Global Platform®

2025-12-09

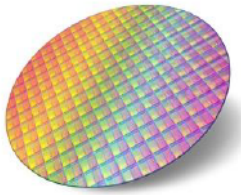
Semiconductor Traceability and Provenance Workshop

Early Lifecycle: Supply Chain Security Automotive Perspective

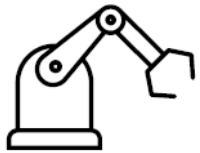
The automotive supply chain | Where does Chain of trust begin?

Microdevice Design

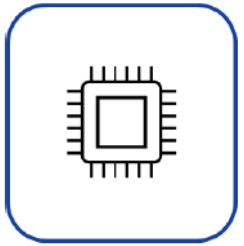
Untrusted Commercial Supply-Chain



Foundry & Wafer Sort



OSAT & package



Packaged Part

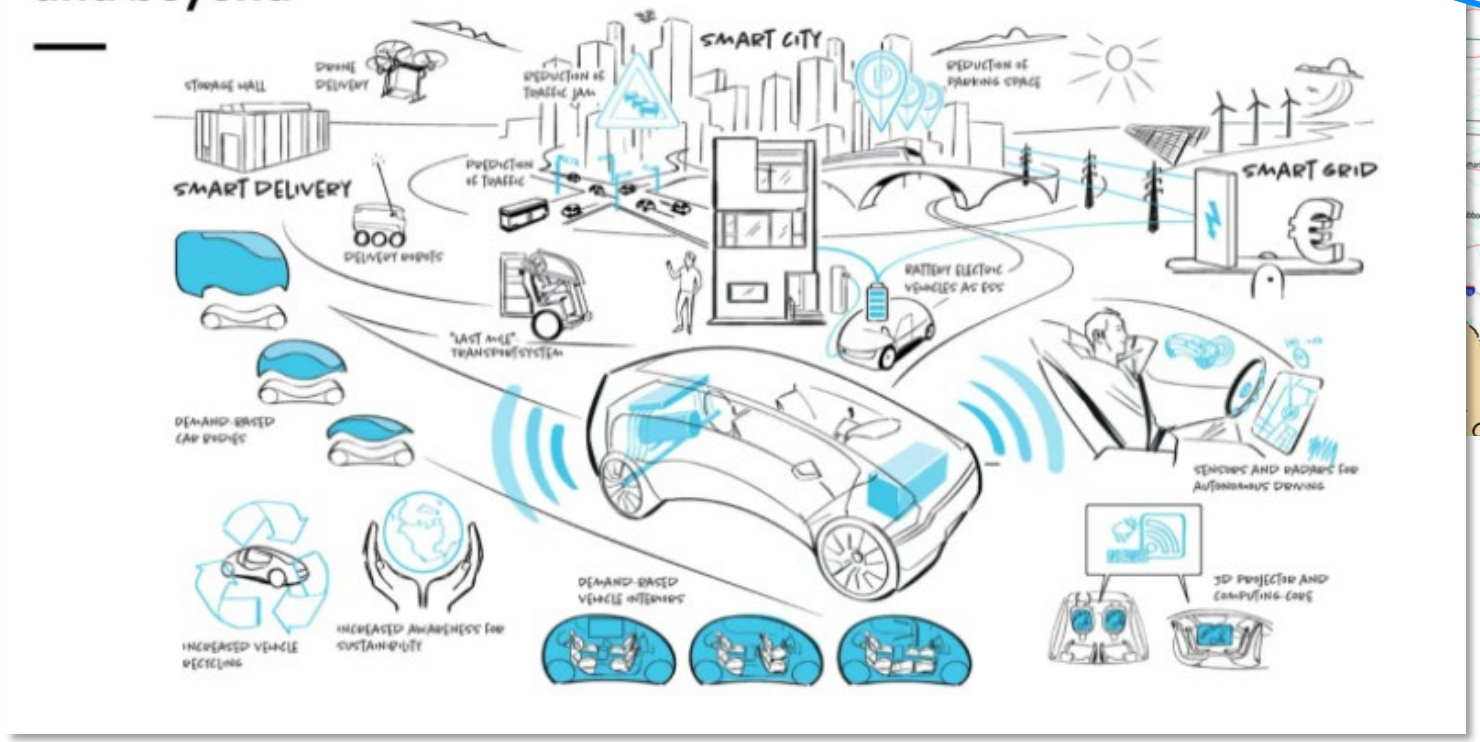
SoC (Tier 2 Supplier)

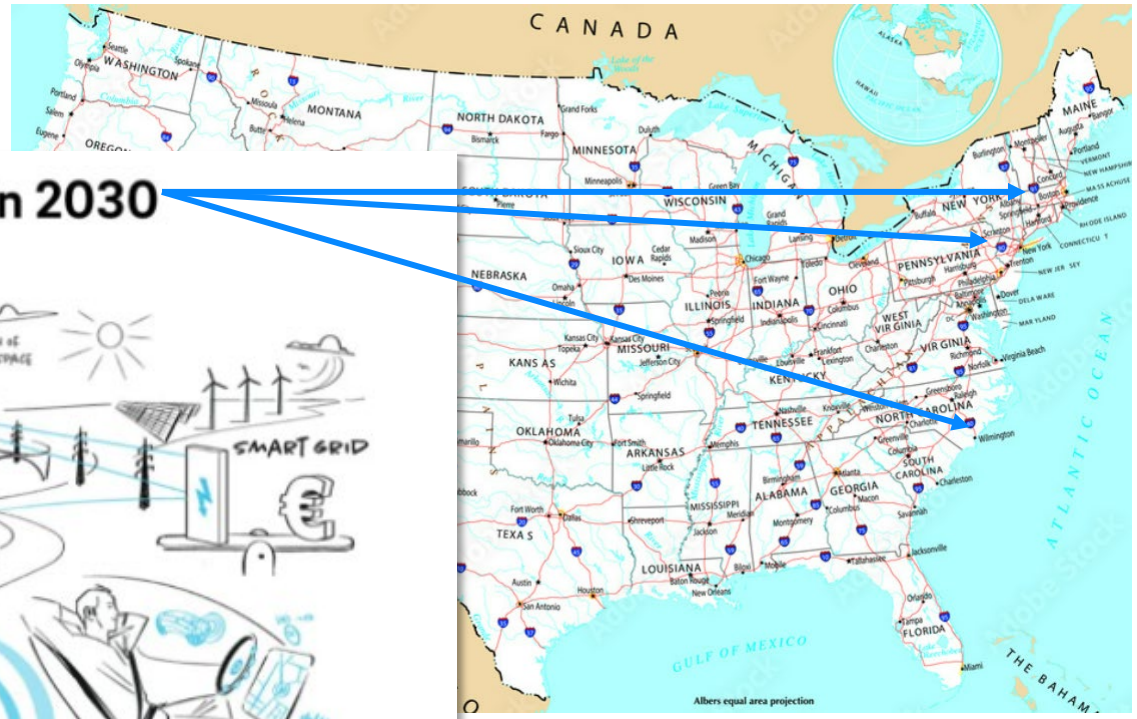
Cyber Relevant ECU (Tier 1 Supplier)

Vehicle EE Architecture (OEM)

Mobility platform & ecosystem

Characteristics of the "Mobility ecosystem in 2030 and beyond"





Homeland Security

Critical Infrastructure: Automotive

Connected

Autonomous

Shared

Electric

FOR IMMEDIATE RELEASE | January 14, 2025 | Media Contact: OCPA@bis.doc.gov

Commerce Finalizes Rule to Secure Connected Vehicle Supply Chains from Foreign Adversary Threats

Download as PDF

Washington, D.C. – Today, the U.S. Department of Commerce's Bureau of Industry and Security (BIS) announced a final rule prohibiting certain transactions involving the sale or import of connected vehicles integrating specific pieces of hardware and software, or those components sold separately, with a sufficient nexus to the People's Republic of China (PRC) or Russia.

Source: https://www.bis.gov/press-release/commerce-finalizes-rule-secure-connected-vehicle-supply-chains-foreign-adversary-threats

SAE J3101 – Hardware protected security environment (HPSE)

SAE INTERNATIONAL Mobility, Advanced

Standards | Publications | Events | News & Media | Explore Topics | STEM Education

Home / Standards / Hardware Protected Security Environment - GlobalPlatform Technologies Information Report J3101-5_202509

J3101-5_202509 - Hardware Protected Security Environment - GlobalPlatform Technologies Information Report

Electrical Systems and Electronics, Connectivity and Software

CURRENT This is a Current Standard

The scope of the analysis is on the GlobalPlatform Secure Element (SE) and Trusted Execution Environment (TEE) standard specifications correspondence to SAE 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 SAE 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 SAE J3101 in order to allow for standardized testing and certification of complete solutions.

https://www.sae.org/standards/j3101-5_202509-hardware-protected-security-environment-globalplatform-technologies-information-report

SoC Implementation examples:

- Security Hardware Extension (HIS)
- Hardware Security Module (EVITA)
- Secure Element (GlobalPlatform)
- TEE (GlobalPlatform)
- HSM-SE (GlobalPlatform – NEW)
- Micro-TEE (GlobalPlatform – NEW)

WHAT IS A “ROOT OF TRUST”?

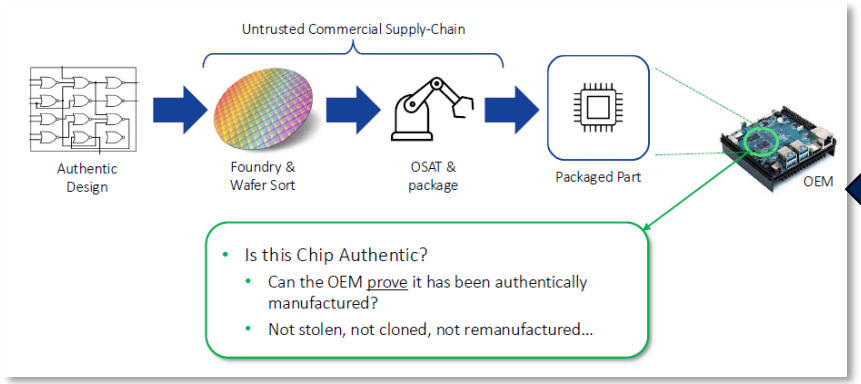
A Root of Trust (RoT) is a foundational, highly reliable component of a system that establishes a secure environment by verifying the integrity and authenticity of hardware, firmware, and software.

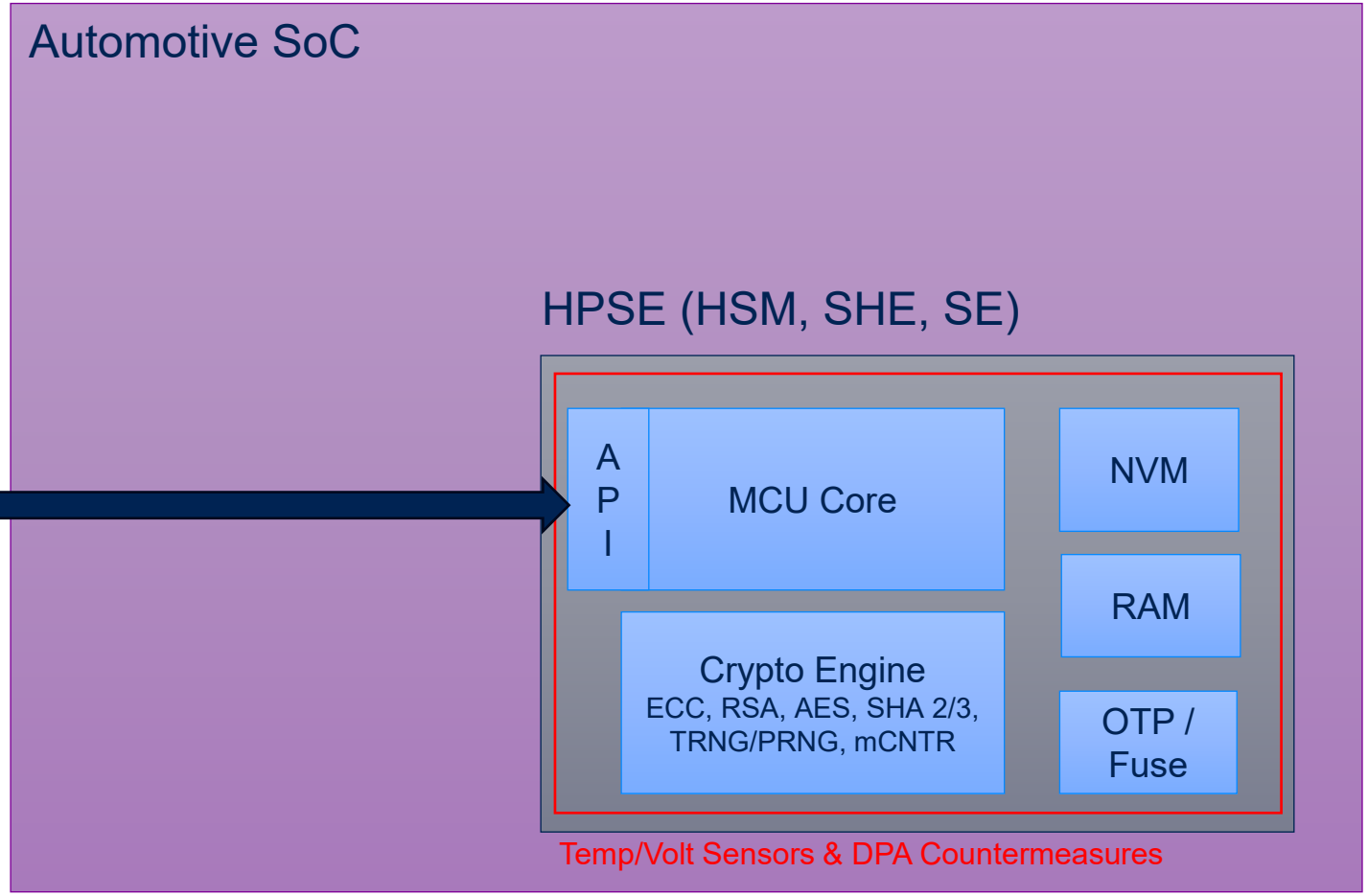
…and trusted

By definition, this must be an integrated HPSE feature

IS AN HPSE A HARDWARE ROOT OF TRUST?

Answer: An HPSE may include a RoT feature but today's automotive HPSEs do not meet the minimal viable requirements for a RoT feature.

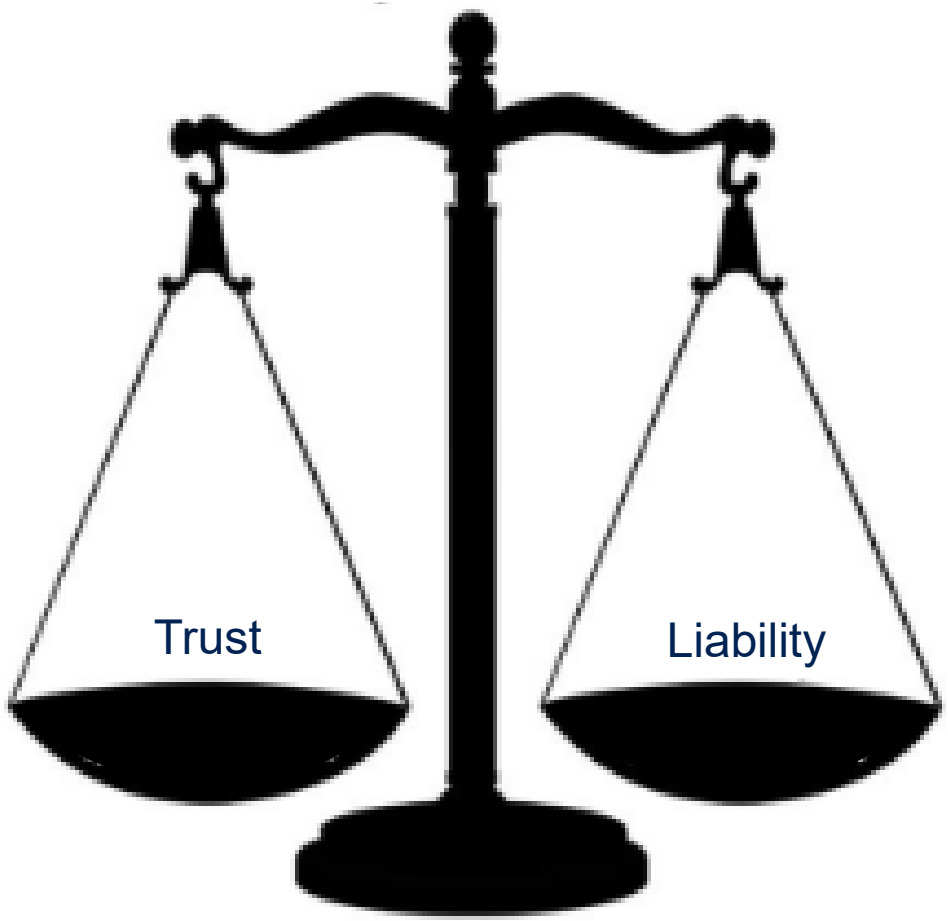


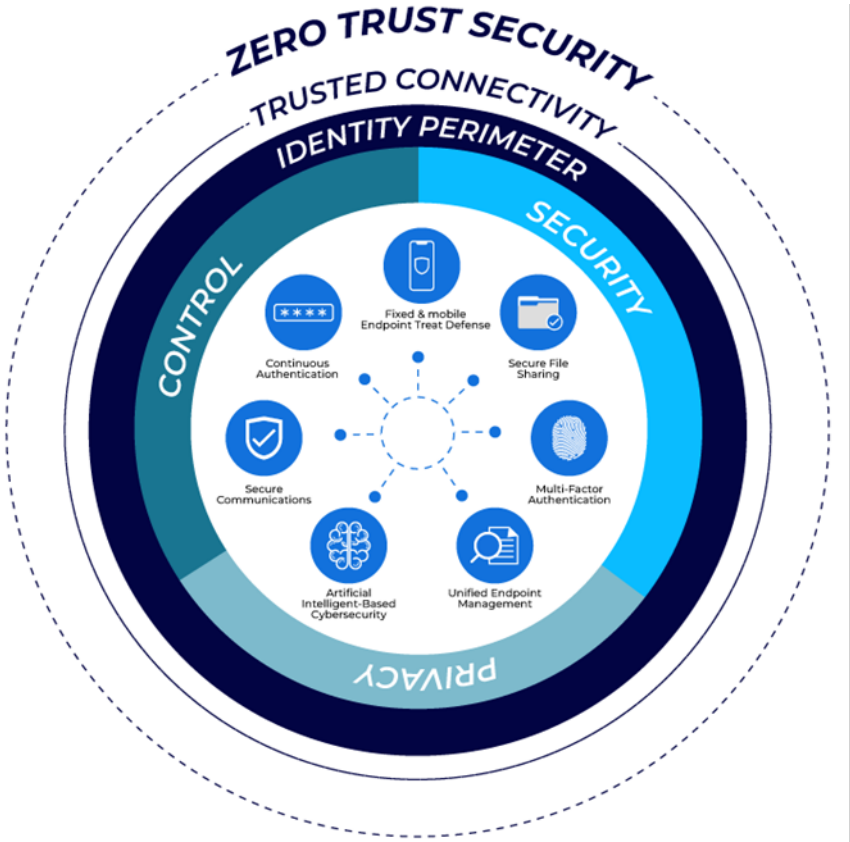


RoT = MIN (UUID & ROTK & SecBoot Auth Code)

WHY NOT JUST TRUST SUPPLY CHAIN SUPPLIERS (BROKEN CHAIN OF TRUST)?

Enterprise Business Risk Exposure





Safety, Data Privacy, Property Damage/Theft, Feature Availability, Brand Protection, Homeland Security,…

csrc.nist.gov/projects/cyber-supply-chain-risk-management

PROJECTS

Cybersecurity Supply Chain Risk Management C-SCRM

HOMELAND SECURITY

Intentional design vulnerabilities for HPSE backdoors—possible state sponsored attacks on critical infra

Overview

Latest updates:

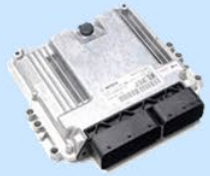
- Released SP 800-18r2, an Initial Public Draft (ipd) of Developing Security, Privacy, and Cybersecurity Supply Chain Risk Management Plans for Systems, for public comment. (6/04/2025)
- Completed errata update of Special Publication (SP) 800-161r1 (Revision 1), *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* to clarify NIST guidance on aspects such as vulnerability advisory reports and software bill of materials and fix errors like inaccurate numbering of control enhancements. (11/01/2024)
- Released SP 1326, an Initial Public Draft (ipd) of NIST Cybersecurity Supply Chain Risk Management: Due Diligence Assessment Quick-Start Guide, for public comment. (10/30/2024)
- Released SP 1305, Cybersecurity Framework 2.0: Quick-Start Guide for Cybersecurity Supply Chain Risk Management (C-SCRM). (10/21/2024)
- Updated the Cybersecurity SCRM Fact Sheet to include the most recent versions of key resources, guidance, and activities. (7/19/24)

IS ROT RELATED TO GLOBALPLATFORM & SESIP?

Answer: Yes. HPSE standardization paves the way for HPSE certification (e.g., CAL).

Today

- Fragmented hardware leads to unmeasurable security assurance levels
- Bespoke Pen Testing Today



SESIP Certification

Tomorrow

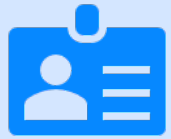
2026 GlobalPlatform ATF Objective:
SESIP for an existing ECU

- Certification using Cross-Vendor common SESIP HPSE profiles for automotive.
- Also differentiated by ECU category

HARDWARE ROT ENABLEMENT… OF WHAT?

HPSE RoT

Supply Chain Security



Identity & Access Management, Attestation Services

TRUSTED MOBILITY PLATFORM & ECOSYSTEM

Homeland Security (Auto + EV Grid +…) = Mobility Platform Security = Road User Security

Global Platform®

Securing the digital future

Q&A

→globalplatform.org