



2024-09-18

# SESIP Profiles

**Cybersecurity Vehicle Forum**

**2025-12-09**

# SESIP Evaluation Methodology

## Core Structure

- Foundation: Based on Common Criteria ISO/IEC 15408-3
- Five Assurance Levels: SESIP1 (self-assessment) through SESIP5 (highest SOG-IS reuse level)

## Security Functional Requirements (6 Categories)

- Identification/Attestation: Platform identity verification (mandatory), genuineness attestation, secure initialization
- Lifecycle Management: Secure update/install (mandatory), factory reset, decommission, field return
- Secure Communication: Channel support and enforcement with specified protocols
- Attacker Resistance: Physical and software isolation capabilities for extended threat scenarios
- Cryptographic Functions: Operations, key generation/storage, random number generation
- Compliance: Secure storage, encryption, audit logging, residual information purging

## Key Features

- Composition Framework: Reuse of evaluated platform parts across different platforms and products
- Threat Model: Base scenario assumes remote-only attackers; extended scenarios cover physical/software attacks
- Documentation: Security Target template, attack potential rating guidance, composition guidelines
- Standards Integration: Maps to some ETSI, ISO/IEC, NIST requirements for regulatory compliance



GlobalPlatform Technology

## Security Evaluation Standard for IoT Platforms (SESIP) Methodology

Version 1.2

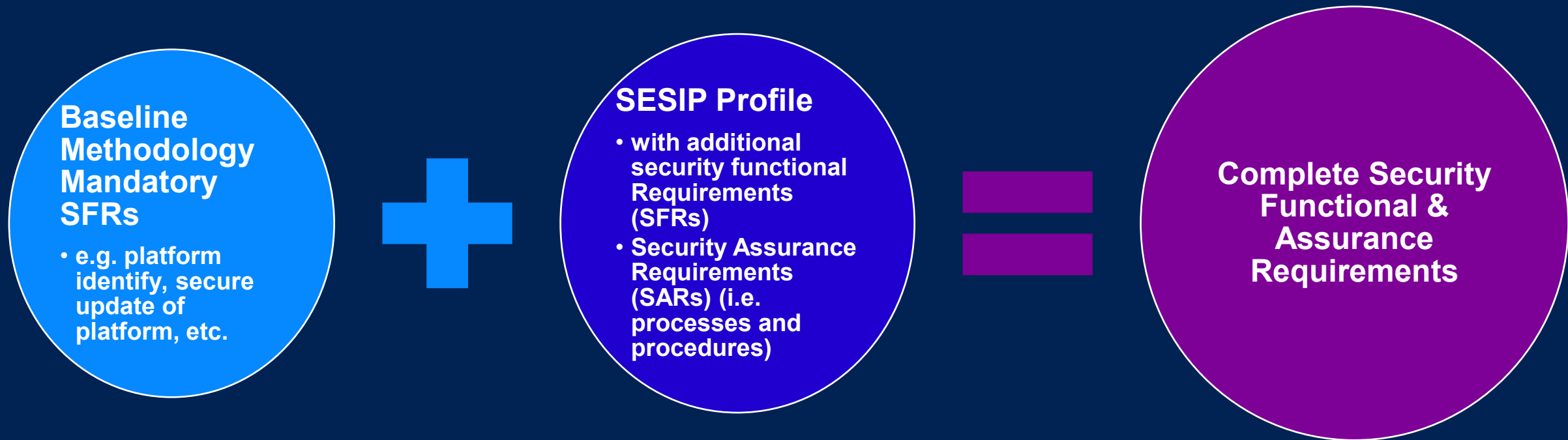
Public Release

July 2023

Document Reference: GP\_FST\_070

[https://globalplatform.org/wp-content/uploads/2021/03/GP\\_SESIP\\_v1.0.0.4\\_PublicRvw.pdf](https://globalplatform.org/wp-content/uploads/2021/03/GP_SESIP_v1.0.0.4_PublicRvw.pdf)

# Security Functional Requirements



# SESIP Profiles: Industry-Standard Security Templates

Profiles (PPs) define **consensus-based security expectations for specific product categories**, creating:

- a common foundation for security evaluation.



