Security Conference 2022

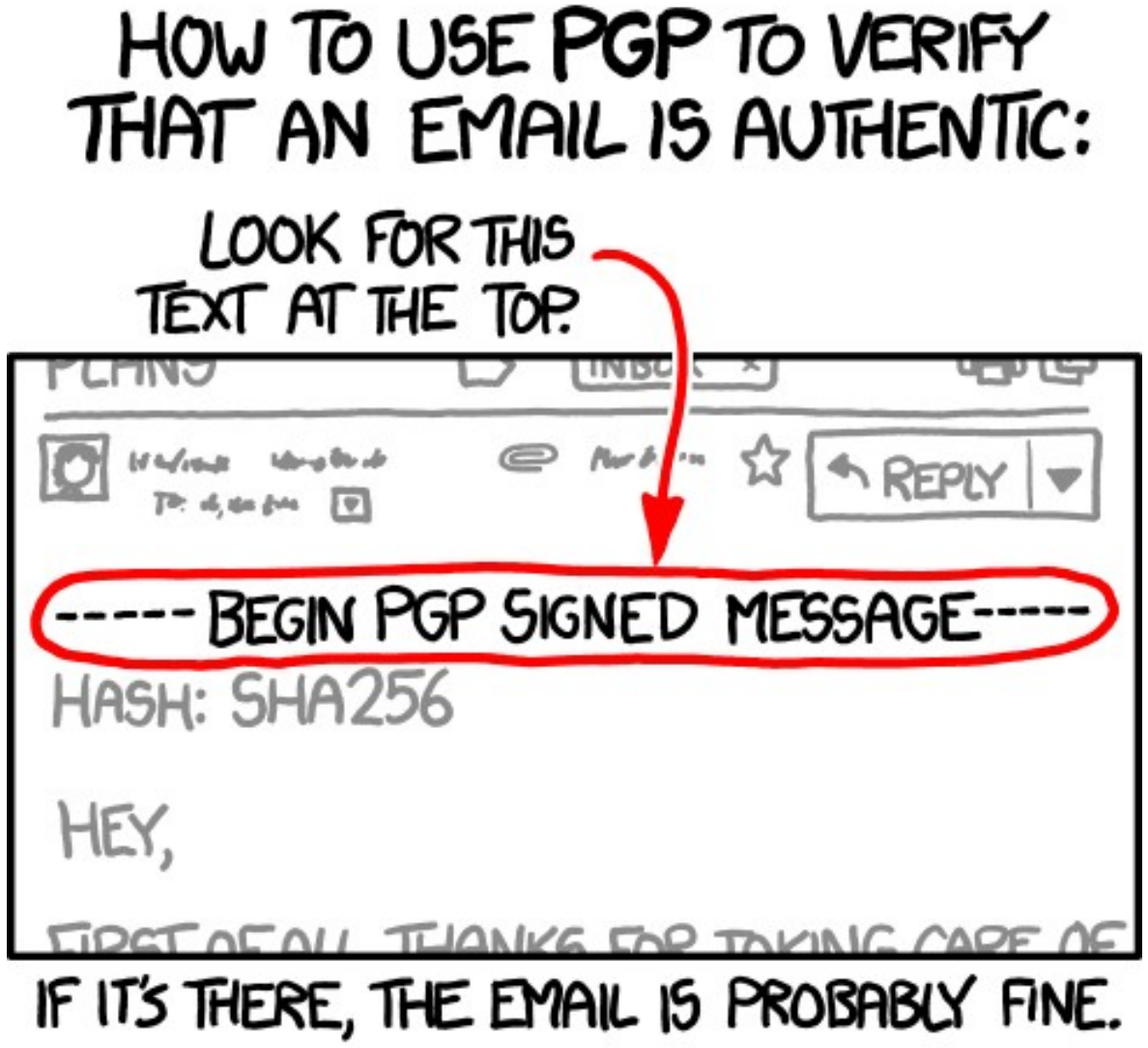
Cyber Security: Legislation & Standards

Dennis Kügler, BSI

03/10/2022

Risk-based Cybersecurity

Source:
https://xkcd.com/1181/



If you want to be extra safe, check that there's a big block of jumbled characters at the bottom.

