TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

"TeleTrusT-Konferenz 2021"

Berlin, 25.11.2021

BSI-Zertifizierung – Aktuelle Entwicklungen

Sandro Amendola, BSI

Inhalt

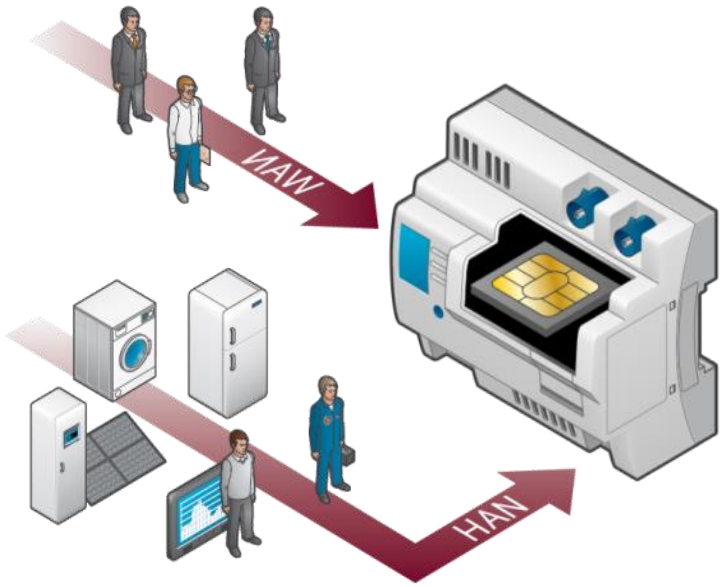
1. Bedeutung der Zertifizierung für die Cyber-Sicherheit
2. Zertifizierungsverfahren des BSI
3. Zertifizierung und Regulierung im CSA

1. Bedeutung der Zertifizierung für die Cyber-Sicherheit

Bedeutung der Zertifizierung für die Cyber-Sicherheit

- **Präventive IT-Sicherheitsmaßnahme**
  - Sicherheit für neue Produkte vor Markteintritt
  - „Security-by-Design“
  - Zertifizierung als Teil des Innovations- und Entwicklungsprozesses
- **Transparente Sicherheitseigenschaften** durch veröffentlichte Kriterien, Standards und Prüfergebnisse
- **Unabhängig** von Geschäftsinteressen der Hersteller
- **Instrument der Regulierung** zur Durchsetzung von Sicherheitsstandards

➢ **Vertrauenswürdige IT**



Herausforderungen im Bereich der Zertifizierung

>> kurze Releasezyklen

Agile Produktentwicklung

>> DevOps >> ToolChains

>> Cloudprodukte

Systembetrachtung

>> Einbettung von Produkten in Systeme

>> ISMS

>> White-Box-Kryptographie

Kryptografie

>> Quantenkryptografie

>> Post-Quantum

>> Verteilte Entwicklungsteams

Verteilte Entwicklungsstandorte

>> Komplexität durch Vernetzung

>> Verantwortlichkeiten

>> Verteilte Systeme

Komplexität

>> Abgrenzung der Sicherheitsfunktionalität

>> Integritätsschutz

Lieferketten

>> Abhängigkeiten von Zulieferern

>> Erhaltung des Zertifikats

Patchmanagement

>> Re-Zertifizierung notwendig?