Profiles transform SESIP certification:

- from a custom evaluation process into a **standardized framework** that balances security rigor with evaluation efficiency, creating:
- recognizable security benchmarks for IoT and embedded systems across industries.

# Example SFR - Diagnostic Access Control

## 5.3.1 Diagnostic Privileged Access Control

### Requirement

The Platform allows access to diagnostic <services / functions / data> using <list of interfaces> only under <list of preconditions>

INFO In most ECUs, this requirement is implemented by UDS session control mechanisms that restrict which diagnostic services can be accessed at each session level (e.g., service 0x10 “Diagnostic Session Control” or OEM-specific access modes).

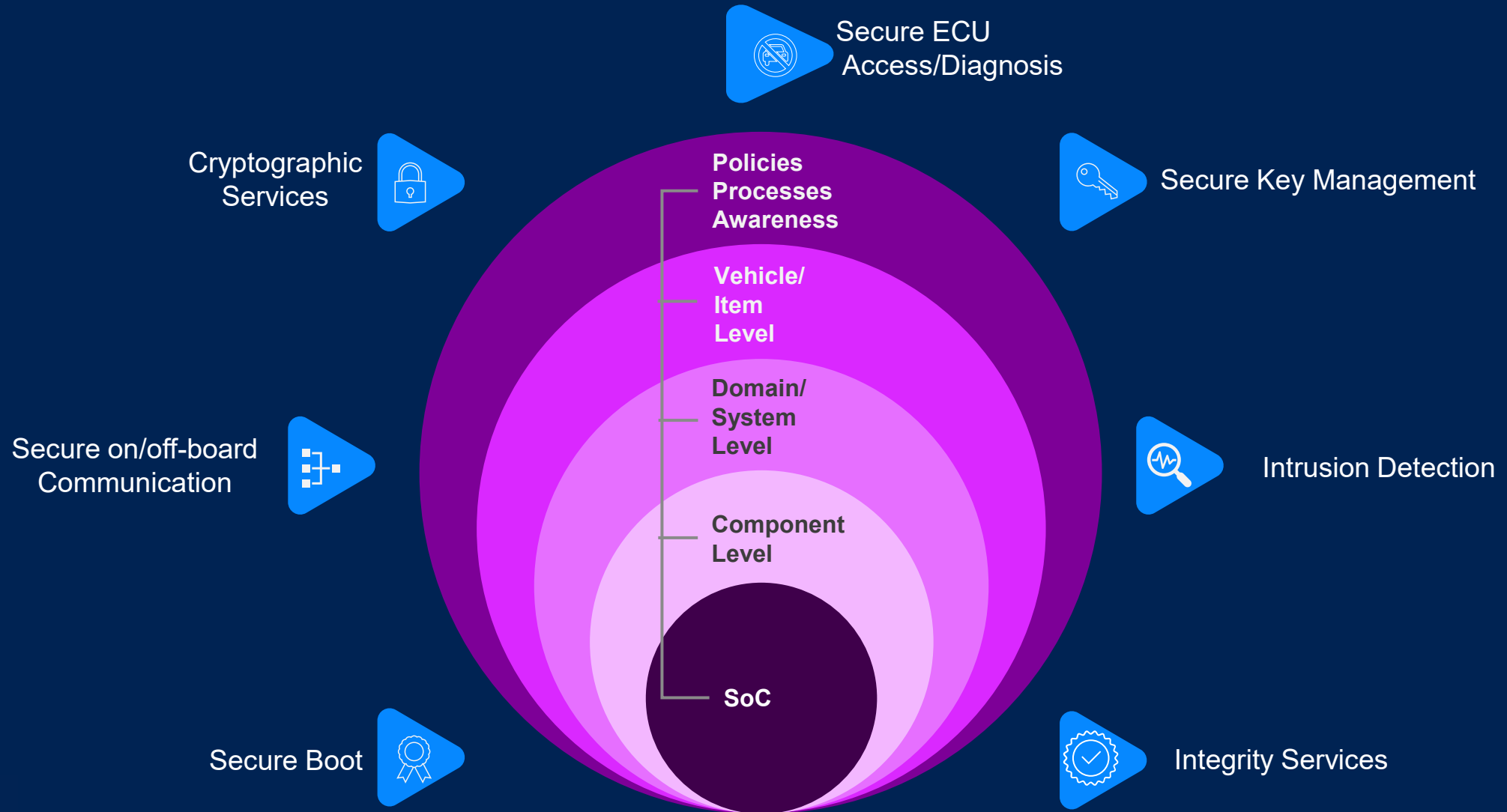
Additional restrictions are commonly enforced based on interface (e.g., external OBD-II port vs. internal vehicle bus) or network origin (e.g., requests from a secure gateway vs. external network).

