DS CYBERDAG

DS
DANSK STANDARD

Sammenhæng mellem lovgivning og standarder
&
Nye cybersikkerhedskrav for radioudstyr

Samspil mellem EU-lovgivning og standarder

Astrid Bækby Knudsen

Standarder er frivillige indtil nogen sætter dem i kraft!

Standarder sættes i kraft på 3 måder

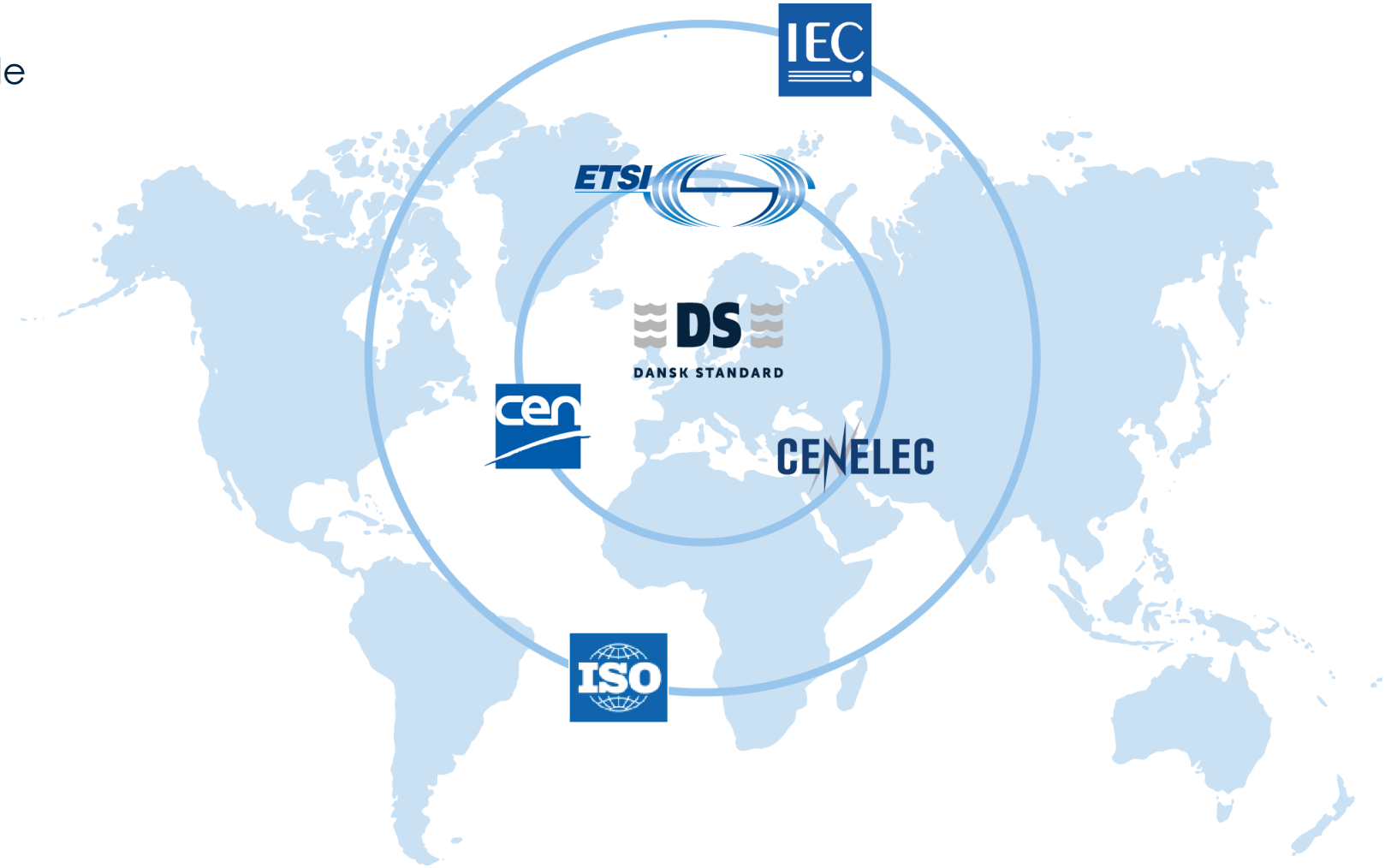
- Aftale mellem to parter
- Dansk Lovgivning, love, bekendtgørelser, regler
- EU-lovgivning, Direktiver, CE-mærkning

Organisationer der udvikler standarder

I Danmark er 98% af standarder europæiske eller internationale.