State of the Art in Cyber Security

Act on the Federal Office for Information Security BSIG §3(1) Nr. 20:
Description and publication of a **state of the art in security requirements** for IT products, taking into account **existing norms and standards** and involving the trade associations concerned.

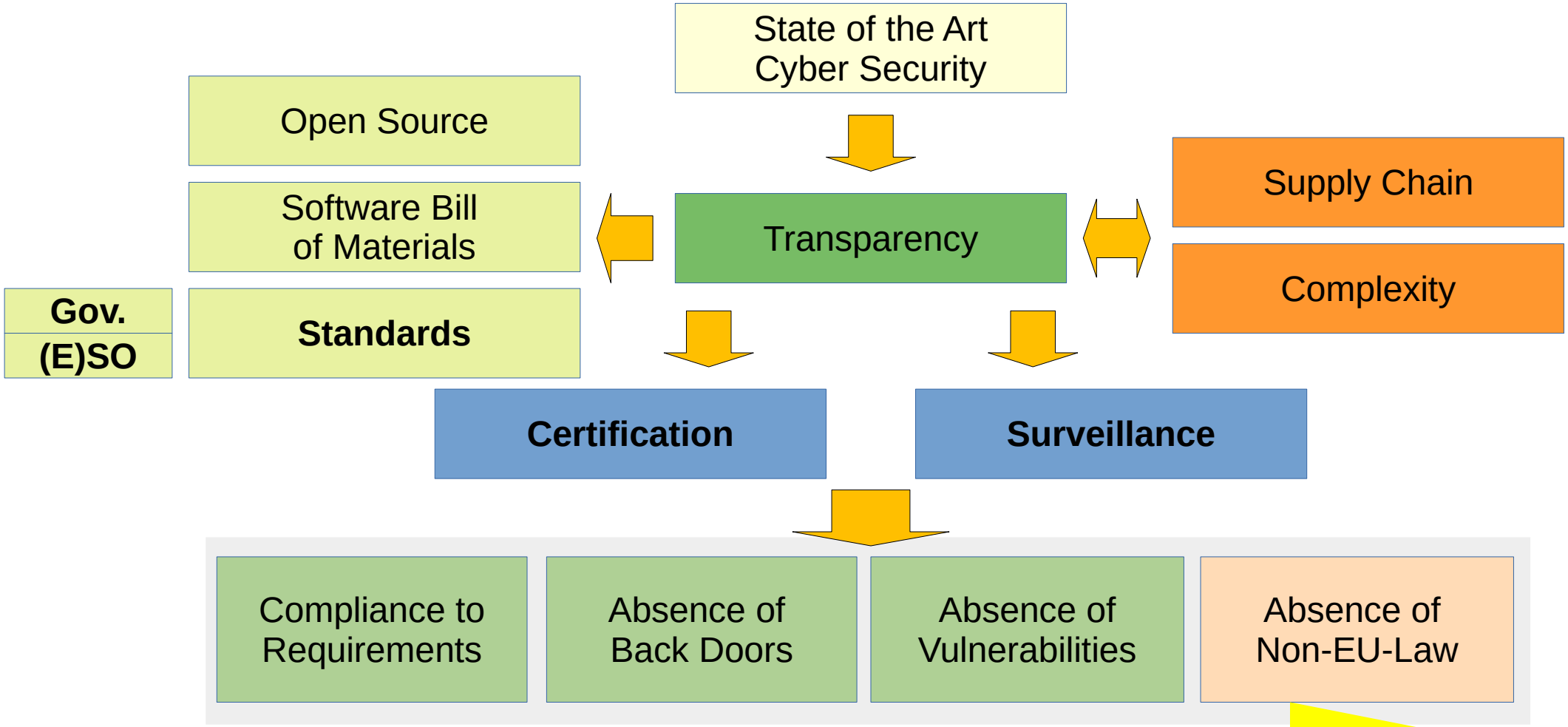
Compliance with state of the art security requirements

- Compliance is voluntary in general, **unless**
- Compliance **required** in specific regulated areas.
  - Passports and Identity cards, Smart Metering, Cash Registers…
- **Certification to demonstrate compliance**

Beschreibung und Veröffentlichung eines Stands der Technik bei sicherheitstechnischen Anforderungen an IT-Produkte unter Berücksichtigung bestehender Normen und Standards sowie Einbeziehung der betroffenen Wirtschaftsverbände.

