PP-0117

Secure Sub-System in System on Chip (SoC) Protection Profile

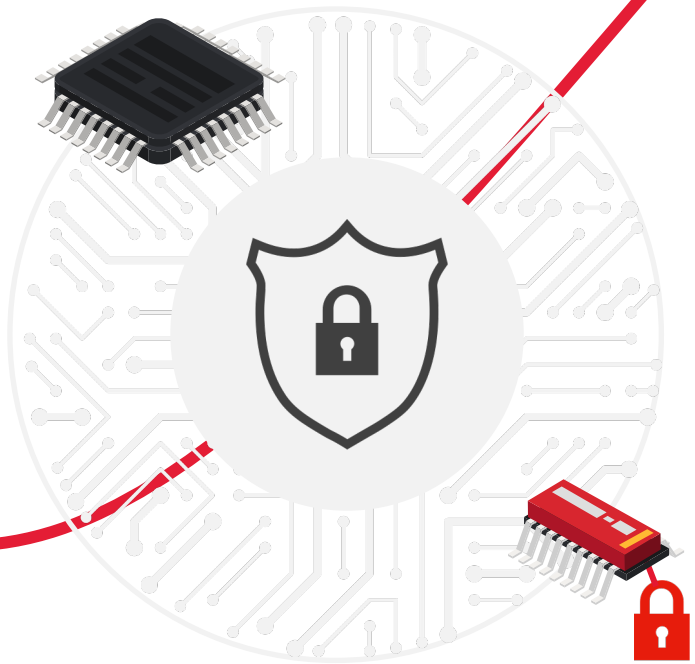
Rachel Menda-Shabat, Winbond, Subgroup Chair

Disclaimer: This document is provided for internal information purposes only. It does not reflect any opinion or position of EUROSMART.

The Rationale for a new Protection Profile

The trend in modern Systems on Chip **(SoC)** and Microcontrollers **(MCU)** is integration of advanced security functions

In particular, the Secure Element **(SE)** / Hardware Security Module **(HSM)** / Trusted Platform Module **(TPM)** can be integrated into the SoC



Filling the Gap

A major **adoption barrier** was the absence of a **Protection Profile (PP)** defining all aspects of using and protecting the security functions being integrated into the SoC

Eurosmart Took this Challenge and
Established the Secure Sub-system (3S) in SoC PP Subgroup
for Developing this Protection Profile

3S in SoC PP Working Group

- 3S in SoC working group includes representatives of developers, labs and certification bodies

- PP editor chosen was T-Systems
- The ITSEF selected for the PP evaluation was SGS
- The Certification Body approving PP evaluation was BSI

Objectives of the PP-0117

Develop a **Protection Profile document** for a Secure Sub-System in SoC

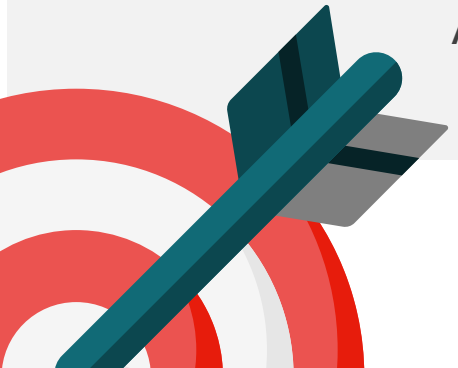
Support external memories (both volatile and non-volatile, Passive and Secure solutions)

Strict conformance to the Security IC Platform Protection Profile (PP-0084)

Add optional packages for software loading and **update**, composite software isolation, crypto, provisioning and **recovery**

PP target is **EAL 4+** (augmented with ALC_DVS.2, **ALC_FLR.2**, ATE_DPT.2 and AVA_VAN.5)

Alignment with groups external to Eurosmart such as GSMA, GlobalPlatform and FIDO