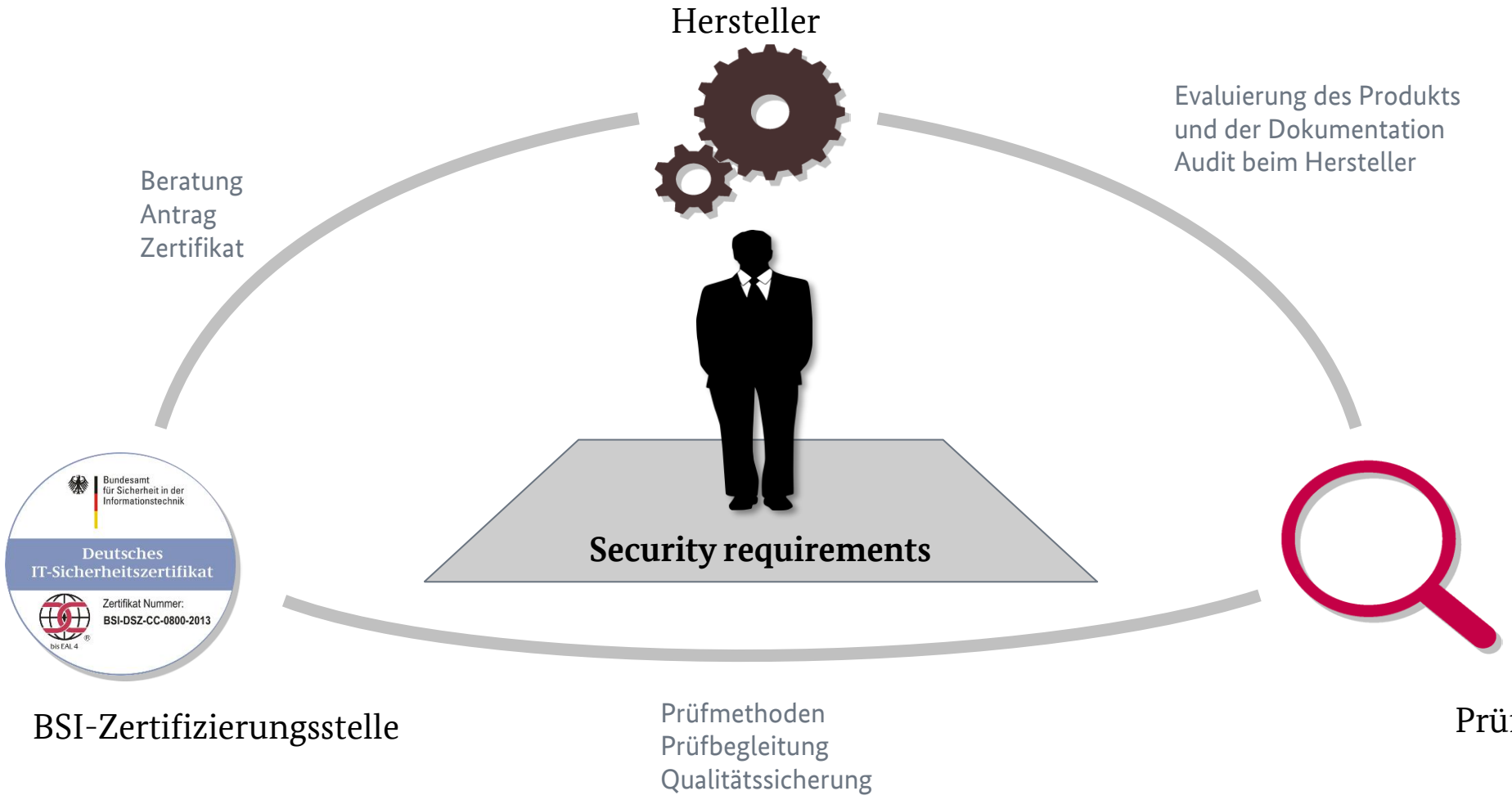
>> Laufzeit von Evaluierungen

Time-to-Market

>> Herstelleraufwände/Kosten

2. Zertifizierungsverfahren des BSI

Zertifizierungsprozess

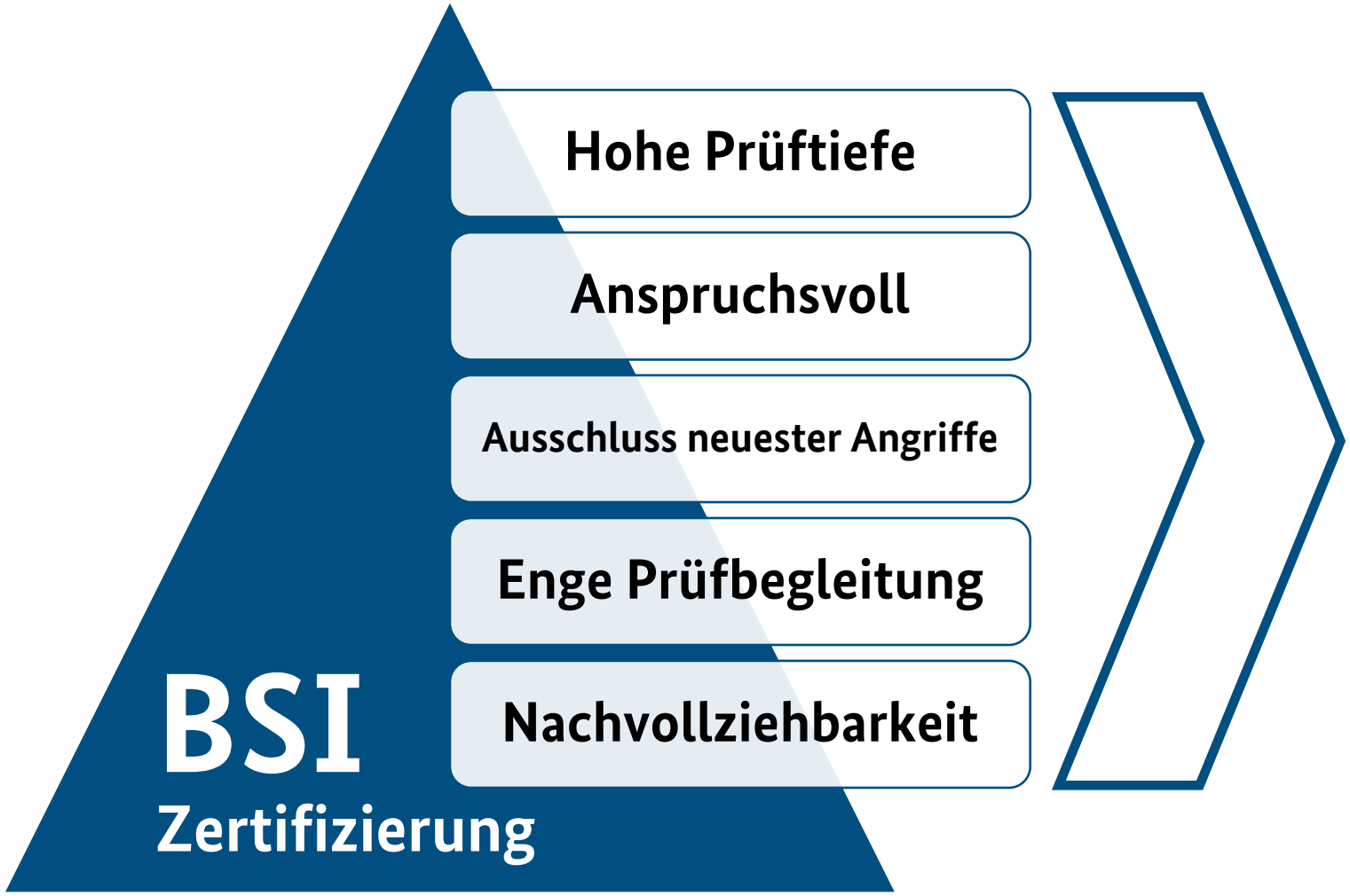


Antrag

Evaluation

Zertifizierung

Positionierung des BSI in Common Criteria



BSI als TOP-Adresse für CC-Zertifizierung weltweit!

Steigerung der Zahl an erfolgreichen Zertifzierungen

Leitbild des BSI als Zertifizierungsstelle

Das BSI-Zertifizierungsteam bietet eine serviceorientierte Zertifizierung und orientiert sich an den folgenden Leitlinien und Prämissen:

- Digitalisierung sicher gestalten!
- Unabhängigkeit gewährleisten!
- Vergleichbarkeit sicherstellen!
- Stakeholder managen!
- Stand der Technik berücksichtigen!
- Transparent und verlässlich agieren!
- Zusammenarbeit fördern!
- Effiziente Prozesse gestalten!