### Value

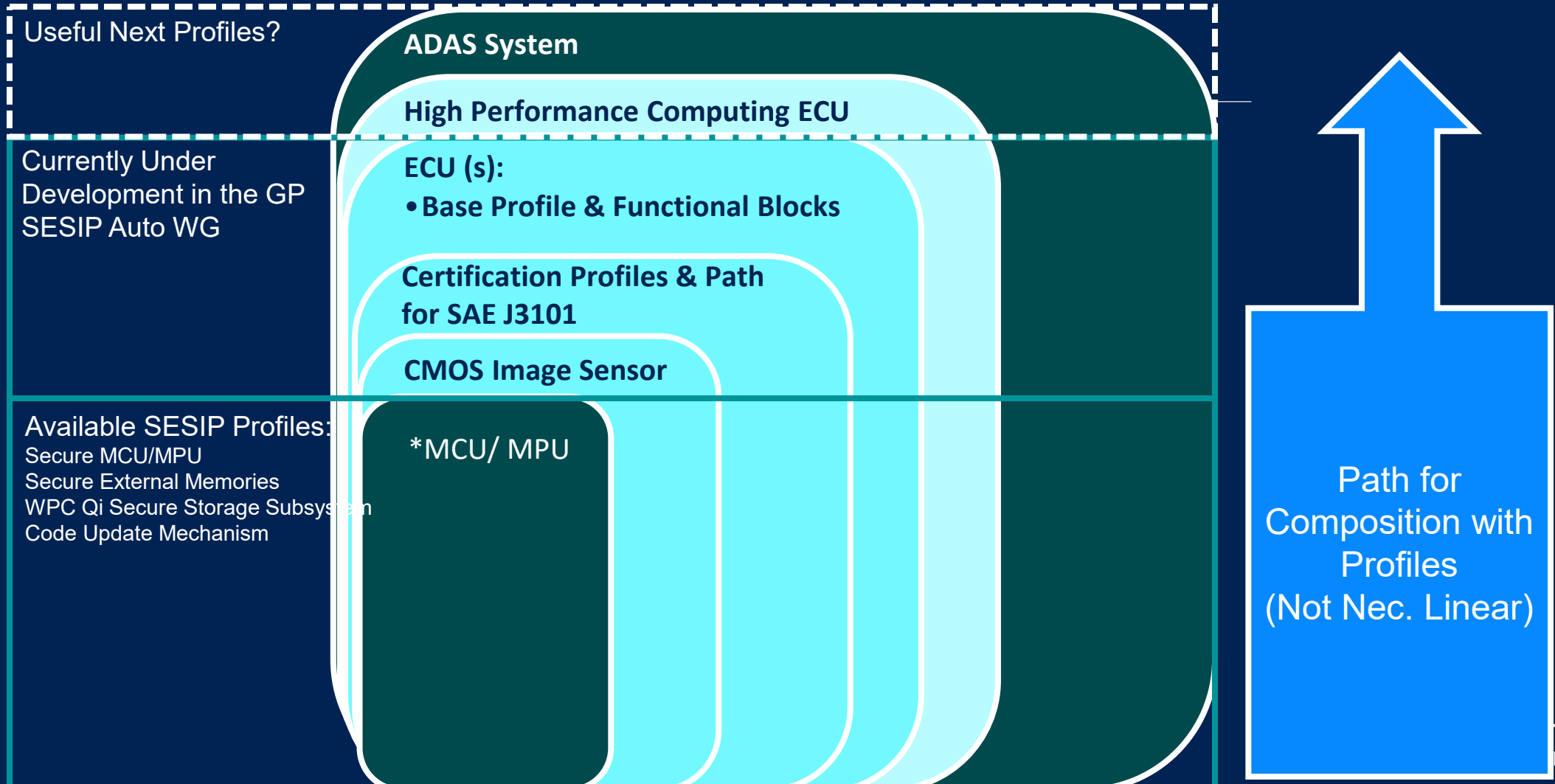
This SFR is used to enforce privileged access control for diagnostic operations that are not necessarily based on user or entity authentication, but rather on contextual conditions or privilege attributes. Typical examples include:

- Physical or logical interface origin (e.g., *internal CAN bus, external OBD-II port, DoIP endpoint*).
- Diagnostic session type or level (e.g., *default, extended, programming, manufacturing*).
- Vehicle or ECU operational state (e.g., *ignition off, vehicle stationary, maintenance mode*).

# SESIP Opportunity: Beyond SoCs



# SESIP Automotive Profiles Roadmap





**SESIP Technical Automotive SG**

**SAE J3101 Profile**

**Hardware Protected Security for  
Ground Vehicles**

# Rationale

The purpose of this information report is to provide an analysis and summary of the coverage of J3101 requirements by existing GlobalPlatform technologies – Secure Elements (SE) and Trusted Execution Environment (TEE).

# Scope

The scope of the analysis is on the GlobalPlatform Secure Elements (SEs) and Trusted Execution Environments (TEEs) standard specifications correspondence to J3101 recommended practices. This analysis includes focuses on the platform specifications but not the scope of any future security application/applets. Both of these GlobalPlatform specifications have associated protection profiles to validate compliance, although GlobalPlatform does not currently have any specific J3101 protection profiles. GlobalPlatform has communicated that it is assessing whether or not to develop application-level protection profiles to more explicitly cover the remaining requirements of J3101, in order to allow for standardized testing and certification of complete solutions.

# Motivation

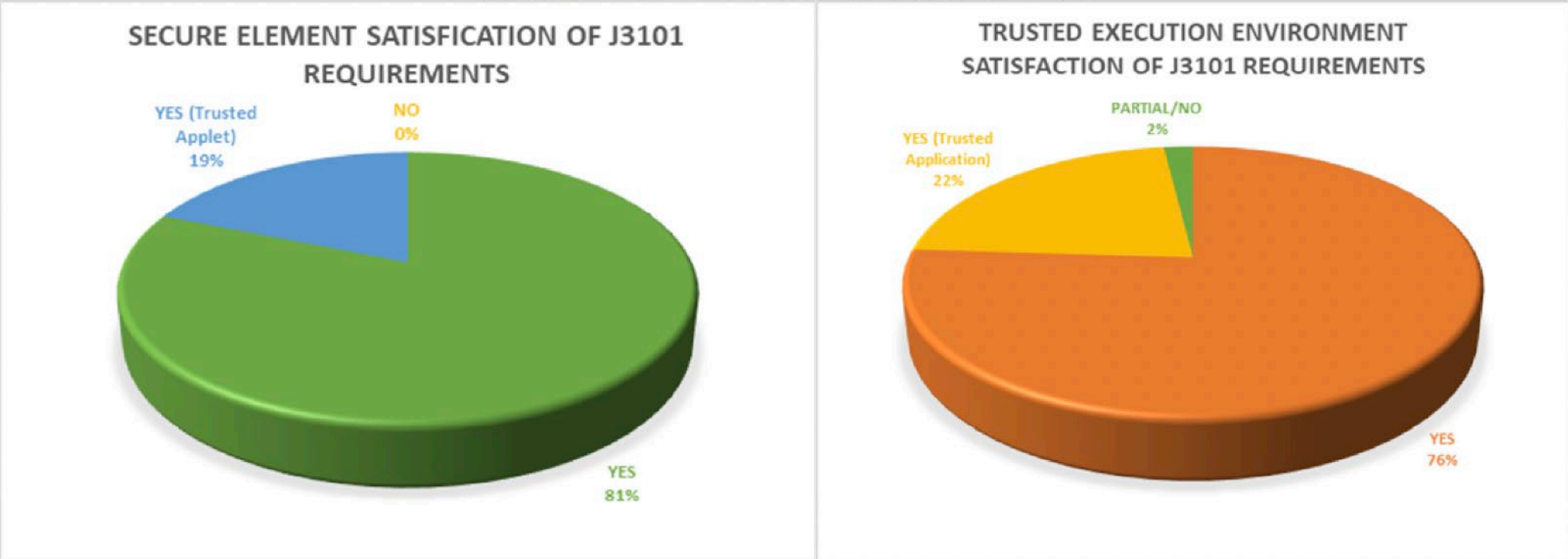
The Goal of J3101-5 is to provide a translation of language to describe Automotive Hardware Security Solutions interchangeably between SAE J3101 implementations and GlobalPlatform implementations.

# Methodology – Requirements Categorization

SAE J3101 Requirements	Description of GlobalPlatform categorization for the mapping
<b>Yes</b>	This J3101 requirement is fulfilled by the assessed specification
<b>Yes: Trusted Application</b>	This J3101 requirement is fulfilled by the assessed specification through the development of Trusted Applet/ Application running on a GlobalPlatform compliant platform.
<b>Partial</b>	This J3101 requirement is partially fulfilled by the assessed specification. The details of this choice are included in the comments section for each requirement.
<b>Not Covered</b>	This J3101 requirement is not fulfilled by the assessed specification.

# J3101 Protection Profile

FIGURE 1: PERCENTAGE OF FULFILMENT OF J3101 REQUIREMENTS BY GLOBALPLATFORM TECHNOLOGIES (MANDATORY + OPTIONAL REQUIREMENTS)



# J3101 SESIP Baseline Profile





**SESIP Technical Automotive SG**

**Automotive CMOS Image Sensor Profile**

# AIST - National Institute of Advanced Industrial Science and Technology

## Mission

- To advance industrial science and technology
- To bridge fundamental research and commercial applications
- To support the competitiveness of Japanese industry and contribute to society

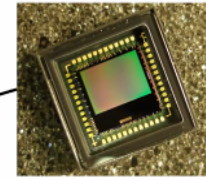
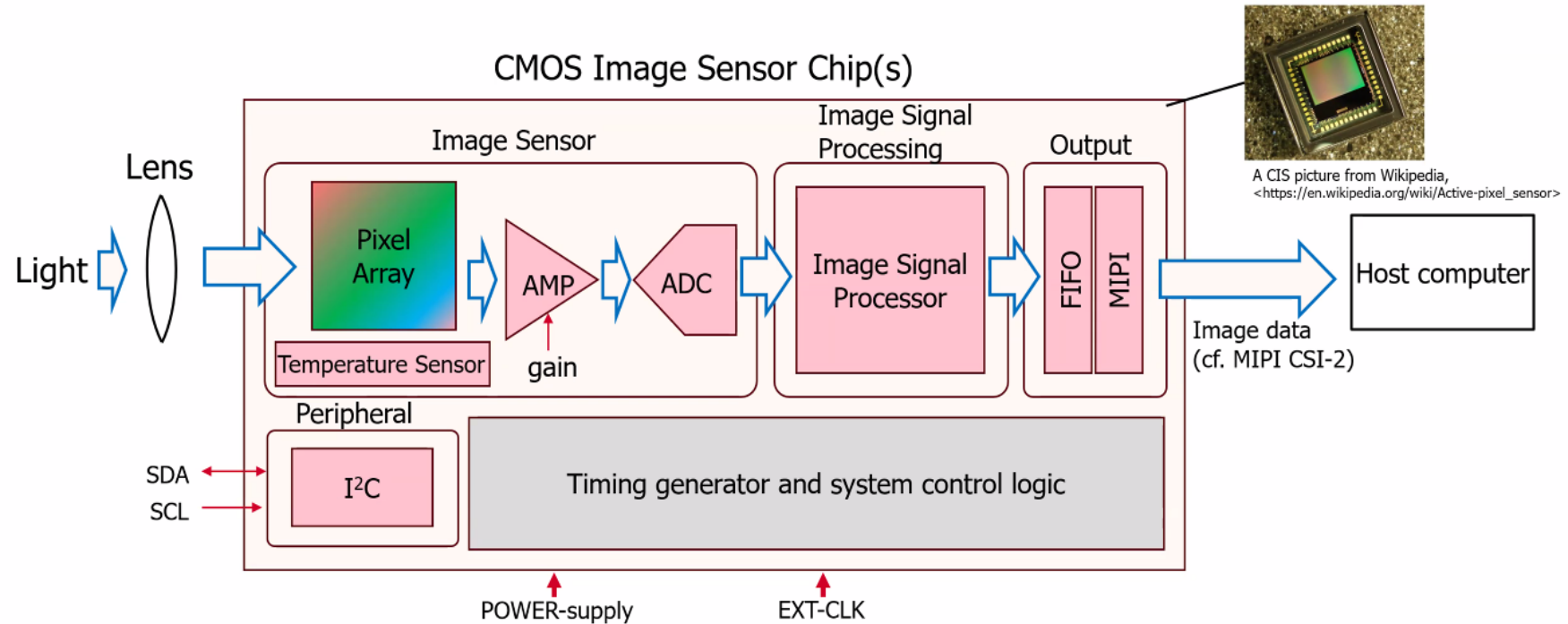


## Key Focus Areas

- Artificial Intelligence & Robotics
- Cybersecurity & IoT Technologies
- Smart Manufacturing (Industry 4.0)

# AIST – CMOS Image Sensor

Incoming light from the environment is processed and its image data is sent to a host computer.



A CIS picture from Wikipedia, [https://en.wikipedia.org/wiki/Active-pixel\\_sensor](https://en.wikipedia.org/wiki/Active-pixel_sensor)



Abbreviation	AMP(Amplifier)、ADC(Analog to Digital Converter)、FIFO(First-In, First-Out Buffer)、MIPI(Mobile Industry Processor Interface)、CSI-2(Camera Serial Interface 2)、I <sup>2</sup> C(Inter-Integrated Circuit)、SDA(serial data line)、SCL(serial clock line)
--------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

# AIST – CMOS Image Sensor

- AIST is actively addressing **security challenges** in CMOS Image Sensors
- Developed a structured **security problem definition**, including:
  -  **Assets:** Image data, sensor configurations, control logic, firmware
  -  **Threats:**
    - Unauthorized access or control of sensor
    - Data leakage or covert exfiltration
    - Tampering with captured image content
  -  **Potential Vulnerabilities:**
    - Insecure interfaces (e.g., test/debug ports)
    - Unprotected memory or firmware regions
    - Lack of authentication in communication protocols
  -  **Security Functional Requirements** under development:
    - Secure boot and firmware update
    - Access control and interface protection
    - Integrity checks for image and configuration data

# AIST – CMOS Image Sensor – 1<sup>st</sup> Draft

- Automotive CMOS Image Sensor Profile
  - Image array considered out of scope
  - SESIP Levels 1,2 and 3
  - Packages: Secure Update & Physical Resistance
  - Mapping to MPU/MCU Profile

SESIP SFR	MCU / MPU Profile	ACIS Profile
Verification of Platform Identity	Base SP	Mandatory
Verification of Platform Instance Identity	-	Mandatory
Secure Initialization of platform	Base SP	Mandatory
Secure Communication Support	-	Mandatory
Secure Communication Enforcement	-	Mandatory
Attestation of Platform Genuineness	-	Optional
Secure Debugging	Base SP	Optional
Secure Data Serialization	Package 'Secure Storage'	Optional
Secure Trusted Storage	Package 'Secure Storage'	Optional
Secure Confidential Storage	Package 'Secure Storage'	Optional
Secure Encrypted Storage	Package 'Secure Storage'	Optional
Cryptographic Operation	Package 'Security Services'	Optional
Secure Update of platform	Base SP	Package 'Secure Update'
Limited Physical Attacker Resistance	Package 'Secure Enclave'	Package 'Hardware Protections'



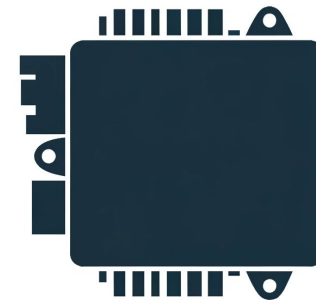
# ECU Profile

# Base Protection Profile

- **Assumptions**
  - Functionality not defined
  - Common automotive interfaces (CAN, LIN or Ethernet)
  - ECU running only RTOS (based on AUTOSAR OS)
- **Reuse of Profiles / Certificates**
  - GP TEE / SE
  - SESIP SAE J3101
  - SESIP MPU / MCU
  - ...
- **Additional Requirements for different SESIP Levels**
  - Potential mapping to CAL
  - Mapping to ASIL levels (?)