Determination of the acceptable remaining risk

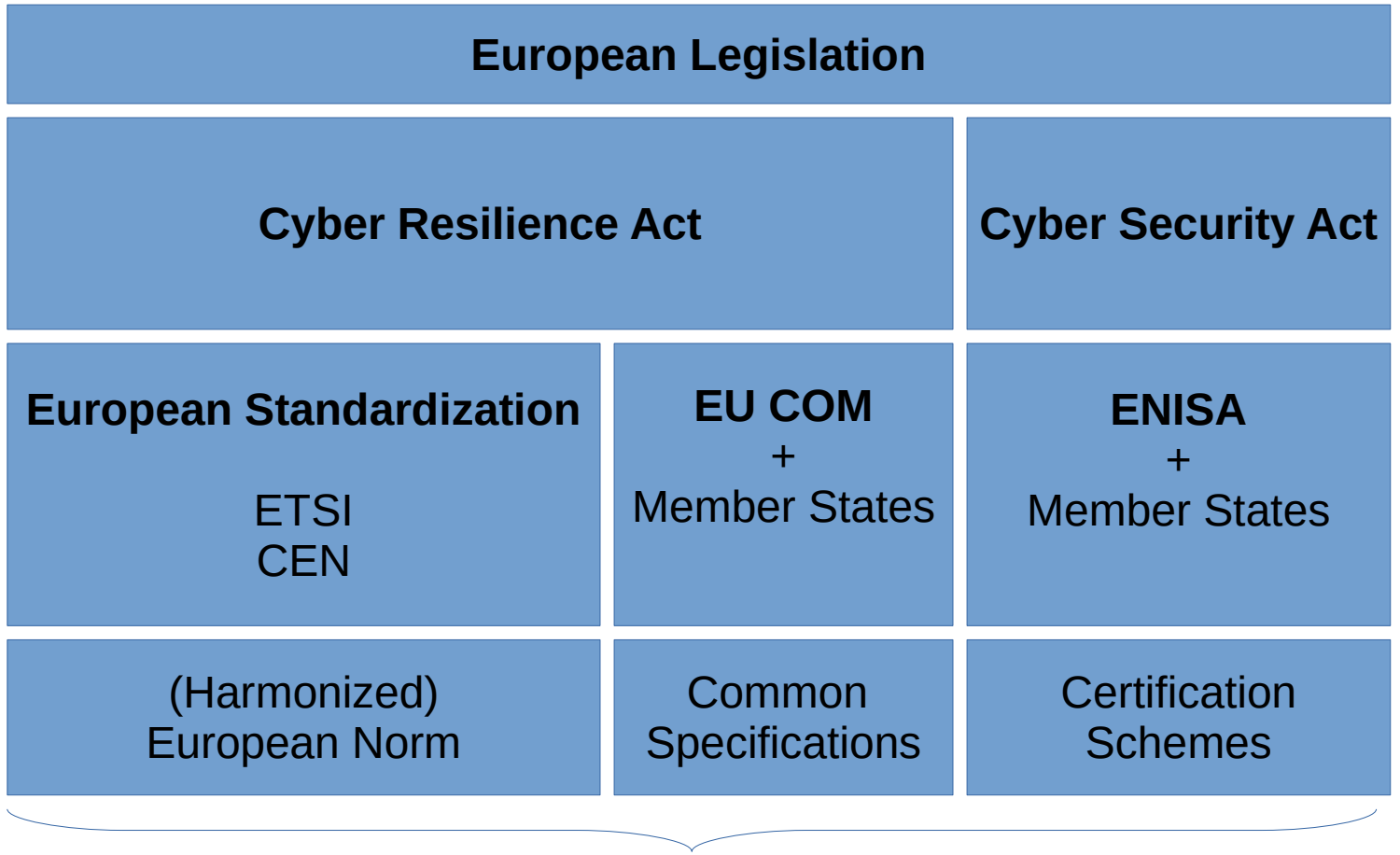
What Contributes to Cyber Security?