Aktuelle Weiterentwicklung des CC-Prüfprozesses im BSI

1. Prüfung der Prüf- und Dokumentationspflichten für CC-Verfahren für Hersteller und Prüfstellen
2. Ausarbeiten eines Workshop-Konzepts
3. AIS-Update
4. Vollständige Digitalisierung des Zertifizierungsprozesses
5. Neues „Zertifizierer-Mindset“ durch intensive Gespräche und Diskussionen
6. Verlässliche Testplanung, verlässliche Kommentierung
7. Austausch mit Herstellern und Prüfstellen
8. Verbesserung der internen Zusammenarbeit
9. Verbesserung des Projektmanagements/ Controllings in der Zertifizierung
10. Kompetenzsteigerung durch dedizierte Schulungen zur PP-Entwicklung und Krypto-Bewertung

Beschleunigte Sicherheitszertifizierung (BSZ)

Risikogetriebener Ansatz mit Schwerpunkt auf Penetrationstests

Festgelegte Verfahrensdauer ermöglicht eine belastbare Zeit- und Kostenplanung

Reduzierter Dokumentenumfang verringert den Aufwand für den Hersteller

Gegenseitige Anerkennung mit CSPN in Frankreich geplant

Internationale Standardisierung (prEN 17640)

Unterschiede zwischen CC und BSZ

Vertrauenswürdigkeitsstufe

- EAL 1 bis EAL 7

Widerstand Angriffsstärke

- AVA_VAN 1 bis AVA_VAN 5

Evaluierung

- Ca. 80% Design-, Codeanalyse, Testen
- Ca. 20% Penetrationstests

Aufwand

- Abhängig von Vertrauenswürdigkeitsstufe/Angriffsstärke
- Dauer ca. 12-24 Monate
- Kosten (extern) von 100 PT bis über 1000 PT

Vertrauenswürdigkeitsstufe

- Keine Stufe definiert

Widerstand Angriffsstärke

- Vergleich CC: AVA_VAN 1 bis AVA_VAN 3

Evaluierung

- 10% Vorgabenprüfung
- 90% Penetrationstests

Aufwand

- Fixiert, anpassbar an Komplexität des Produkts
- Dauer ca. 3 - 6 Monate
- Kosten (extern) 60 bis 80 PT (geschätzt)

Network Equipment Security Assurance Scheme (NESAS)

Umsetzung zunächst als nationales Zertifizierungsschema **NESAS Cybersecurity Certification Scheme – German Implementation** (NESAS CCS-GI)

- weitgehend kompatibel zum GSMA NESAS
- derzeit in der Pilotierung
- Produktivsetzung im 2. Quartal 2022 geplant
- Schnittstellentest und Audit des Lebenszyklus

Harmonisierung und Weiterentwicklung der vorhandenen Ergebnisse zu einem **Candidate EU 5G Cybersecurity Certification Scheme**

- ENISA ad hoc working group AHWG wird derzeit konstituiert
- BSI entsendet Vertreter als Observer

IT-Sicherheitskennzeichen

- Verfahren für den **Low-Assurance-Bereich**
- **Herstellererklärung** nach anerkannten Standards
- Vorgehensweise etabliert analog zum CE-Kennzeichen
- Etablierung im deutschen Markt inkl. einer **Marktaufsicht**
- **Router** und **E-Mail-Dienste**, **IoT** wird in 2022 folgen