## Limited Surface

- **ECU with SoC** (AUTOSAR RTOS)
- **Wired Interfaces** (CAN, LIN)
- **Example:** Rear Lamp system integrating one SoC using AUTOSAR OS with 2 x CAN and a LIN interface



# Profile Structure

- **Core Package:** Secure boot/integrity, identity, crypto, key mgmt, secure comms, secure update, hardening
- **Functionality packages (select):** Secure Diagnostics (UDS/DoIP), Secure Update, Secure Logging, Secure Time, Secure Storage, Secure Debug, Secure Measurement/Calibration
- **Protocol Packages (select):**
  - CAN, LIN, FlexRay, Automotive Ethernet, *Wi-Fi (?)*, *Bluetooth (?)*
- **Optional SFRs:** Attestation, Decommissioning, Field Return, ...
- **Testing Methods:** Explicitly include testing methods from ISO 21434 (Functional Testing, Penetration Testing, Fuzzing, Vulnerability Analysis)
  - Optional: References to ISO/SAE 8477 & SAE J3322

# Example Requirements (Core)

- **Secure Boot:** The ECU verifies authenticity & integrity of boot components and application images before execution; failed checks prevent normal boot and trigger defined recovery.
- **Identity & Keys:** The ECU maintains a device-unique identity; private keys remain non-exportable; key lifecycle covers generation/import, storage, rotation, decommissioning.
- **Crypto:** Approved algorithms & parameters; authenticated encryption; hardware acceleration if available; side-channel/tamper considerations per SESIP level.
- **Secure Update:** Updates are authenticated, integrity-checked, anti-rollback enforced, and applied atomically with recovery paths.
  - Alignment with ISO 24089
- **Hardening:** Least privilege, memory protection, secure configuration baselines.

# Example Requirements (Functional Packages)

- **Secure Diagnostics (UDS/DoIP)**

- Access levels with cryptographic challenge-response; attempt limiting & lockout.
- Separation of safety-critical routines; audit of security-relevant services.
- Secure seed/key algorithms and protection of secrets in HPSE.

- **Secure Logging**

- Secure logging storage
- Log retention/rollover policy; privacy filtering;
- export via authenticated channels.

- **Secure Debug**

- Debug disabled in production or gated by hardware tokens/cert-based unlock; all unlocks logged; time-bounded authorization.

# Example SFR - Secure Debugging

## 5.2.4 Secure Debugging

### Requirement

The platform only provides <list of endpoints> authenticated as specified in <specification> with debug functionality.

~~The platform ensures that all user data stored, with the exception of <list of exceptions>, is made unavailable.~~

INFO The secure debug functionality (e.g., debug port lockdown, authentication, or controlled unlock mechanisms) may be fully or partially provided by a certified Platform Part, such as a SESIP-certified MCU/MPU.

In such cases, the evaluator shall verify that:

- The secure debug features of the certified Platform Part are enabled and configured according to the component's security guidance and manufacturer documentation.
- Any higher-level debug management implemented by the ECU firmware correctly integrates and enforces the Platform Part's access control mechanisms.
- The integration ensures that debug authentication material (e.g., tokens, certificates, or challenge-response keys) is handled securely throughout the ECU lifecycle.

When these conditions are met, evaluation activities, such as AVA (Vulnerability Analysis) or equivalent tests, do not need to be repeated for the secure debug mechanisms as they are already covered by the referenced certification. The evaluator shall instead focus activities on integration assurance, confirming that no new vulnerabilities are introduced through configuration, interface exposure, or the operational use of debug functions.

# Specialized Profiles

- **Additional Profiles to Consider**
  - **TCU Profile:** adds Cellular, eSIM/eUICC, TLS mutual auth, backend bindings, OTA hardening
  - **Infotainment (IVI):** adds user data protection, app sandboxing, media ingress hardening, Bluetooth/Wi-Fi packages
  - **Security Gateway:** adds multi-net segmentation, policy enforcement, IDS/IPS, key orchestration



# Questions?



# Global Platform™

The standard for  
secure digital services  
and devices

→ [globalplatform.org](https://globalplatform.org)