionally confirm that:
  - it is implemented using the secure communication mechanism according to SCM; and
  - a software update from an unauthorized source is not installed; and
  - the secure communication channel does not allow to impersonate the authorized software updates source via a man-in-the-middle attack; and
  - a software update that is modified during communication is not installed.
- [AU.SUM-2.AccContMech]: When the implementation is based on [IC.SUM-2.AuthIntVal.AccContMech], functionally confirm that:
  - it is implemented using the access control mechanism according to ACM; and
  - a modified software update with a valid hash for the unmodified software update is not installed; and
  - a software update with a hash generated by an unsupported hash function is not installed; and
  - a software update provided by an unauthorized entity is not installed.
- [AU.SUM-2.Generic]: When the implementation is based on [IC.SUM-2.AuthIntVal.Generic], functionally confirm that:
  - a software update whose integrity is not valid is not installed; and
  - a software update whose authenticity is not valid is not installed.

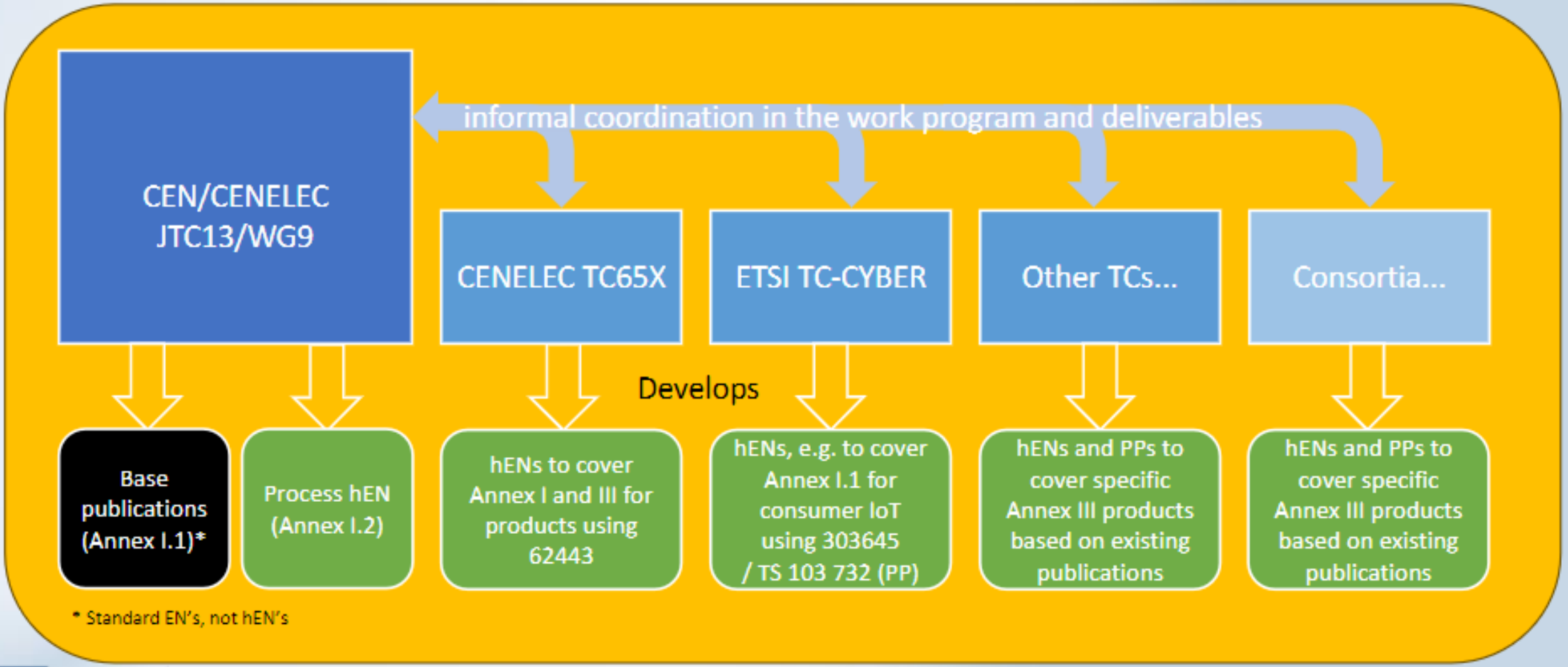
Take-aways

- Standards are available for purchase in some countries (f.ex. https://webshop.ds.dk/)
- Uncertainty if full citation is possible
- Expected statement from the commission early September about the way forward
- It is the first harmonized standard ever addressing legal cybersecurity requirements for radio products
- The standards are the only existing standards aimed for article 3.3.(d), (e) and (f)
- Notified Bodies are of the opinion that these are the best standards existing for the purpose
- It seems they will be used actively, so make yourself familiar with the standards and make your gap analysis
- There are a limited number of Notified Bodies available in EU certified to Article 3.3

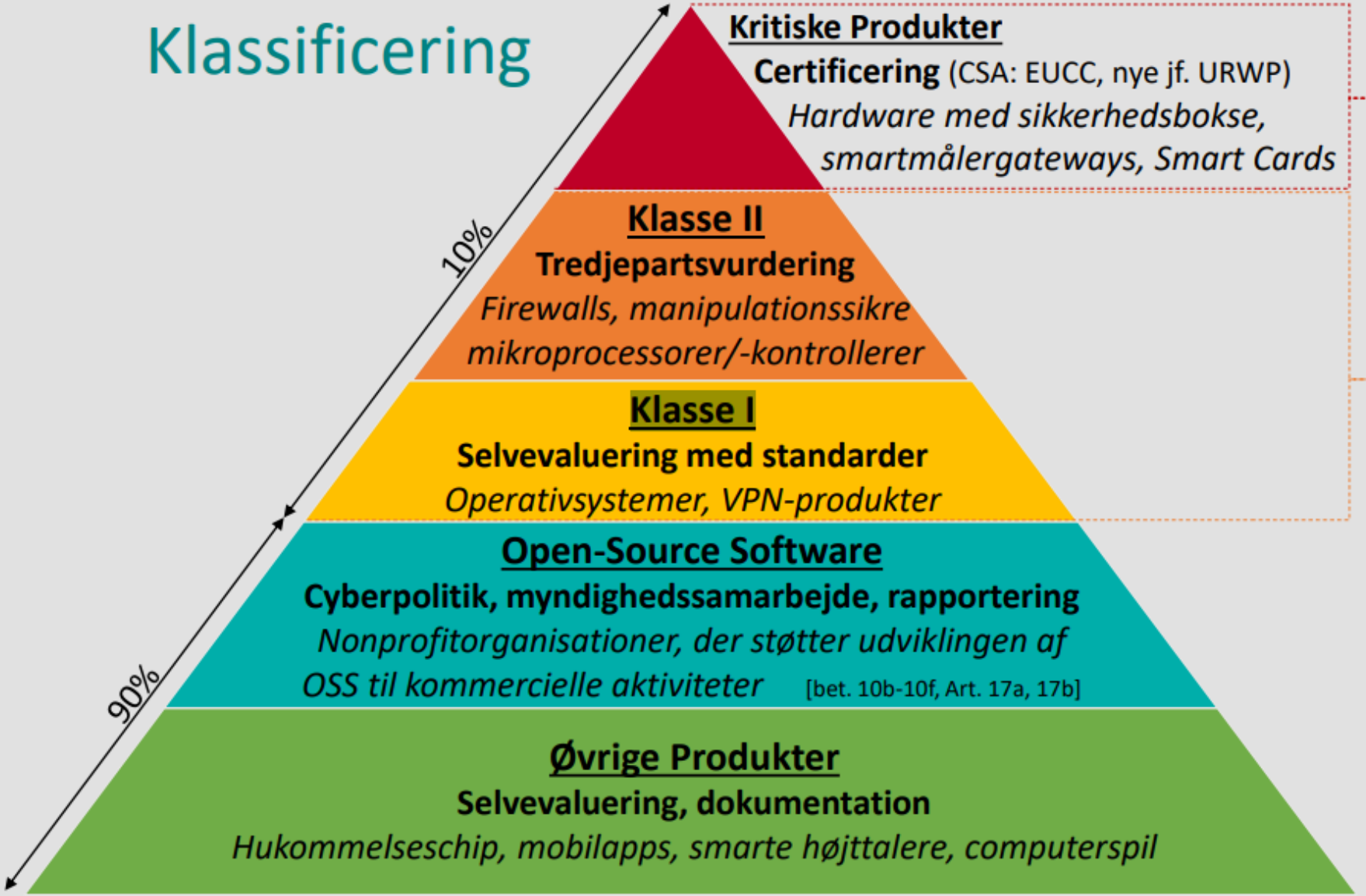
Thank you!