Særligt for europæiske standarder (EN) gælder:

- De skal implementeres som nationale standarder af 34 lande(CEN/CENELEC medlemmer)
- Nationale standarder i konflikt skal trækkes tilbage (gælder også EN/ISO/IEC).



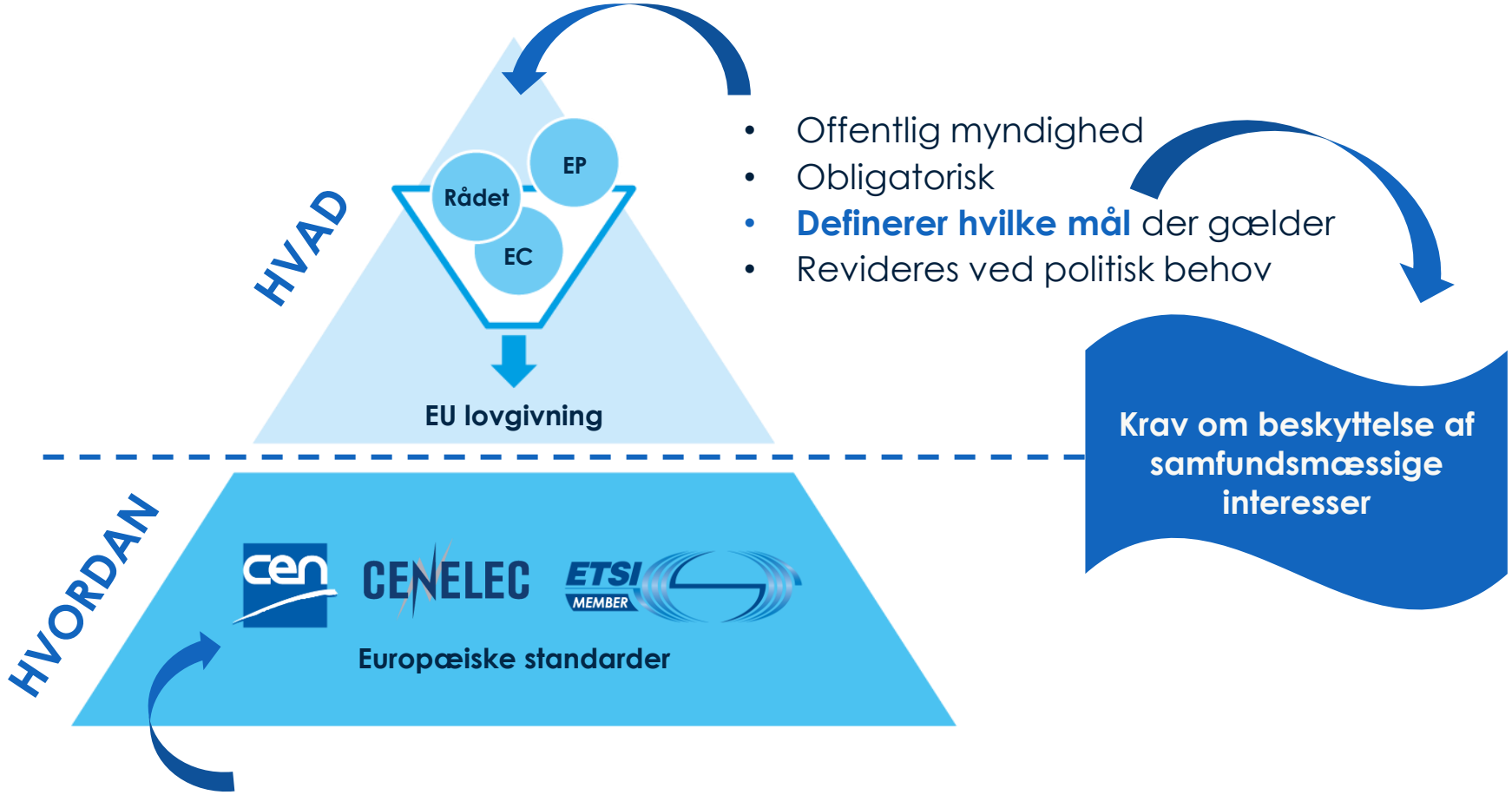
14 %

af CEN CENELECs standarder er harmoniserede standarder (hEN)