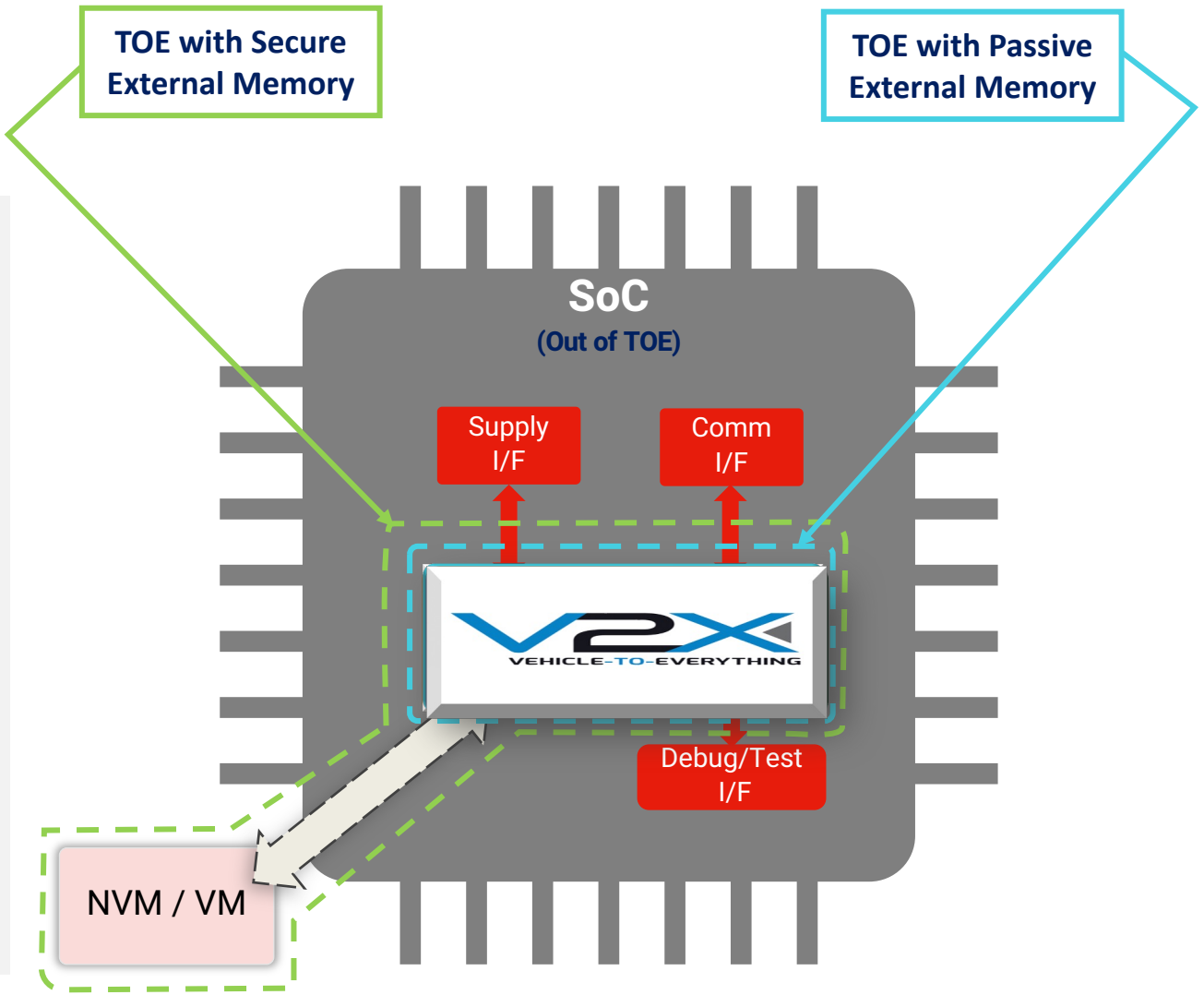
The Target of Evaluation (TOE)

A Secure Sub-System (3S) implemented as a functional block of a System on Chip (SoC) as hardmacro or programmable logic macro