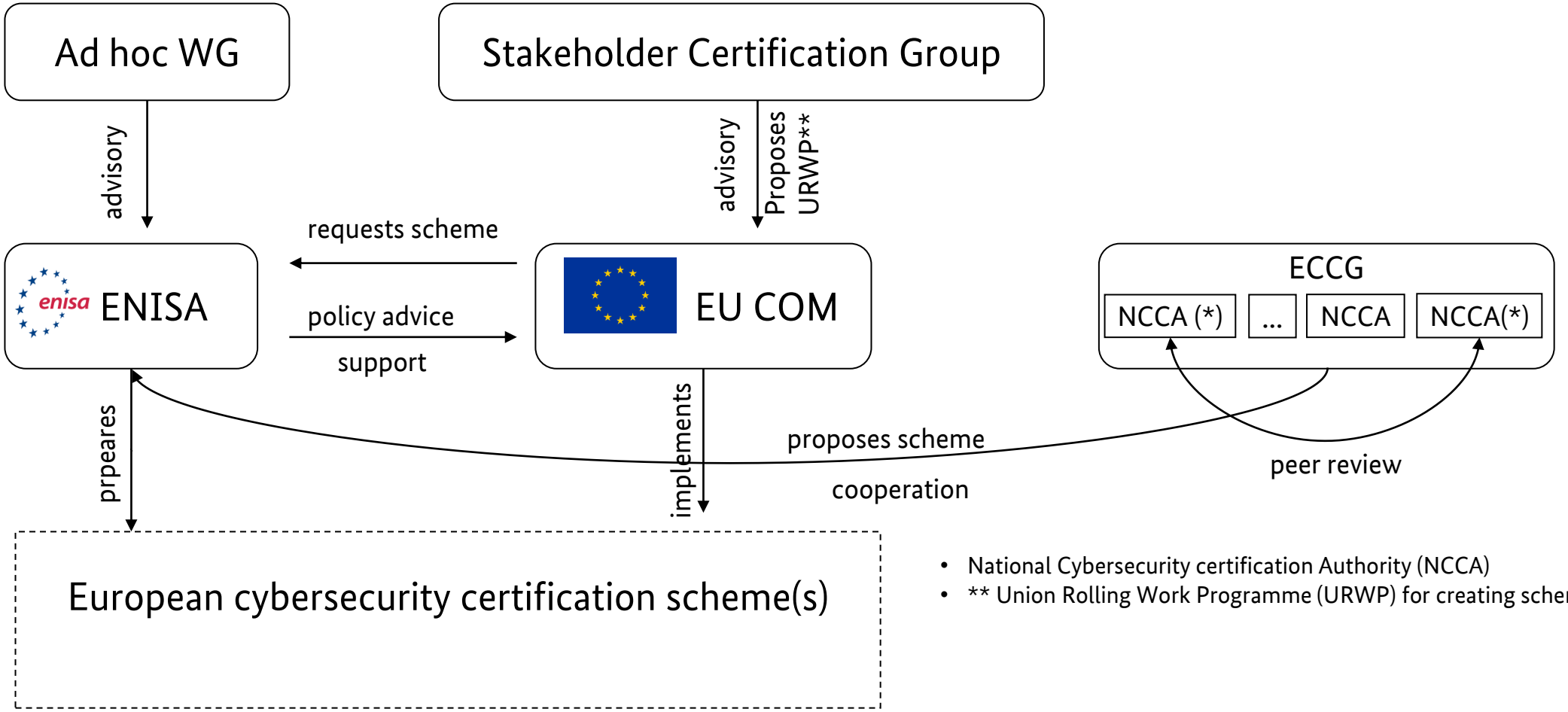
3. Zertifizierung und Regulierung unter dem CSA

Cybersecurity Act (CSA)

- **Zertifizierung**
  - **Niedrig** (Basic): **Akkreditierte CAB** oder **Konformitätsselbstbewertung**
  - **Mittel** (Substantial): **Akkreditierte CAB** oder in begründeten Fällen durch staatliche Stelle
  - **Hoch** (High): **Zertifizierung durch staatliche Stelle** oder private CAB in deren Auftrag