Hvad er en harmoniseret standard (hEN)?

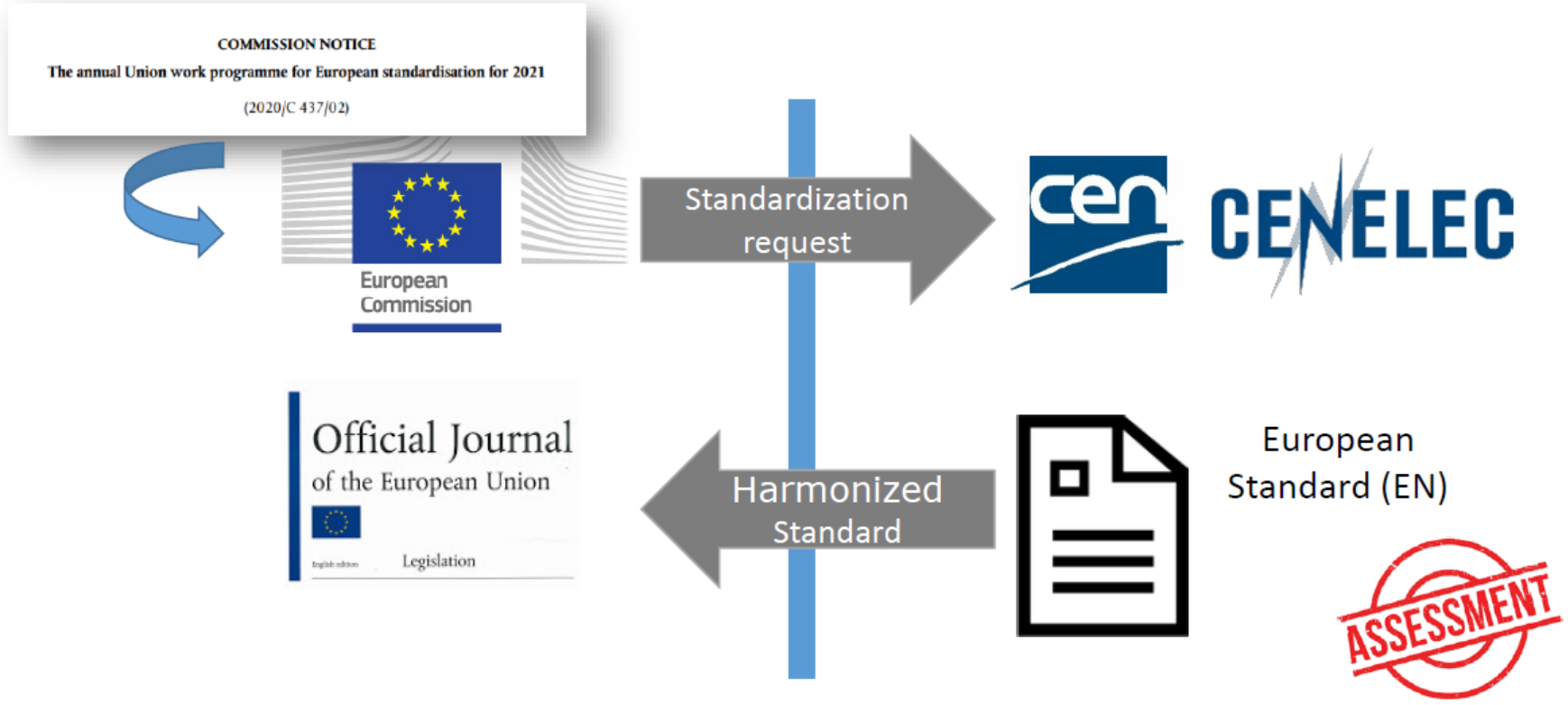
En harmoniseret standard er en europæisk standard (EN) som er blevet til på **baggrund af et "Standardisation Request"** udstedt af EU Kommissionen til anvendelse for at **understøtte harmoniseret EU-lovgivning** (Art. 2, Reg. 1025/2012).