toma@kamstrup.com

Proposal considering the availability of experts in specific area's, including non-ESO organizations



Klassificering



"Kritiske Produkter"

- Kritisk afhængighed hos 'væsentlige enheder' (NIS2)
- Risiko for alvorlige forstyrrelser af kritiske forsyningskæder på tværs af det indre marked

[Art. 6a & Bilag IIIa]

"Vigtige Produkter"

- Udfører primært funktioner kritiske for cybersikkerheden i andre produkter, netværk eller tjenester
- Indebærer en betydelig risiko for negative effekter eller skade på et stort antal produkter eller brugere

[Art. 6 & Bilag III]

digitaliserings og ligestillingsministeriet

Hvilke produkter er omfattet?

- **Produkter med digitale elementer**, der er gjort tilgængelige på markedet, hvis tilsigtede formål eller rimeligt forudsigelige brug omfatter en direkte eller indirekte logisk eller fysisk dataforbindelse til en enhed eller et netværk.
  - Ethvert software- eller hardwareprodukt og dets fjerndatabehandlingsløsninger, herunder software- eller hardwarekomponenter, der skal markedsføres separat.

✚ **Hardware produkter** og komponenter, der tilgængeliggøres på marked separat
- Fx bærbare computere, smarte apparater, mobiltelefoner, netværksudstyr, CPU'er, industrielle robotter
- **Komponenter**: fx grafikkort, bundkort og sensorer

✚ **Software produkter** og komponenter, der tilgængeliggøres på marked separat
- Fx operativsystemer, tekstbehandling, regneark, spil, browsere og mobilapps
- **Komponenter**: fx tilføjelser, plugins og browserudvidelser