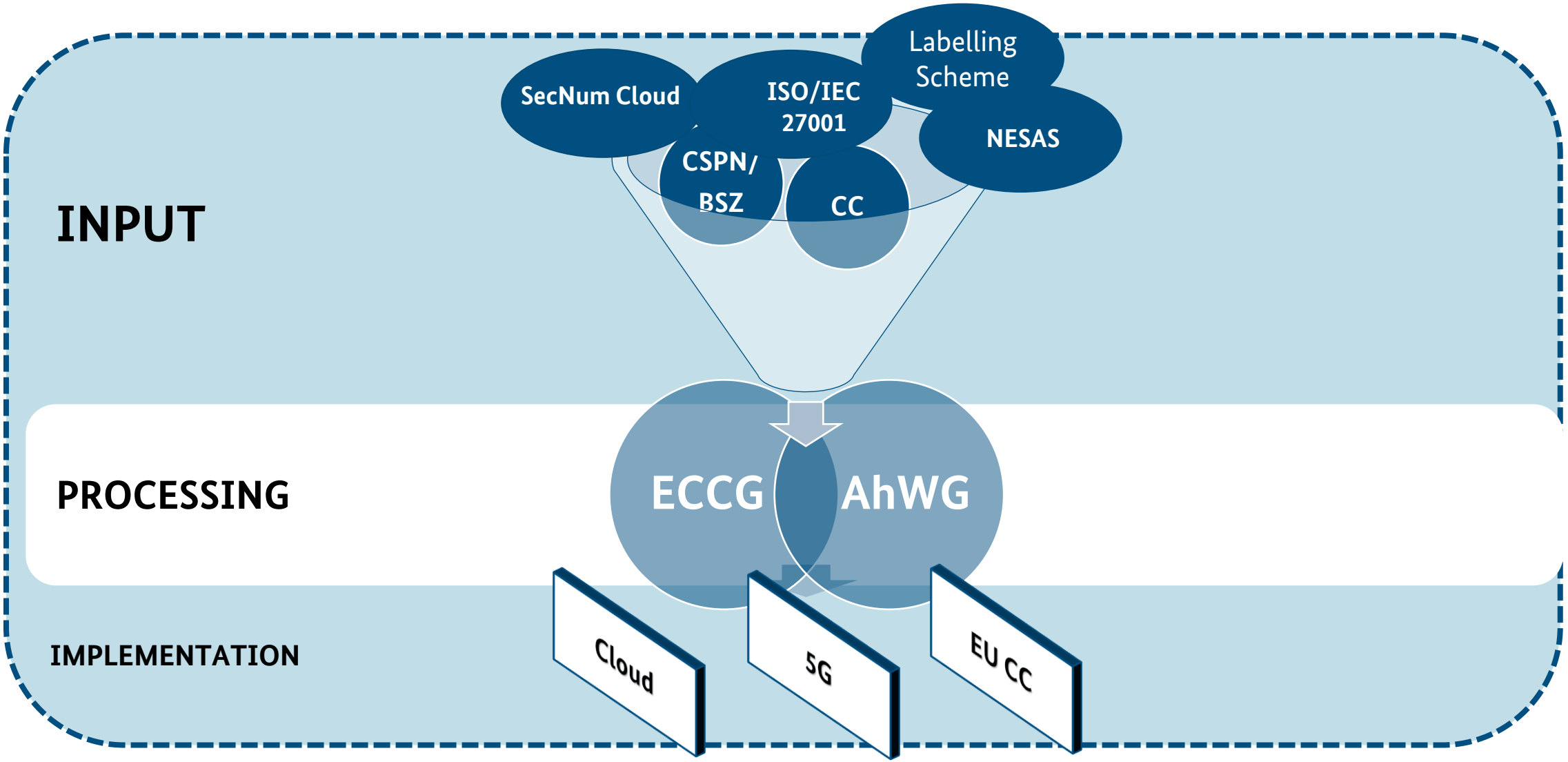
- Zertifikate sind **in allen EU-MS gültig**
- **Zertifizierung ist freiwillig**, so sie nicht durch andere nationale oder europäische Vorgaben verpflichtend gemacht wird

Cybersecurity Act (CSA)



- National Cybersecurity certification Authority (NCCA)
- ** Union Rolling Work Programme (URWP) for creating schemes

Cybersecurity Act (CSA)



Verbindliche Regulierung: Radio Equipment Directive (RED)

