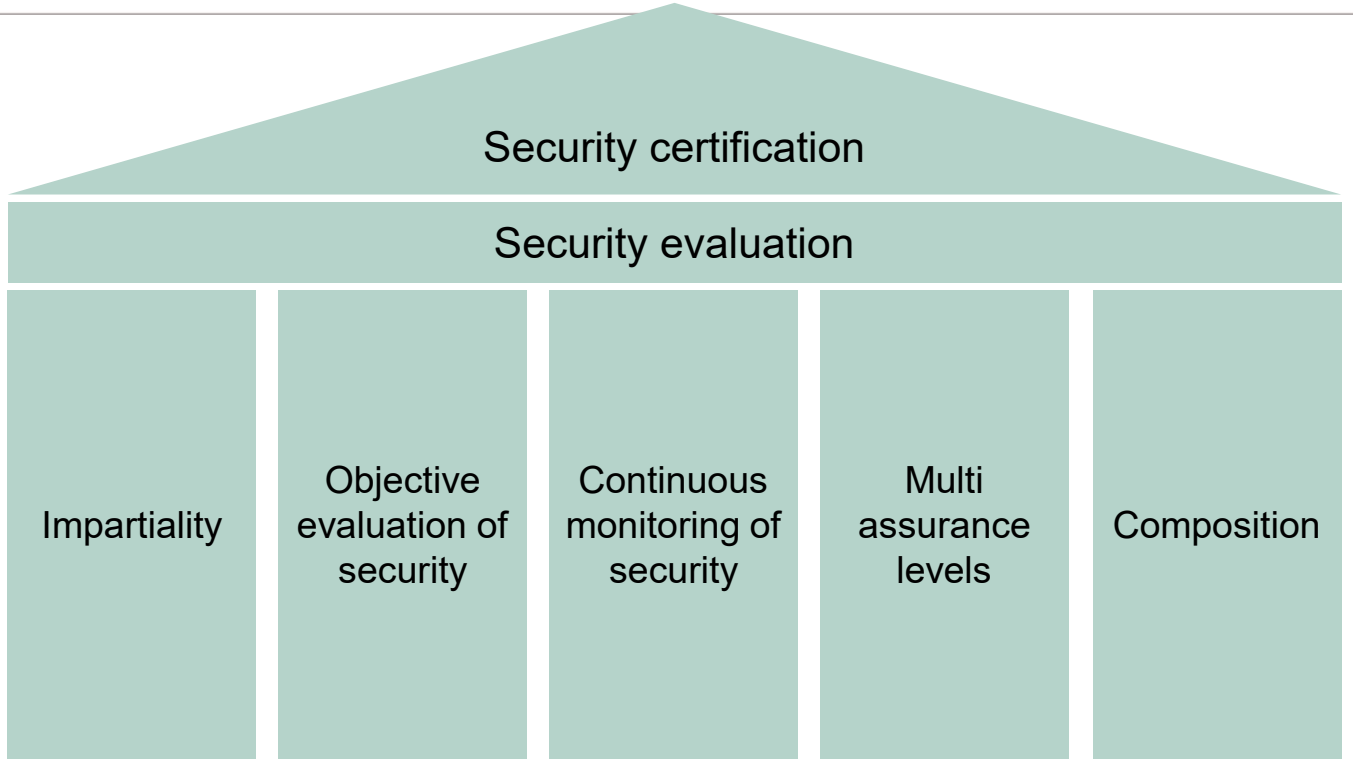
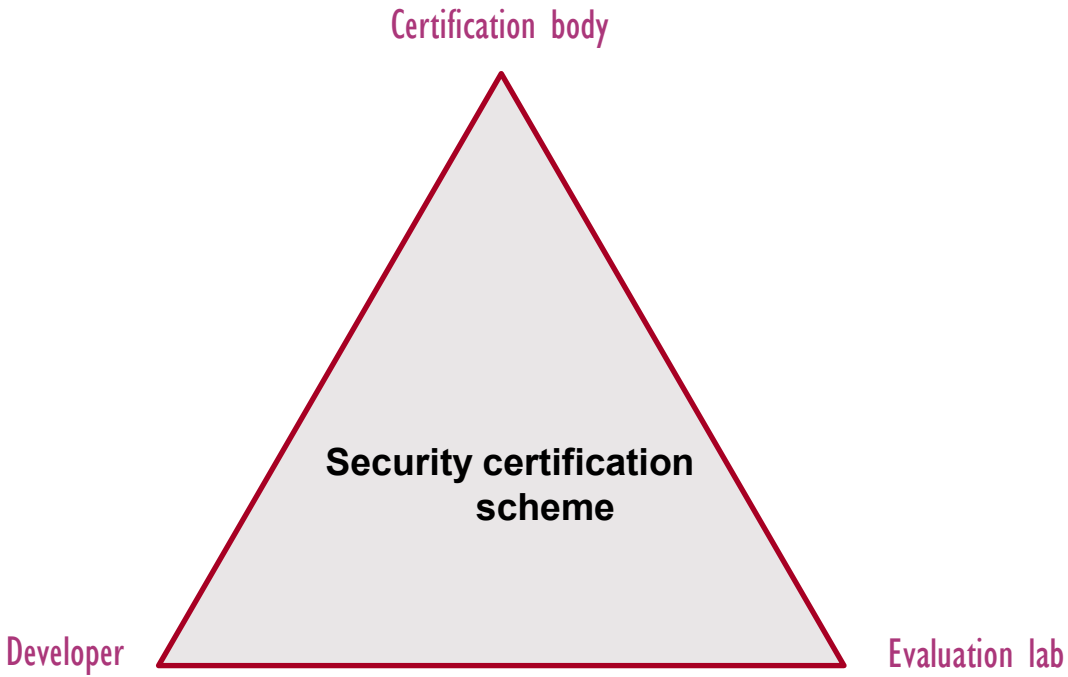
Security certification for trusted chips

Mariela Pavlova
Infineon Technologies

The role of security certification is to build confidence in the security of a product



Impartiality



Objective evaluation of the security

Common understanding on how a security evaluation shall be performed

- Common evaluation methodology for products and processes
- Common attack catalogue
- Common attack ratings
- Etc.

Continuous monitoring and surveillance of certified products

To address the problem of

- Threats evolving and product security erosion over time

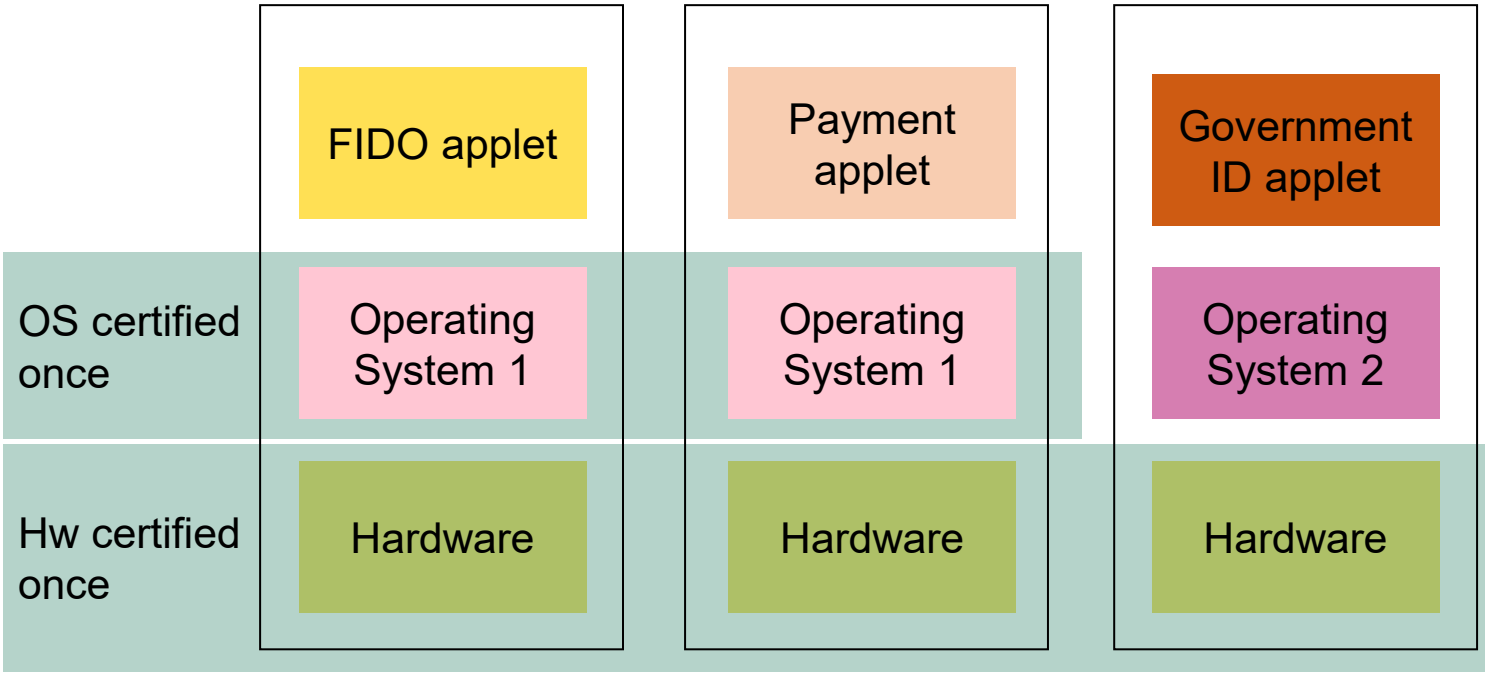
there is a need for a

- Regular reassessment/recertification of product security
- Surveillance of the security of certified products

Multiassurance levels

- Different levels of security assurance commensurate with the security strength claimed by the product.
- The more sophisticated the attacks in scope of the evaluation and certification the higher the assurance level.

Composition



Security evaluation standards for chips

Evaluation Methods	Region	Standardisation	Note
Common Criteria(CC)	Worldwide	ISO 15408	Used for the evaluation of smart cards and similar devices in Europe
SESIP	Worldwide	Currently in standardization at CENELEC JTC 13 WG3	Targets IOT platforms. Provides an efficient composition approach
FITCEM	EU driven	EU standard EN 17640	Focuses on fixed time evaluation processes

Chip security certification schemes also already exist

Schemes	Geographic region	Multiassurance levels	Evaluation method	Continuous monitoring	Composition	Third party independent assessment	JIL attack rating	Note
SOGIS	EU	Yes	CC	Yes	Yes	Yes	Yes	To be superseded by EUCC, see below. EU governments driven. Used for government procurement. Mainly used for smart card certifications.
EUCC	EU	Yes	CC	Yes	Yes	Yes	Yes	EU driven developed under the Cyber Security Act(CSA). Covers CSA high and substantial assurance levels and so targets to show resistance of products to high end attacks. Inherits from SOGIS
EMVCo	Worldwide	No	proprietary	Yes	Yes	Yes	Yes	Payment industry driven. Targets to show resistance of products to very sophisticated attacks
PSA Certified	Worldwide	Yes	SESIP	Yes	Yes	Yes	Yes	Industry driven. Targets the certification of the ROT of MCUs used in the IOT domain. Covers CSA low and substantial assurance levels. Shows resistance of products to basic/enhanced basic attacks. Required by Amazon for Alexa enabled devices
GP SESIP	Worldwide	Yes	SESIP	Yes	Yes	Yes	Yes	Industry driven. Targets the certification of MCUs used in IOT. Similar to PSA in terms of assurance levels and targeted attack resistance of products.

Part of your life. Part of tomorrow.