DIN FOCUS.ICT WS III – Cybersecurity Regulation in Europe

NLF and CSA

Considerations of the FOCUS.ICT working group on "Cyber security regulation in Europe"

Administrative Support of the group and contact partner:
Benjamin Helfritz | DIN, Deutsches Institut für Normung e.V. | benjamin.helfritz@din.de | +49 30 2601-2791

NLF and CSA - Two parallel approaches for regulation

NLF

CSA

Elements of a horizontal Cybersecurity NLF based Regulation (1/2)

FOCUS.ICT

Essential Requirements

- Only a horizontal regulation brings essential requirements that are mandatory for all market participants and represent legal obligations
- Degree of fulfillment according to the state of the art
- Mandatory requirements for products can only be made compulsory through a NLF regulation (according to Decision 768/2008).

Up-to-dateness State of the art

- Requirements in harmonized standards must reflect the state of the art
- Harmonized standards are regularly updated by the experts in the committees and the latest technologies are taken into account/included

Coverage of different risk levels

- Different conformity assessment modules of the NLF take into account the risks of the intended use of the products
- Use case “high-risk area”: the involvement of third parties (NB) can be made mandatory

Elements of a horizontal Cybersecurity NLF based Regulation (2/2)

High technical expertise and international connectivity	• Standards are developed by technical experts of all stakeholders in open and transparent processes. • The main bodies in which the experts are active are, for example: ISO / IEC JTC 1 SC 27; IEC TC 65 / WG10; CEN / CENELEC JTC 13; ETSI TC Cyber, DIN NIA 27, DIN NIA 41-1, DKE / UK 931.1
Innovation friendly	• NLF approach is technology open and promotes new, improved solutions • The example of “safety” shows the continuous improvement dynamics
Openness, transparency and predictability	• Simplification for the legislature from defining detailed requirements • Any expert can participate and contribute on standardization. • The progress of standardization is transparent for everyone, so that there is a high degree of planning reliability on all sides
Marktet surveillance	• Sovereign tasks for national authorities

Using certification schemes to demonstrate presumption of conformity

Horizontal Cybersecurity regulation under NLF

Essential requirements mandatory for all market participants

Standardisation request(s) to ESOs

> Development of harmonised standards
> Listing of harmonised standards in OJEU

Presumption of conformity

Assessment according to modules under NLF – all risk-levels are addressed (including mandatory certification)

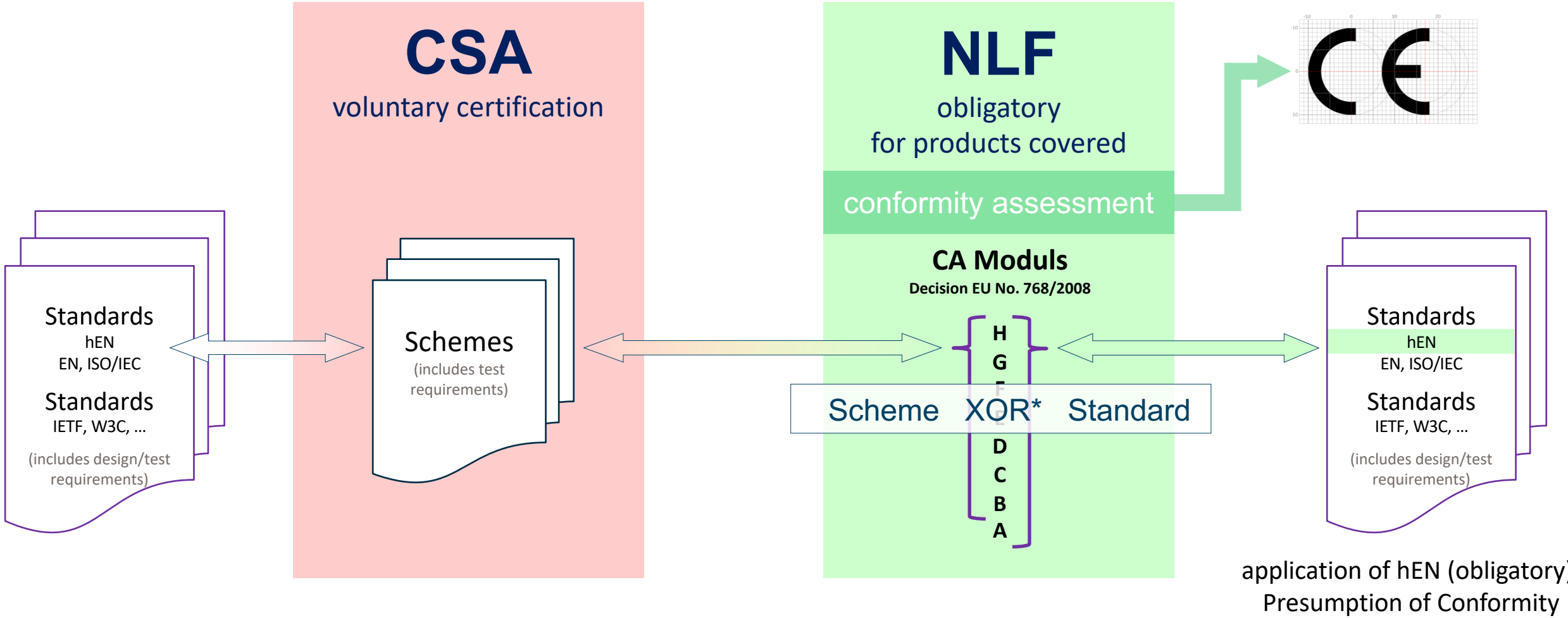
Use of standards is voluntary; alternative ways are allowed.

CSA, Art 54, Abs 3. “Where a specific Union legal act so provides, a certificate or an EU statement of conformity issued under a European cybersecurity certification scheme may be used to demonstrate the presumption of conformity with requirements of that legal act.”

Certification scheme may be used (voluntarily and alternatively) to demonstrate the presumption of conformity of that legal act.

CSA-NLF/CE Bridge

based on: CSA art. 54, par. 3



*XOR-Logic Freedom of choice for the manufacturer (only one - not twice):
The application of a CSA scheme as part of a conformity assessment procedure leads to compliance with the NLF legal act.

FOCUS.ICT

	2020	2021	2022	2023	202x
CSA		Schemes under the CSA are put into force	First experience with application of schemes available Voluntary certifications		Possibly further schemes under the CSA Conformity assessment (The application of a CSA scheme as part of a conformity assessment procedure leads to compliance with the NLF legal act)
NLF		Implementing measures under RED to include cybersecurity	Draft for horizontal cybersecurity regulation based on the NLF	Horizontal cybersecurity regulation adopted Transition period Standardization mandates to ESA´s	NLF regulation - requirements mandatory after transition period Harmonized standards available Presumption of conformity