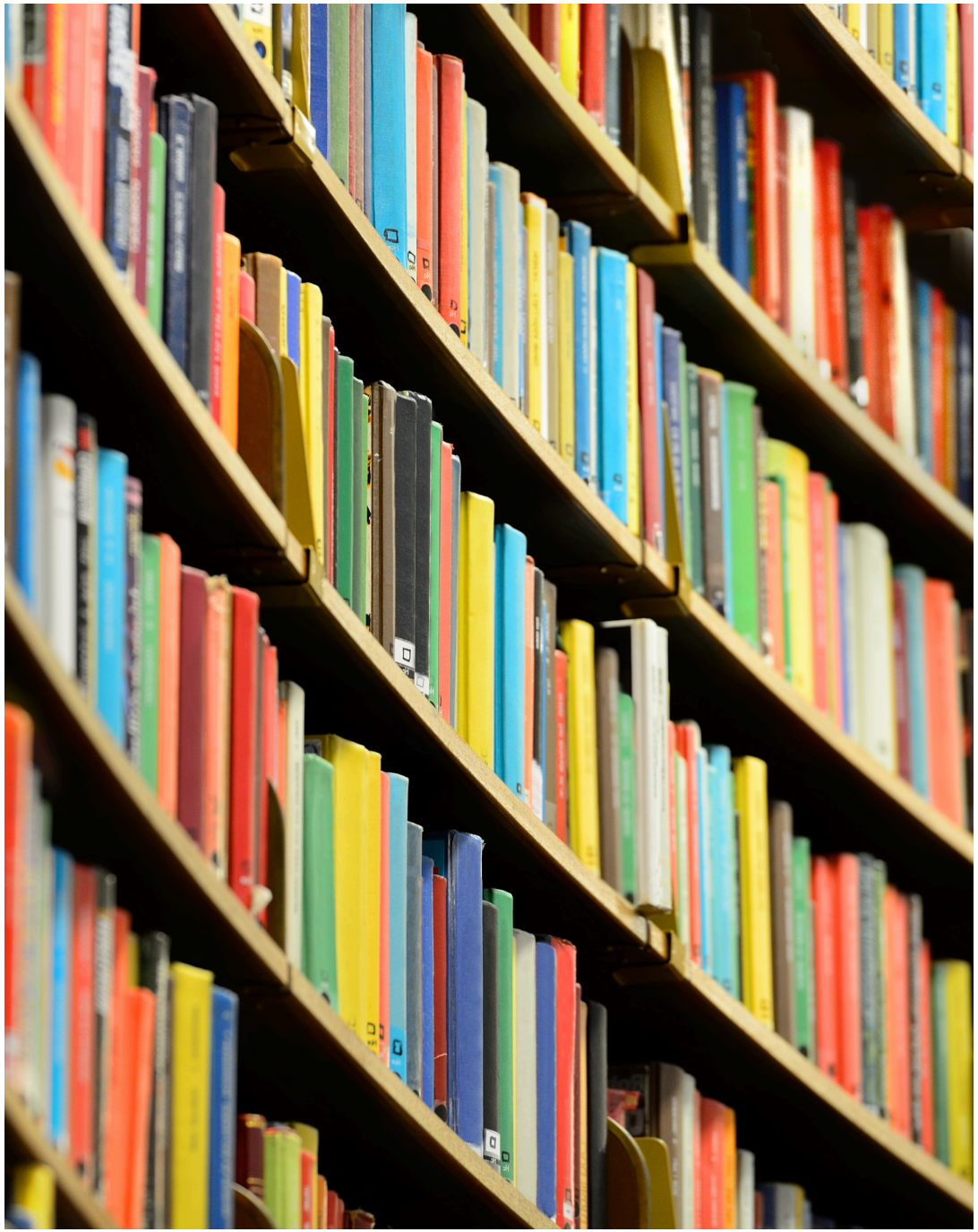
✚ **Fjerndatabehandling**
- Kontrolfunktion til en smart-termostat hostet i clouden;
- Indkøbs-app, der gemmer indkøbslisten i en database på producentens server;
- Browser der gemmer adgangskoder, bogmærker eller historik på producenternes servere;
- Cloud-baseret tekstbehandling

✖ **Ikke-kommercielle produkter**
- Open Source (uden betalte tillægstjenester/support)
- Offentlige løsninger som ikke er del af en kommerciel aktivitet

✖ **Tjenester** (fx enkeltstående Cloud / SaaS / hjemmesider)
- Dækket (delvist) af NIS2
- KOM vurderer at 80-90% af digitale tjenester i realiteten omfattes

✖ **Særregulering, nationale kompetencer, m.fl.**
- Identiske reservedele
- Produkter udelukkende udviklet eller tilpasset tbf. national sikkerhed og militære formål
- Køretøjer (2019/2144 EU)
- Medicinsk udstyr (2017/745 & 2017/746 EU)
- Certificeret luftfartsudstyr (2018/1139 EU)

digitaliserings og ligestillingsministeriet



Standarderne kan købes i Dansk Standards webshop https://webshop.ds.dk/

DS/EN 18031-1:2024 Generelle sikkerhedskrav til radioudstyr – Del 1: Radioudstyr med internetforbindelse

DS/EN 18031-2:2024 Generelle sikkerhedskrav til radioudstyr – Del 2: Radioudstyr, der behandler data, herunder radioudstyr med internetforbindelse, radioudstyr til brug i forbindelse med børneomsorg, radioudstyr til legetøj og bærbart radioudstyr

DS/EN 18031-3:2024 Generelle sikkerhedskrav til radioudstyr – Del 3: Radioudstyr med internetforbindelse, der anvendes til virtuel valuta eller valutaværdi

Spørgsmål?

DS CYBERDAG

DANSK STANDARD

3. oktober 2024

Tilmelding via https://www.ds.dk/da/ydelser/kurser/cyberdag

DANSK STANDARD