State of the Art in Cyber Security at the European Level

Harmonization of Essential Requirements (Cyber Security)

...and their implementation



Harmonization of (national) Certification Schemes

EUCC

EUCS
BSI C5
SecNumCloud

EU5G

ETSI IoT

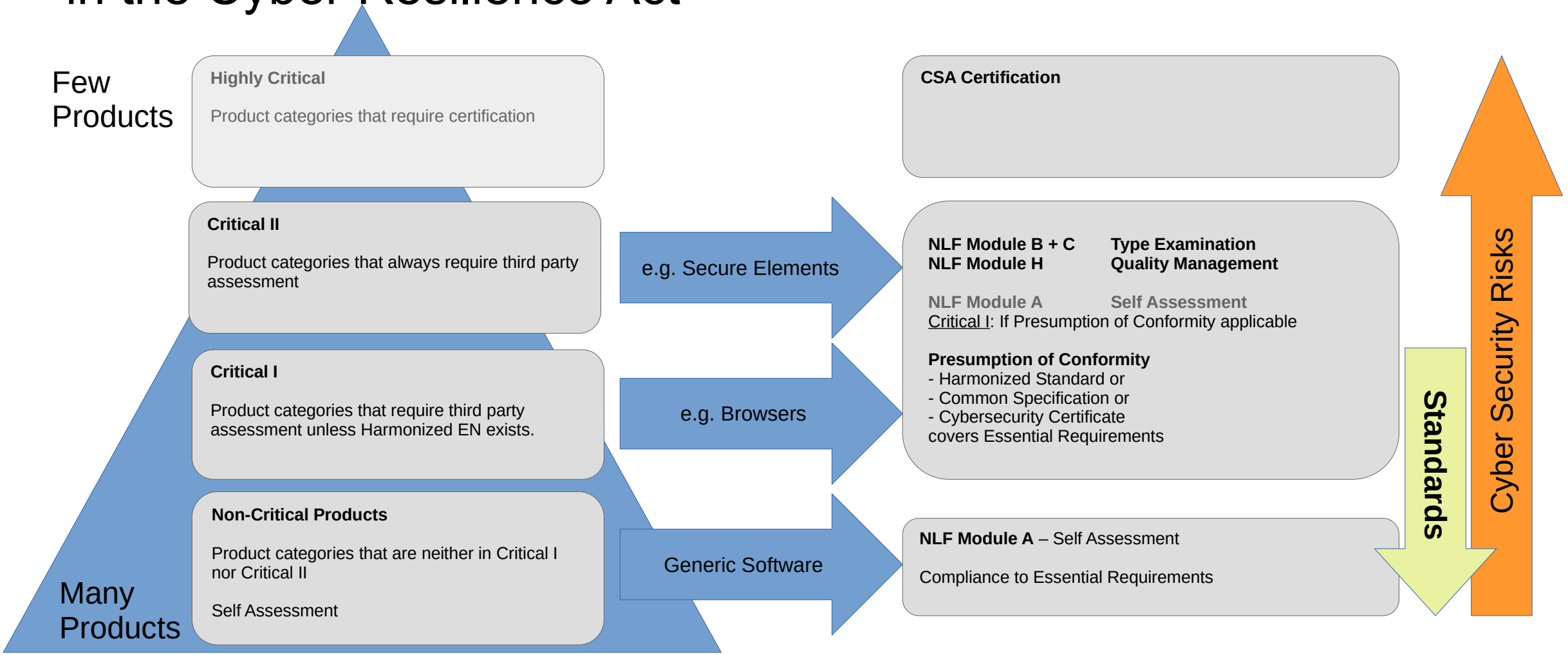
BSI BSZ
ANSSI CSPN
CEN FITCEM

....