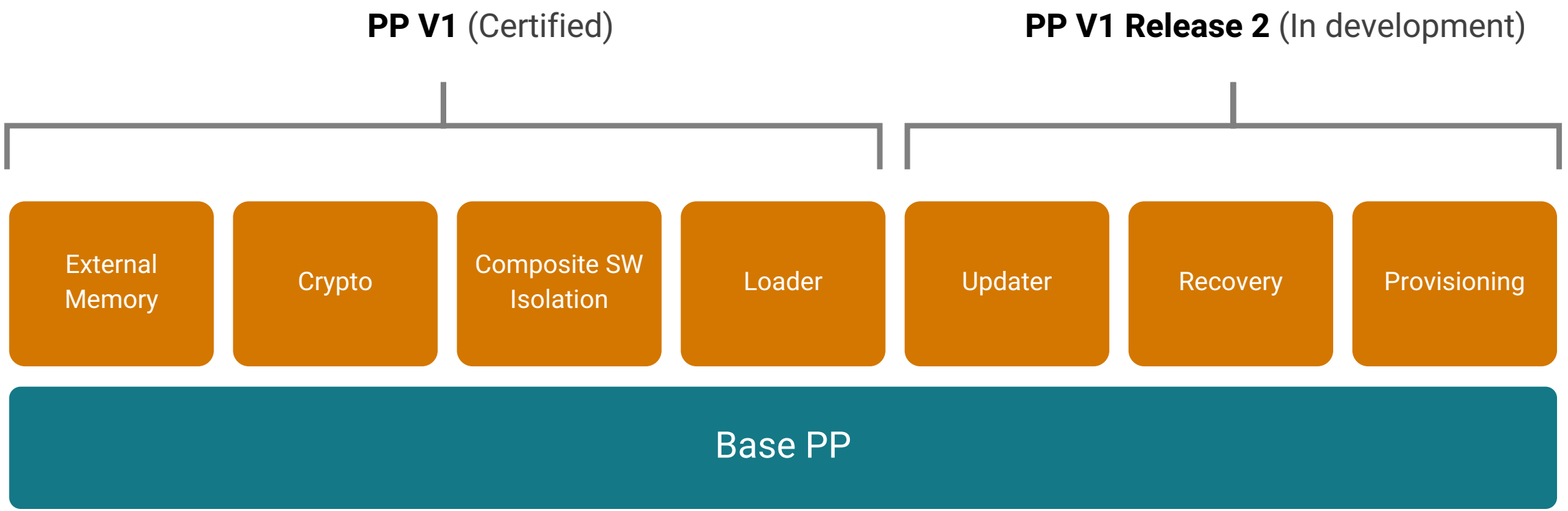
Implements a range of security functionalities covering a defined set of security objectives for the security integrated solutions as SE, eUICC, iSIM, HSM,TPM,V2X and more

Provides its services isolated from the other SoC components based on physical and/or logical isolation mechanisms

In most cases 3S will be relying on external memories



Functional Packages of the PP-0117



Covered Threats in PP-0117

	Internal Memory	Passive Memory	Secure Memory
T.Leak-Inherent	✓	✓	✓
T.Phys-Probing	✓	✓	✓
T.Malfunction	✓	✓	✓
T.Phys-Manipulation	✓	✓	✓
T.Leak-Forced	✓	✓	✓
T.Abuse-Func	✓	✓	✓
T.RND	✓	✓	✓
T.Insecure-State	✓	✓	✓
T.Mem-Content-Abuse		✓	✓
T.Mem-Clone-Replace		✓	✓
T.Mem-Cmd-Replay		✓	✓
T.Mem-Unauth-Rollback		✓	✓
T.Mem-Abuse-Interface			✓

Threats covered by PP-0084

Additional threats in PP-0117

PP-0117 Certified by BSI on March 1st, 2022

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat
erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-CC-PP-0117

