Global Platform™

Cybersecurity Vehicle Forum

June 20th, 2023

Global Platform™

Welcome!

Richard Hayton
Trustonic Ltd
Global Platform Chair Automotive Task Force
Global Platform Chair TEE Committee

Welcome!

Cybersecurity Vehicle Forum

OEMS

BUGATTI
CARIAD
mazda
CATERPILLAR
NAVISTAR
Ford
NISSAN MOTOR CORPORATION
GM
STELLANTIS
GENERAL DYNAMICS Land Systems
HONDA
VOLVO
JAGUAR LAND ROVER
VIA

Tier 1s

APTIV
Motional
BOSCH
MITSUBISHI ELECTRIC Changes for the Better
Continental
Panasonic AUTOMOTIVE
DENSO Crafting the Core
SUMITOMO ELECTRIC Connect with Innovation
ETAS
Quon Technology
GARMIN
SwRI SOUTHWEST RESEARCH INSTITUTE
HARMAN A SAMSUNG COMPANY
ZF INDIA ZF STEERING GEAR (INDIA) LIMITED
LUMINAR

Silicon & Solution Vendors

ANALOG DEVICES AHEAD OF WHAT'S P
STMicroelectronics life.augmented
Infineon
RENESAS BIG IDEAS FOR EVERY SPACE
SAMSUNG ELECTRONICS
Giesecke+Devrient

GP Solutions

NXP
PROVENRUN
Qualcomm
THALES Building a future we can all trust
TRUSTONIC

Test Labs

riscure Driving your security forward
TTL 財團法人電信技術中心 TELECOM TECHNOLOGY CENTER
UBIVELOX

Industry Organizations

AUTOSAR
SAE INTERNATIONAL
Global Platform™

Government

NIST
U.S. Department of Defense

Universities

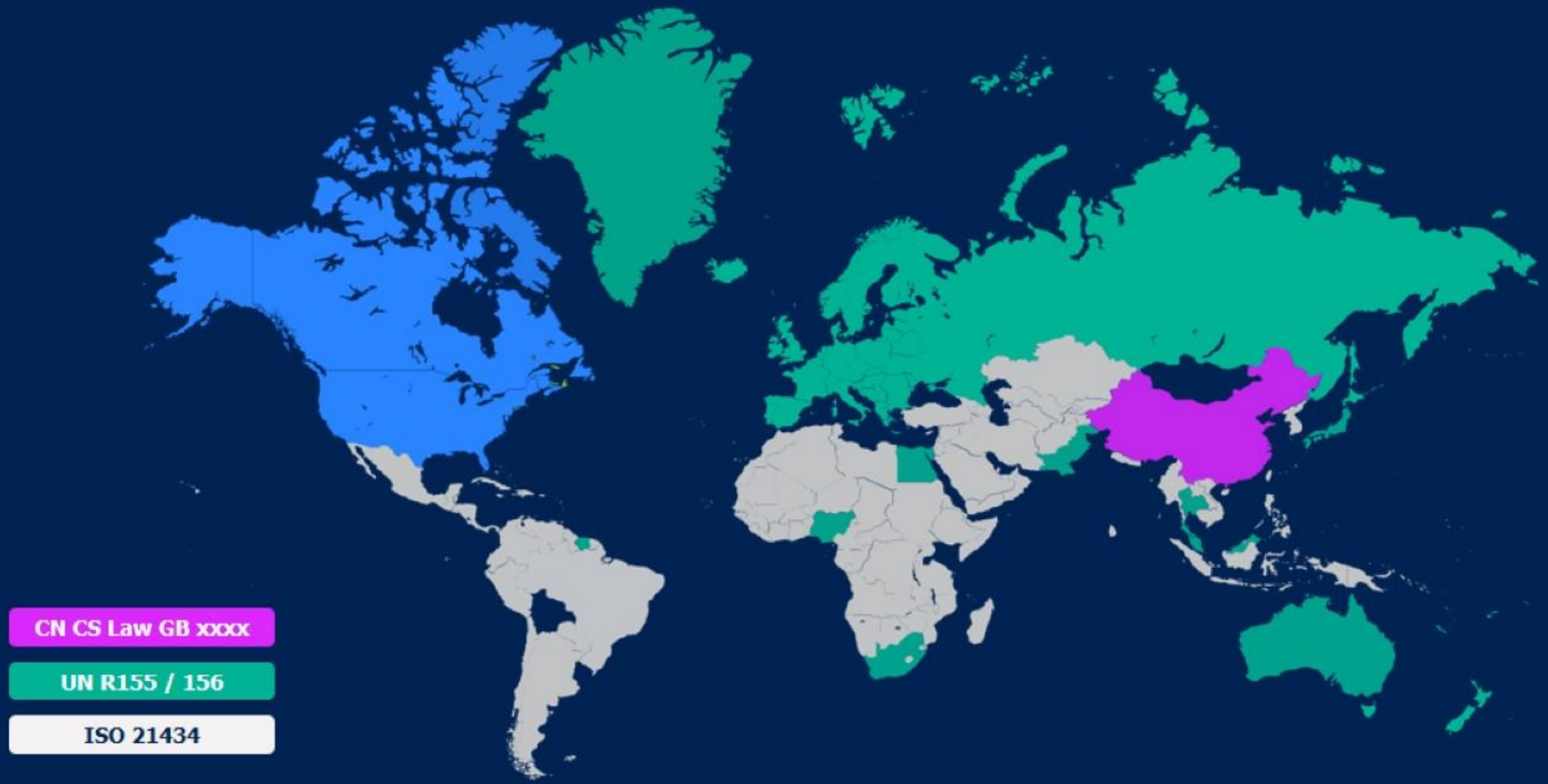
EASTERN MICHIGAN UNIVERSITY
Middlesex University

Broader Ecosystem

Applus laboratories
P3
CYBEATS
Rambus
CYBER PACK VENTURES
CYMOTIVE TECHNOLOGIES
PQ SHIELD
C2A security
Red Balloon Security
DEVICE AUTHORITY
INTEGRATING SECURE MOBILITY SOLUTIONS
EATON
SBD
flex
SONY
IOActive
High North Inc
TII Technology Innovation Institute
kaspersky
MIRA
unify
Mimer
utimaco

Global Platform™

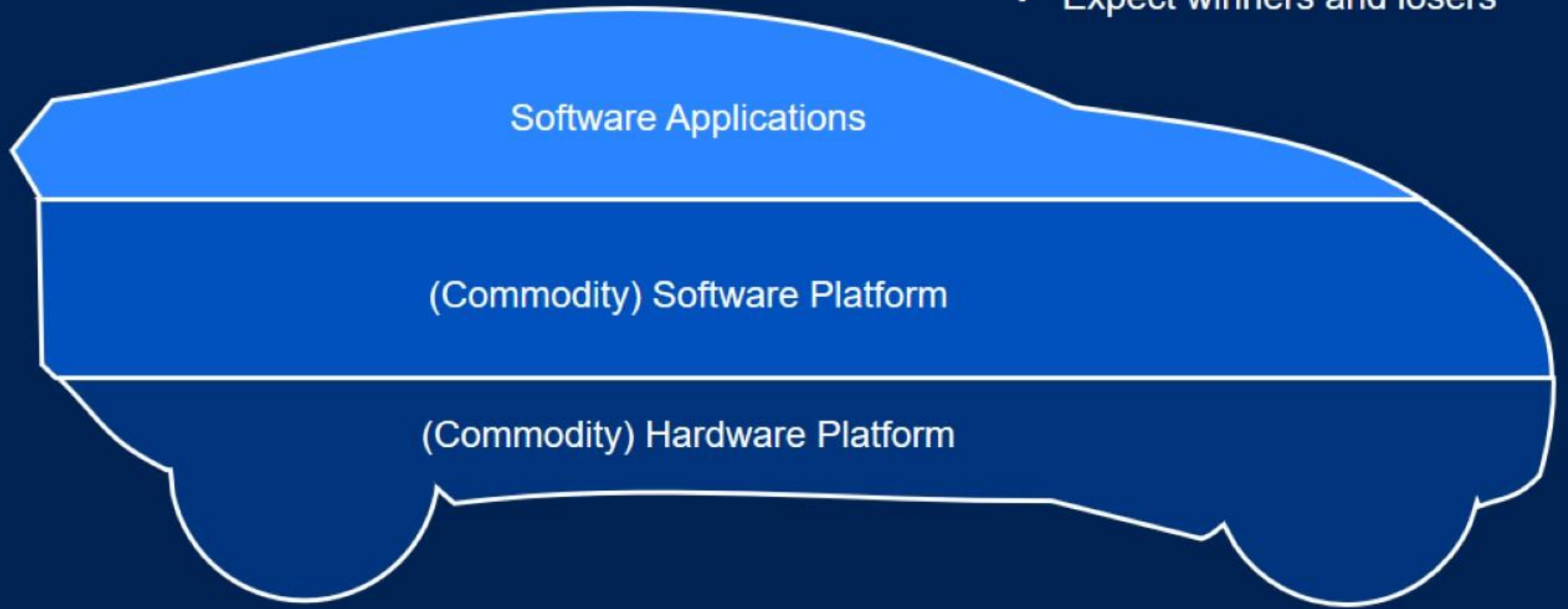
Global Regulation has changed the game



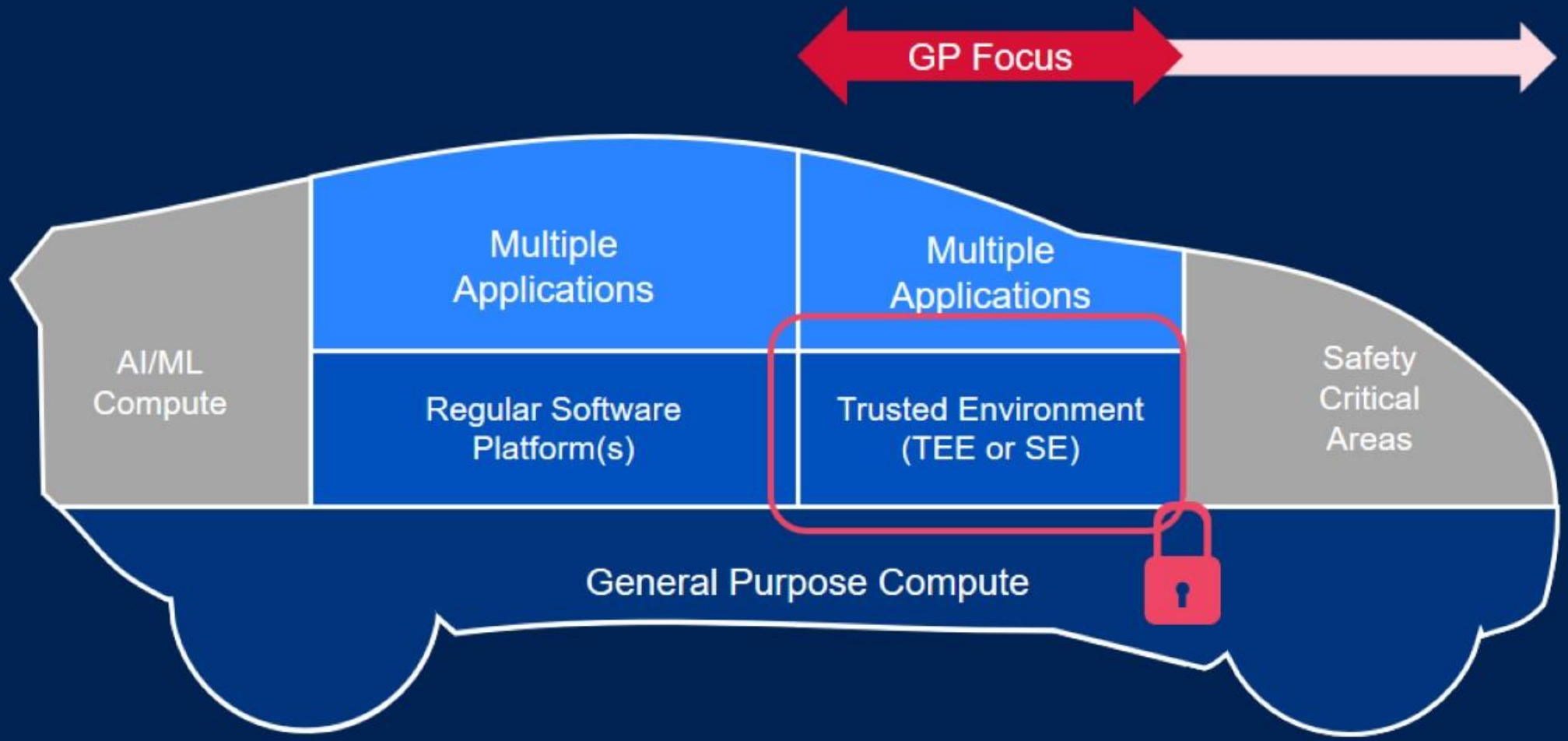
Software Defined Vehicles

Trend is accelerating

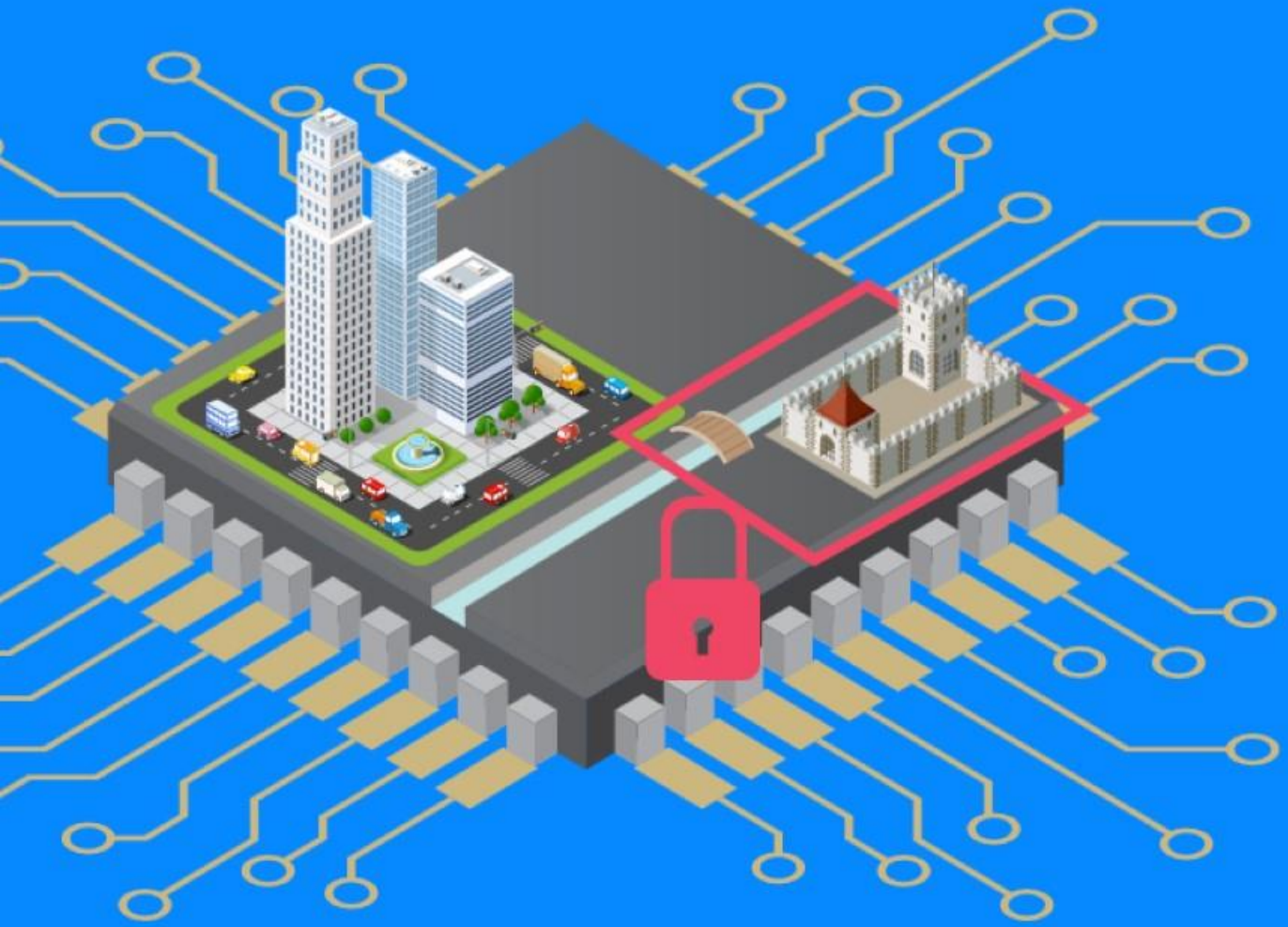
- Regulation requiring software updates
- Consumers expect up-to-minute tech
- Chip shortages highlighted problem of traditional approach
- Expect winners and losers



