SESIP short introduction

RISC-V Security HC

GlobalPlatform SESIP Working Group

March 31, 2022



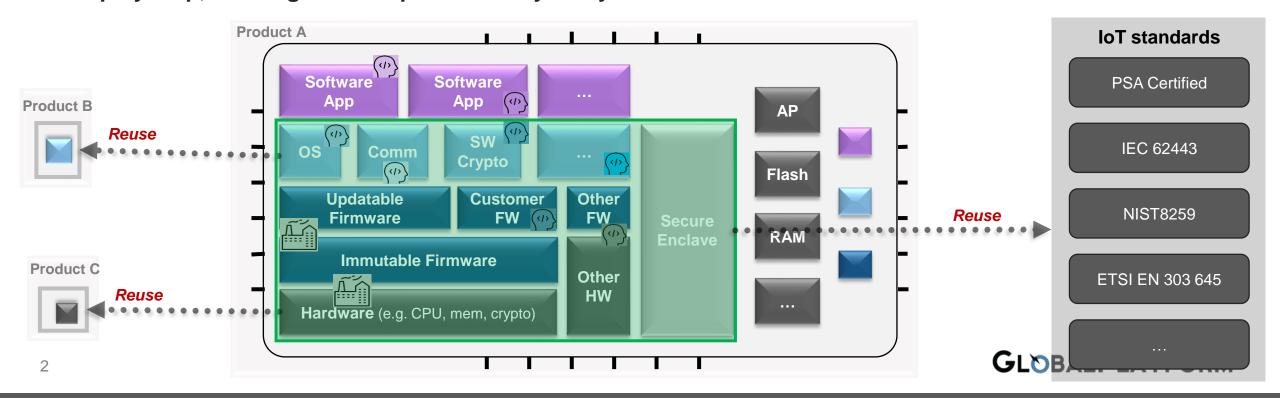
SESIP overview

Security Evaluation Standard for IoT Platforms

- Evaluation of <u>platform parts</u> N & any type of <u>compositions</u> of subcomponents, from different developers ()

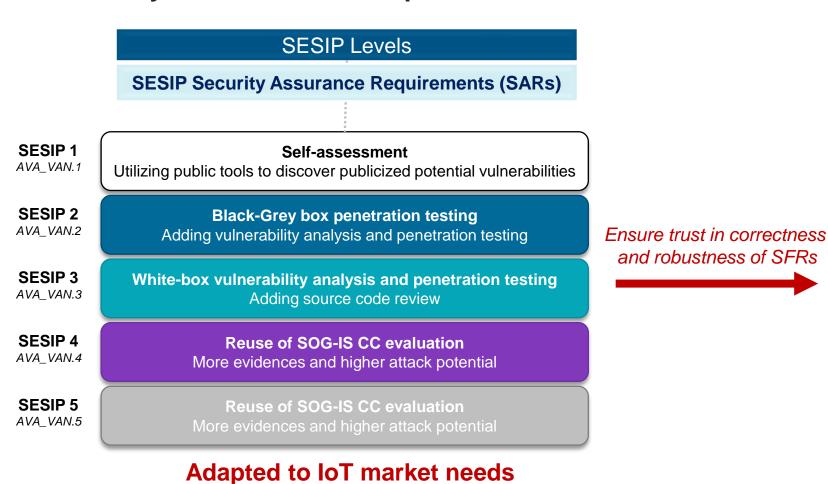
- Reuse of evaluation results for composition evaluations, in different devices
- Reuse of evaluation results as support for compliance demonstration IoT standards

Step by step, building of a complete security analysis



SESIP base tools

Security and Assurance requirements & SESIP levels



SESIPSecurity Functional Requirements (SFRs)

SFRs categories

Identification and Attestation

Life cycle management

Cryptographic functionalities

Secure communication

Compliance functionalities

Extra attacker resistance

Intuitive, generic to all IoT standards



SESIP extended tools

Security Targets

- Security claim of a specific product
 - Generic descriptions, evaluation scope, use cases, etc.
 - Security Functional Requirements (which security features)
 - Security Assurance Requirements (which evaluation activities)

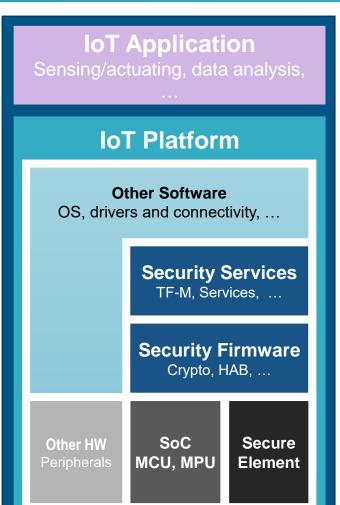
SESIP Profiles

- Generic requirements per type of products
 - Security Functional Requirements (which security features)
 - Security Assurance Requirements (which evaluation activities)
- Ensure comparability between certificates
- Written upon need by stakeholders

SESIP Mappings

- Map SESIP SFRs & SARs to standards requirements
- Allow the reuse of SESIP evaluation results for compliance demonstration to standards

Mapping to standard Req X supported by SFR a Req Y supported by Req Z not supported ST/SP [standard] support Secure comm ST/SP core HW Secure storage HW Secure initialization Secure update [Crypto HW]





SESIP process