Presumption of Conformity
=
State of the Art

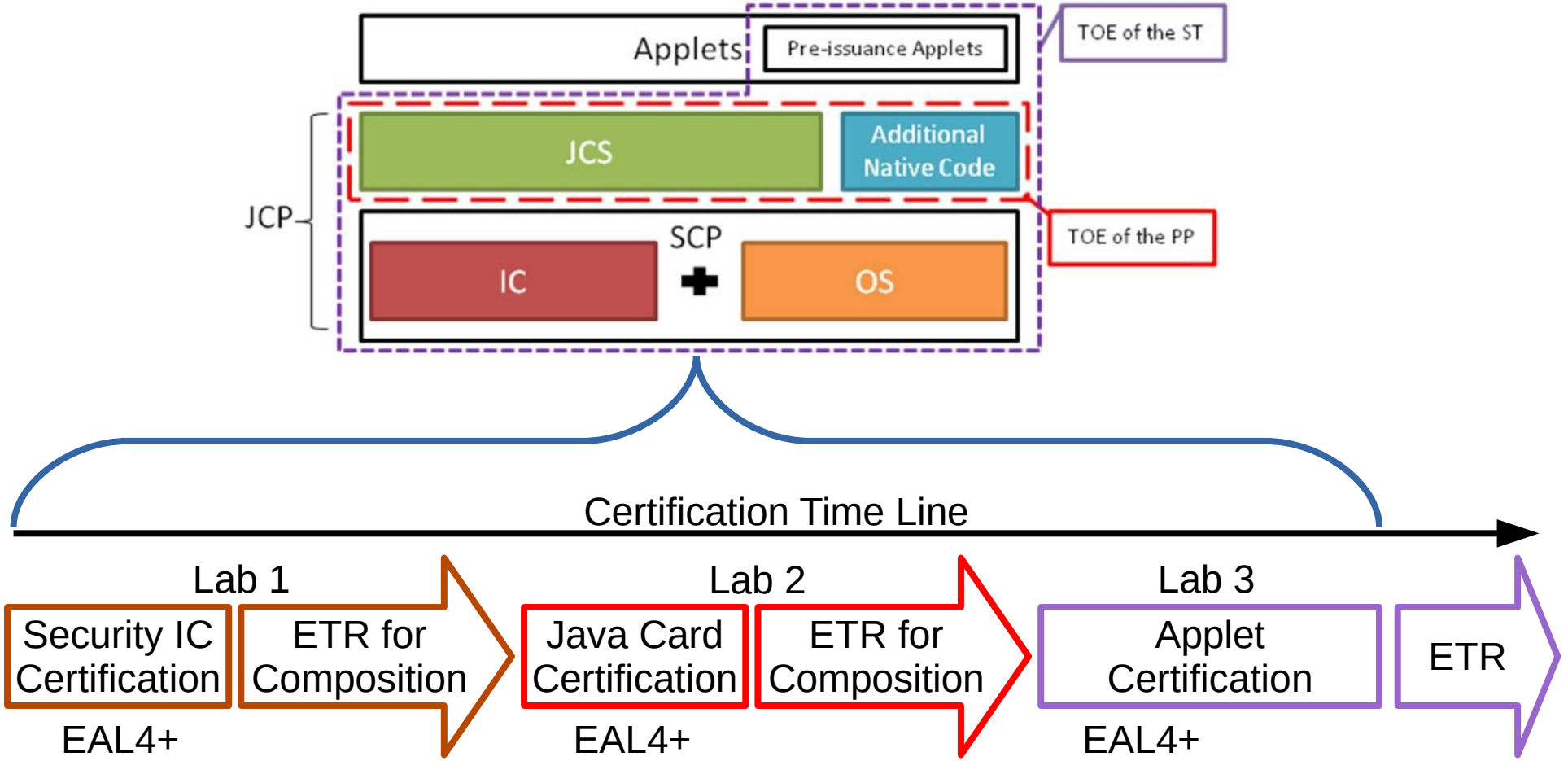
Bundesamt
für Sicherheit in der
Informationstechnik

The Role of Certification and Standards in the Cyber Resilience Act



Federal Office for Information Security

Example: Secure Element Certification



Demand for Standardization

State of the Art:

- Unstructured development process

- Sequential certification of components
- Consistent certification scheme and Level
- Limited reuse of certification results

Goals:

- **Secure Development Process**
  - Certify process not product

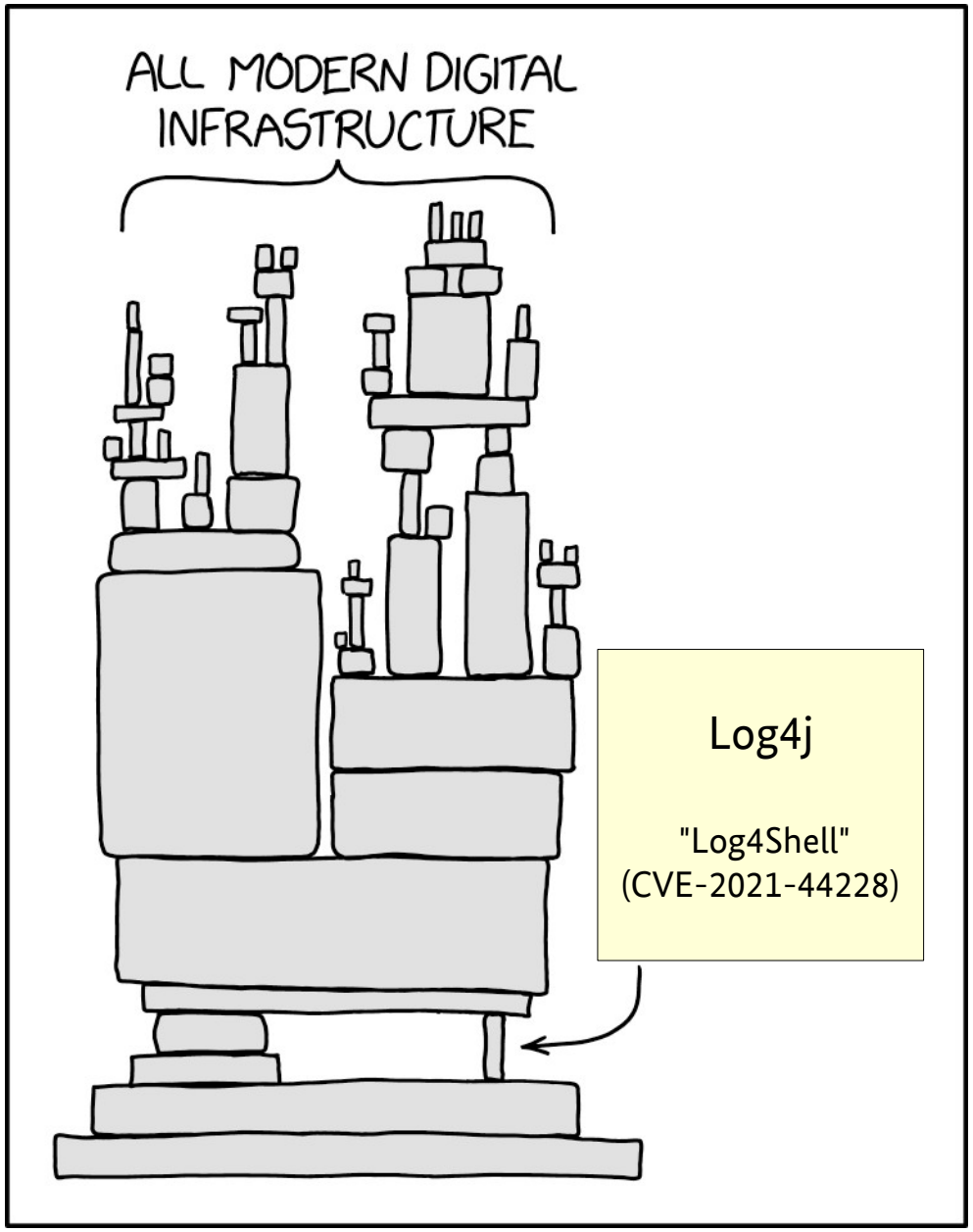
- **Standardization of interfaces**
  - Parallelize certification of modules
  - Use adequate certification schemes
  - Reuse certified modules

A (FiTCEM) certified Applet should run on any (EUCC) certified Java Card without loosing the certification!

Surveillance

- Certification does not prevent vulnerabilities
  - Vulnerability disclosure
  - Update requirements

- **Automated monitoring of vulnerabilities and tracking dependencies**
  - Publication of affected products
  - Security State
  - Mitigation of threats



Source: https://xkcd.com/2347/

Demand for Standardization

NOT State of the Art:

- **Software Bill of Materials (SBoM)**
- **Common Security Advisory Framework (CSAF)**

Goals:

- **Standards for description of products**
  - Software, Firmware, Hardware
  - Associated Services
  - Supply Chains
- **Standards for Vulnerability Management**
  - ...

Thank you
for your attention!

Contact

Dr. Dennis Kügler
Head of Branch Standardization, Certification Policy, Supervision
dennis.kuegler@bsi.bund.de
Tel. +49 (0) 228 99 9582 5183
Fax +49 (0) 228 99 109582 5183

Federal Office for Information Security
Branch SZ1
Godesberger Allee 185-189
53175 Bonn
www.bsi.bund.de

Federal Office
for Information Security