EU's harmoniserede lovgivning for produkter (Ny Metode)



- Offentlig myndighed
- Obligatorisk
- **Definerer hvilke mål** der gælder
- Revideres ved politisk behov

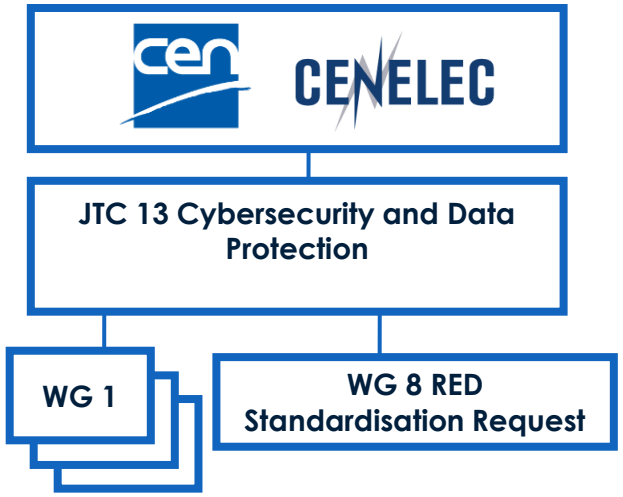
Processen for "Standardization Requests"



Standardization Request a **precondition** for citation of harmonized standards in OJEU

3 harmoniserede standarder undervejs

Standarderne udvikles i WG 8



EN XXXXX Common security requirements for internet connected radio equipment

The harmonised standard includes test methods or equivalent approaches and conditions to verify compliance of radio equipment with the essential requirement set out in Article 3(3), **point (d)** of Directive 2014/53/EU for the categories and classes specified by **Article 1(1)** of Delegated Regulation (EU) 2022/30.

EN XXXXX Common security requirements for radio equipment processing data, namely internet connected radio equipment, childcare radio equipment, toys radio equipment and wearable radio equipment

The harmonised standard includes test methods or equivalent approaches and conditions to verify compliance of the radio equipment with the essential requirement set out in Article 3(3), **point (e)** of Directive 2014/53/EU for the categories and classes specified by **Article 1(2)** of Delegated Regulation (EU) 2022/30.

EN XXXXX Common security requirements for internet connected radio equipment processing virtual money or monetary value

The harmonised standard includes test methods or equivalent approaches and conditions to verify compliance of the radio equipment with the essential requirement set out in Article 3(3), **point (f)** of Directive 2014/53/EU for the categories and classes specified by **Article 1(3)** of Delegated Regulation (EU) 2022/30.

Tidslinje

Februar 2021 - oktober 2021: 11 forberedende møder i "SRAHG" (Standardization Request Ad Hoc Group) i CEN/CENELEC ETSI regi. Vurdering af udkastet - forhandling - præcisering.