Common Criteria Protection Profile

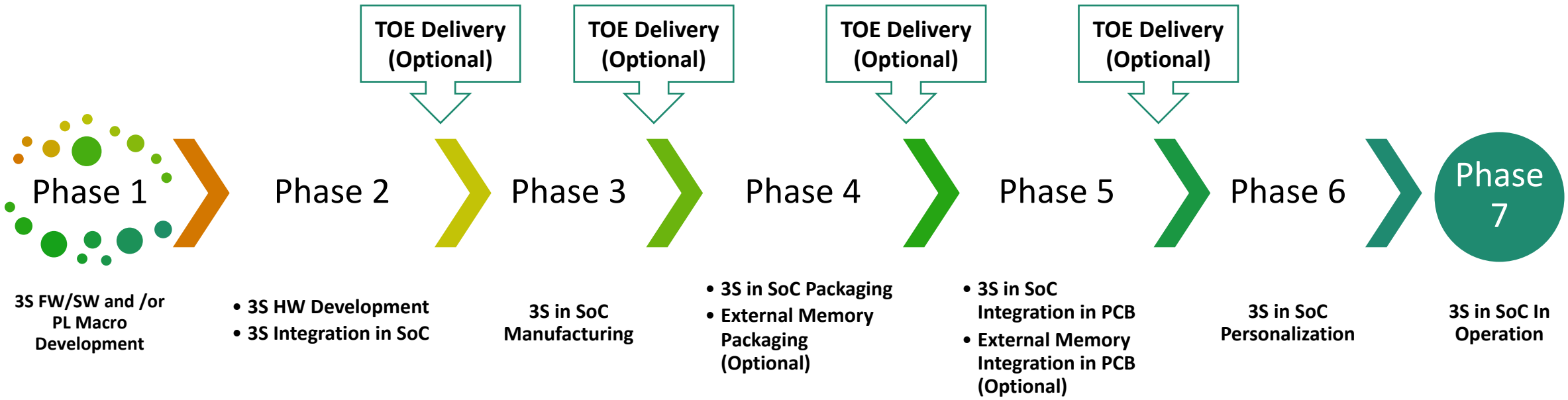
Secure Sub-System in System-on-Chip (3S in SoC), Protection Profile, Version 1.5

developed by EUROSMART

Assurance Package claimed in the Protection Profile:
Common Criteria Part 3 conformant
EAL 4 augmented by
ATE_DPT.2, AVA_VAN.5, ALC_DVS.2 and ALC_FLR.2

SOGIS Recognition Agreement

PP-0117 Life-Cycle

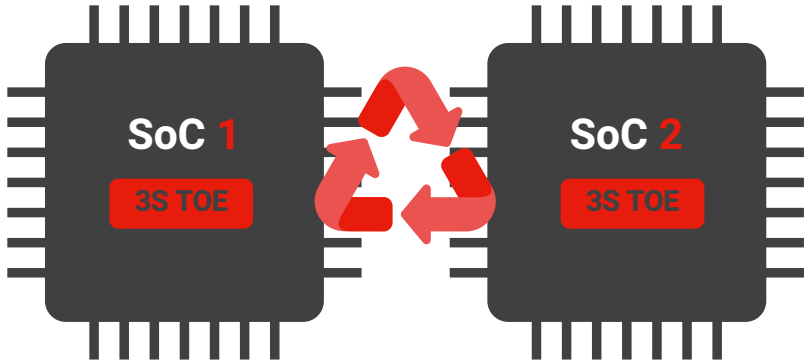


3S Re-Use Methodology

PP-0117 aims to favour re-use of the 3S TOE in multiple SoCs based on integration guidance.

The lab performing the evaluation in the first SoC generates the Evaluation Test Report “ETR for Integration” to facilitate evaluation in subsequent SoCs by other labs:

- Contains relevant information from the initial 3S evaluation to ease evaluating the same 3S in a different SoC
- Identifies dependencies of the 3S TOE from the surrounding SoC to allow optimal re-use



Re-use of a certified 3S TOE from one SoC to another one

Collaboration with External Entities

- Mapping exercise between FIDO Authenticator security requirements and PP-0117 as part of FIDO Companion Program
- Working towards PP-0117 being accepted by GlobalPlatform wherever PP-0084 is accepted
- Collaboration with GSMA to ensure PP-0117 is used for “integrated eUICC” evaluation
- Collaboration with Java Card Form to ensure PP-0117 is used for “Java Card System – Open Configuration” evaluation

Thanks for your attention!

Rachel Menda-Shabat

Eurosmart Contact: Pierre-Jean Verrando
<pierrejean.verrando@eurosmart.com>

EUROSMART
The Voice of the Digital Security Industry

Cooperation between all groups

- For best synergy the work is performed in cooperation with JHAS and ISCI-WG1 subgroups:
  - ITSC defines the PP
  - ISCI defines the evaluation methodology
  - JHAS defines the attacks

PP-0117 Compared to PP-0084

Main Additions

- ✓ Support of external volatile and non-volatile memories (supplement to PP-0084 Augmentation Package: External NVM Storage)
- ✓ Support for flaw remediation
- ✓ Root-of-Trust functionality
- ✓ Physical and/or logical isolation with other SoC components
- ✓ Support of composite software isolation

Additional Changes

- ✓ RNG extended to include active attacks
- ✓ Generalize Crypto package