EU CYBERSECURITY ACT

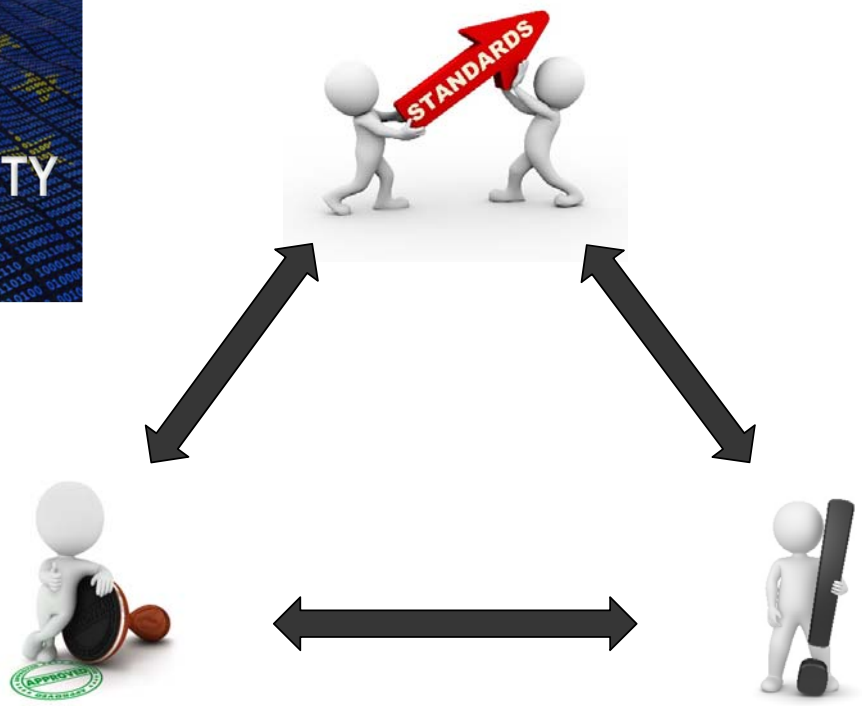
Martin Schaffer

Global Head of Secure Products & Systems

ETSI Security Week – Version 1 – 2019-06-18

SGS DIGITAL TRUST SERVICES

PROTECTING CITIZEN WITHOUT ENFORCEMENT?



- Mature manufacturers will use voluntary certification
- Immature stakeholders will most probably not use certification
- How to handle cheaters in the supply chain without enforcements?

CONFORMITY ASSESSMENT – A NEW CHALLENGE

- Definition according to EN ISO/IEC 17000:2004:
  - *“Demonstration that specified requirements relating to a product, process, system, person or body are fulfilled”*

- Traditional setup
  - Criteria are usually static: physical laws do not change
  - Check-list approach

- Cybersecurity setup
  - Criteria are dynamic: Attacks are moving
  - Check-list approach („security functional compliance“) vs. asset-based vulnerability assessment approach („security robustness“)

3 THINGS ARE KEY WHEN LOOKING AT STANDARDS

- Standardized Security Criteria (the „What“)
  - Security Functional Compliance (Checklists/Automation)
  - Security Robustness (Semiautomation/Ethical Hacking)
  - Focus at building blocks and make composition easy

- Standardized Way of Handling Attacks (the „Expert Groups“)
  - State-of-the-art attack monitoring
  - Attack rating
  - Consistency across sectors, use cases and technologies

- Standardized Certification Methodology (the „How“)
  - Product, process & service certification
  - Composition models
  - Flexibility, Efficiency, Time-to-Market

WWW.SGS.COM

WHEN YOU NEED TO BE SURE