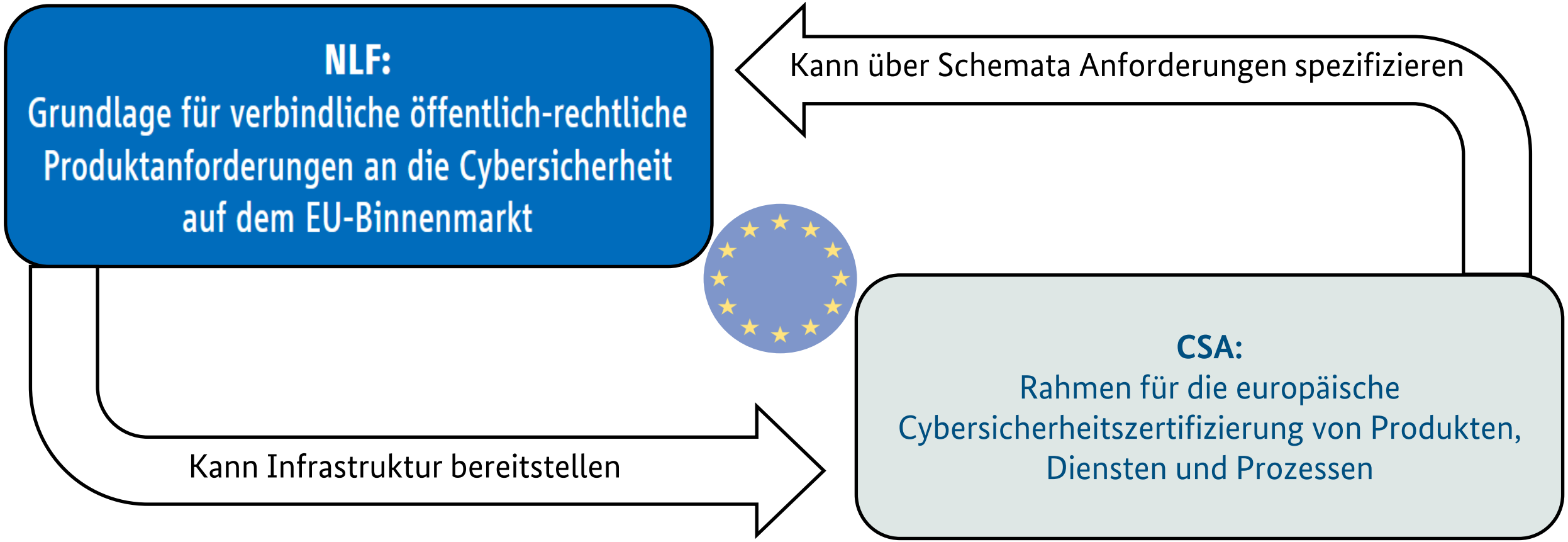
Implementierung

- Horizontale Regulierung für „funkende Geräte“ im etablierten New Legal Framework als Delegated Act
- Schutzziele „Protection of personal data and privacy“ und „Protection from fraud“
- Marktaufsicht bei BNetzA in Deutschland

Wirkung

- Die Konformitätserklärung basiert auf **Eigenversicherungen** der Hersteller
- Konformitätsbewertungsstellen **können** Anforderungen bestätigen, **müssen** dies tun, bevor es harmonisierte Standards gibt
- Nationale Regulierungen bei Produkten mit Funk-Schnittstelle im Verbrauchermarkt mit **RED unzulässig**

CSA und New Legislative Framework (NLF) im Kontext einer horizontalen europäischen Regulierung



Vielen Dank
für Ihre Aufmerksamkeit!

Kontakt

Hr. Sandro Amendola
Abteilungsleiter Abteilung SZ - Standardisierung, Zertifizierung und Sicherheit von Telekommunikationsnetzen

Abteilung-sz@bsi.bund.de
Tel. +49 (0) 228 9582 4182

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185-189
53175 Bonn
www.bsi.bund.de
www.bsi-fuer-buerger.de