29. Oktober 2021: Kommissionen vedtager Delegated Regulation (EU) 2022/30

November 2021 - Juni 2022: 6 møder i SRAHG til yderligere afklaring

Juni 2022: ETSI ekskluderet

Juni/Juli 2022: Afstemning i "Standardiseringskomiteen (Cos)" (Erhvervsstyrelsen er DK's repræsentant her)

August 2022: Afstemning i CEN/CENELEC om accept af Standardisation Request (SR)

7. september 2022: SR Accepteret af CEN/CENELEC: Standardisation Request endeligt vedtaget

13. Oktober 2022: Deadline for formel afstemning om opstart i CEN/CENELEC JTC 13

Januar-Marts 2023: De tre standarder på offentlig høring i 2 måneder

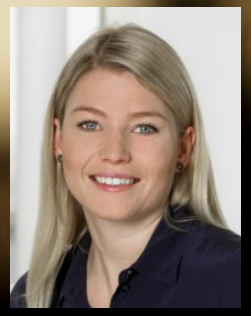
9. juni 2023: Standarderne skal ud til den sidste og endelige afstemning

1. oktober 2023: Deadline for CEN og CENELEC for levering af standarder

1. august 2024: Nye regler træder i kraft

WG 8 på arbejde

Tak



Astrid Bækby Knudsen
Standardiseringskonsulent
abk@ds.dk // 29 43 43 75

RED hEN requirements

Jeppe Pilgaard Bjerre

30.09.2022

DISCLAIMER

ALL CONTENT SUBJECT TO CHANGE

Applicable to: 3.3(d)

M/585 requirement

(a)
include elements to monitor and control network traffic, including the transmission of outgoing data;

(b)
are
designed to mitigate the effects of ongoing denial of service attacks;

hEN requirement

The radio equipment shall monitor on a risk base network traffic, which is sent or received by the device.

Applicable to: 3.3(d,e,f)

M/585 requirement

(c)
implement appropriate authentication and access control mechanisms;

hEN requirement

- The internet-connected RE shall have an authentication mechanism implemented to prevent unauthorized access of an entity via a local or remote network interface.
- The authentication mechanism shall only use a random per device or a user defined authentication value.
- The authentication mechanism shall use best practice cryptography for the identification and authentication of an entity.

Applicable to: 3.3(d,e,f)

M/585 requirement

(d)
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 network or its functioning or
misuse of network resources;

hEN requirement

- At the moment of placing on the market, the radio equipment shall not include any software or hardware that does contain publicly known vulnerabilities that, on a risk basis, could be exploited to harm the network *(similar requirements for privacy and financial)*

Applicable to: 3.3(d,e,f)

M/585 requirement

(e)
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 the radio equipment harming the network or its functioning or the misuse of network resources;

hEN requirement

- The radio equipment (RE) shall support the ability to be securely (using state of the art *cryptographic techniques*) upgraded, *whether in an automated or manual way*, as well as to disallow version downgrade.
- The radio equipment (RE) shall support the ability to be securely (using state of the art cryptography), and whenever possible, timely updated and upgraded as well as to disallow version downgrade.

Applicable to: 3.3(d,e,f)

M/585 requirement

(f)
protect the exposed attack surfaces and minimise the impact of successful attacks.

hEN requirement

All external communication interfaces that are not necessary for the intended use of the RE shall be disabled

Applicable to: 3.3(e,f)

M/585 requirement

(a)
protect stored, transmitted or otherwise processed personal data against accidental or unauthorised processing, including storage, access, disclosure, destruction, loss or alteration or lack ofavailability;

hEN requirement

The RE shall protect personal data and/or financial data (primary assets stored and processed on the device and transferred from the device outside) by appropriately using one or all of the following protection mechanisms

Applicable to: 3.3(e)

M/585 requirement

(e)
include functionalities to inform the user of changes that may affect data protection and privacy;

hEN requirement

- RE shall notify a user about changes related to data protection or privacy.
- If a change to the personal data processing requires consent or reconsent of a user, RE shall ask the user for an explicit permission.
- If a user wants to cancel notifications related to changes in data protection or privacy, RE shall display a warning.
- A user shall not be able to mute notifications related to consent or reconsent of a user.

Applicable to: 3.3(e,f)

M/585 requirement

(f)
log the internal activity that can have an impact on data protection and privacy;

hEN requirement

log the internal activity that can have an impact on data protection and privacy

Keep in touch

Jeppe Pilgaard Bjerre
Specialist
jpbj@force.dk
+4543251548
forcetechnology.com

Follow us on: