Security certification standards for trusted and secure chips in support of the Chip Act

Mariela Pavlova
Infineon Technologies

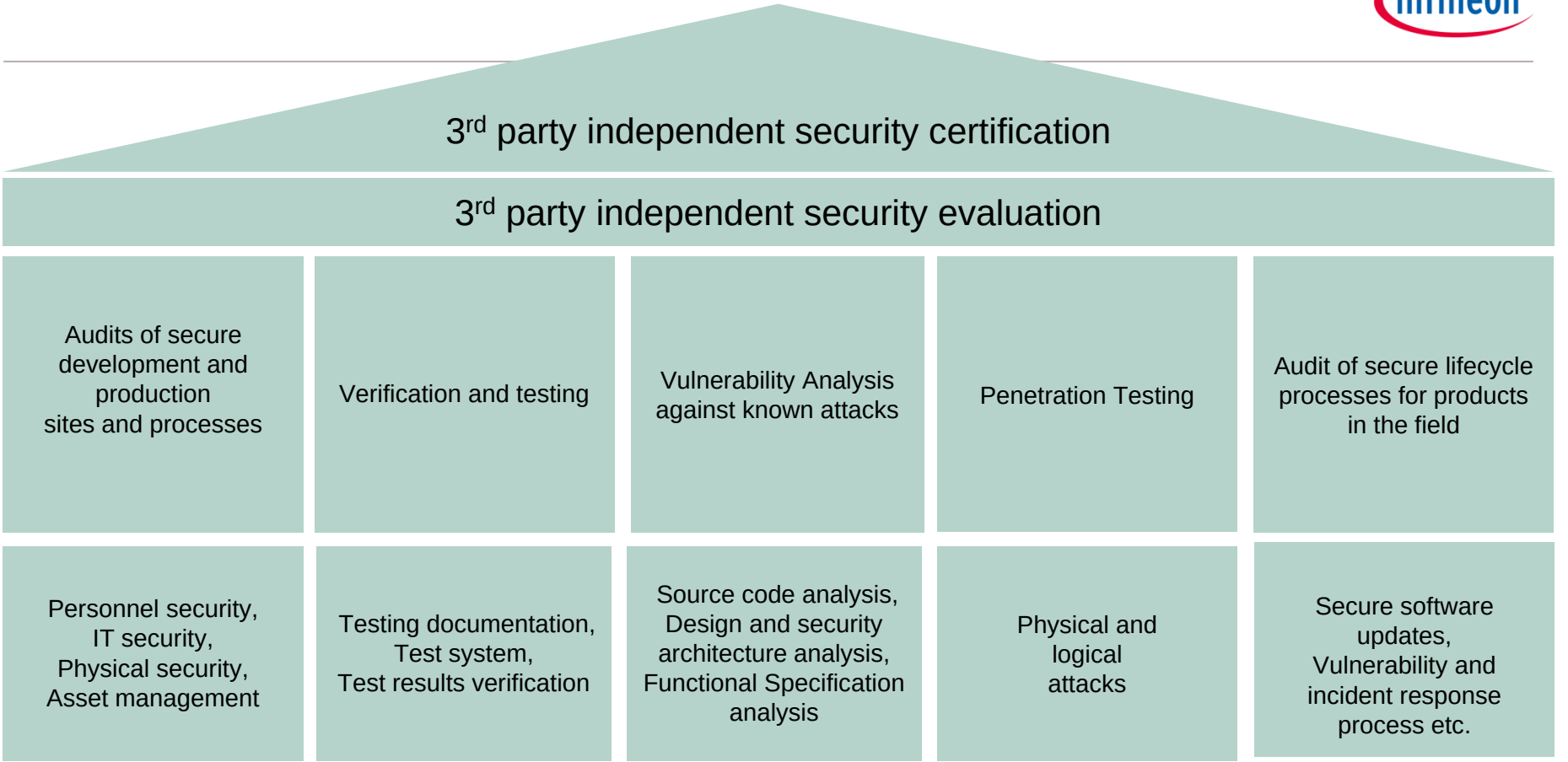
Chip Act Regulation proposal

Pages 27/28 of the Chip Act regulation proposal:

“The internal market would greatly benefit from common standards for green, trusted and secure chips. Future smart devices, systems and connectivity platforms will have to rely on advanced semiconductor components and they will have to meet green, trust and cybersecurity requirements which will largely depend on the features of the underlying technology. To that end, the Union should develop reference certification procedures and require the industry to jointly develop such procedures for specific sectors and technologies with potential high social impact.”

Page 30 of the Chip Act regulation proposal:

“In order to facilitate effective monitoring, in-depth assessment of the risks associated with different stages of the semiconductor value chain is needed, including on the origins and sources of supplies beyond the Union. Such risks may be related to critical inputs and equipment for the industry, including digital products that may be vulnerable, possible impact of counterfeit semiconductors, manufacturing capacities and other risks that may disrupt, compromise or negatively affect the supply chain”



Security evaluation standards for chips

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

Chip security certification schemes also already exist

Schemes	Assurance level as per the EU CSA	Evaluation method	Continuous monitoring	Third party independent assessment	Note
SOGIS	High	CC	Yes	Yes	To be superseded by EUCC, see below. **EU governments driven**. Used for government procurement. targets to show resistance of products to **highly sophisticated attacks. Mainly used for smart card certifications.**
EUCC	High and Substantial	CC	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 **highly sophisticated attacks. Inherits most features from SOGIS.**
EMVCo	High	proprietary	Yes	Yes	Payment industry driven. Targets to show resistance of products **to highly sophisticated attacks.**
PSA Certified	Basic, Substantial	SESIP	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.**
GP SESIP	Substantial	SESIP	Yes	Yes	**Industry driven**. Targets the certification of MCUs used in IOT. **Shows resistance of products to basic/enhanced basic attacks.**

Part of your life. Part of tomorrow.