Global Platform Relevance



GlobalPlatform Trusted Execution Environment



- A secure operating system running on a standard CPU alongside regular OS/Applications
- Protected against attack by hardware chip features + software mechanisms
- Runs a full operating system providing standardized APIs and functions
- Commonly used in Mobile Devices, Automotive and IoT
- 3rd party Security Certification
- Full support for App and OS update over the air

GlobalPlatform Secure Element

- A secure enclave protected against physical and software attack
- Runs an embedded JavaCard OS providing standard APIs and functions
- Commonly used in SIM cards, Passports, Bank Card and embedded applications
- 3rd party Security Certification
- Full support for App and OS update over the air

GP Protection Profiles

Objectives

Set of security objectives and requirements for a category of products

- Independent from any specific implementation
- Reusable
- Enables the development of functional standards
- Helps in defining the security specification of a product

Requirements

A set of security requirements which are useful and efficient to satisfy identified objectives

Products will be tested to ensure they meet these requirements

Certification

Evaluated by an accredited Common Criteria (CC) lab

- The lab checks that the Protection Profile is consistent, i.e. requirements match the objectives, objectives are consistent with products and usage

Publication

GlobalPlatform Protection profile accessible from http://www.globalplatform.org/specificationsdevice.asp

The protection profile can then be used by 3rd party labs to validate a product meets the agreed security level

Common Criteria

SESIP

How Global Platform Works for Automotive

GlobalPlatform in Numbers 2022

Collaboration →

2600+

GlobalPlatform is driven by approximately 2600+ representatives from 90+ member companies

6 Task Forces

and 3 Sub-Task Forces

provide guidance on market sector and geographical requirements, trends, opportunities, and challenges

3 Technical Committees

manage the maintenance and evolution of GlobalPlatform's standardized technologies and certifications

Supported by 14 Working Groups focused on specific technology areas

34 Industry Partners

across the world, from international standards organizations to regional industry bodies

New Industry Partners welcomed this year include ioXt Alliance, Alliance pour la Confiance Numérique and CEN CENELEC

Standardized technologies →

100%

of SIMs and eSIMs rely on GlobalPlatform technology

as do most Android devices

More than **70bn**

GlobalPlatform-certified components are used in devices across market sectors, including payments, mobile connectivity and IoT.

Approximately 200 specifications and technical documents available

27

In 2021, we published 27 new specifications.

Global Platform™

Objectives for Today's Meeting

- What is are the biggest challenges?
- Where is the sweet spot in cross-industry collaboration ?
- How to Support Agility in Deployment of Solutions

Exchange

Increasing Understanding

Contribute to Supporting Needs

Opportunities for Cross-Industry Engagement

Determine Regional Needs

Agenda for Today

10:00	CyberSecurity Vehicle Forum	Welcome & Overview	Richard Hayton, Trustonic
10:30	Recent GlobalPlatform Activities	Automotive in GlobalPlatform	Francesca Forestieri, GlobalPlatform
10:45		Mapping of Secure Component Compliance to Hardware Protection Profiles	Gil Bernabeu, GlobalPlatform
11:15	Coffee Break		
11:45	Recent GlobalPlatform Activities	Trust Anchors & Roots of Trust Guidelines	Francesca, Forestieri, GlobalPlatform
12:00	Hardware Protected Security Environments	SAE and Autosar alignment	Philip Lapczynski, Renesas
12:30		Discussion on Common Areas for Cross-Industry Work	ALL
13:00	Lunch		
14:00	Forward Looking: Automotive Evolutions	ISO/SAE 21434	John Krzeszewski, Eaton
14:30		SESIP Evaluation Methodology and Automotive	John Boggie, NXP
15:00		An Overview of V2X Security Challenges	William Whyte, Qualcomm
15:30		Management of Post Quantum Crypto	Olivier Van Nieuwenhuyze, STMicroelectronics
16:00	Coffee Break		
16:15	Regional Considerations		Francesca Forestieri, GlobalPlatform
16:25	Brainstorming Priority Cross-Industry Work Items		All
16:55	Thank you and Close		Richard Hayton, Trustonic

Global Platform™

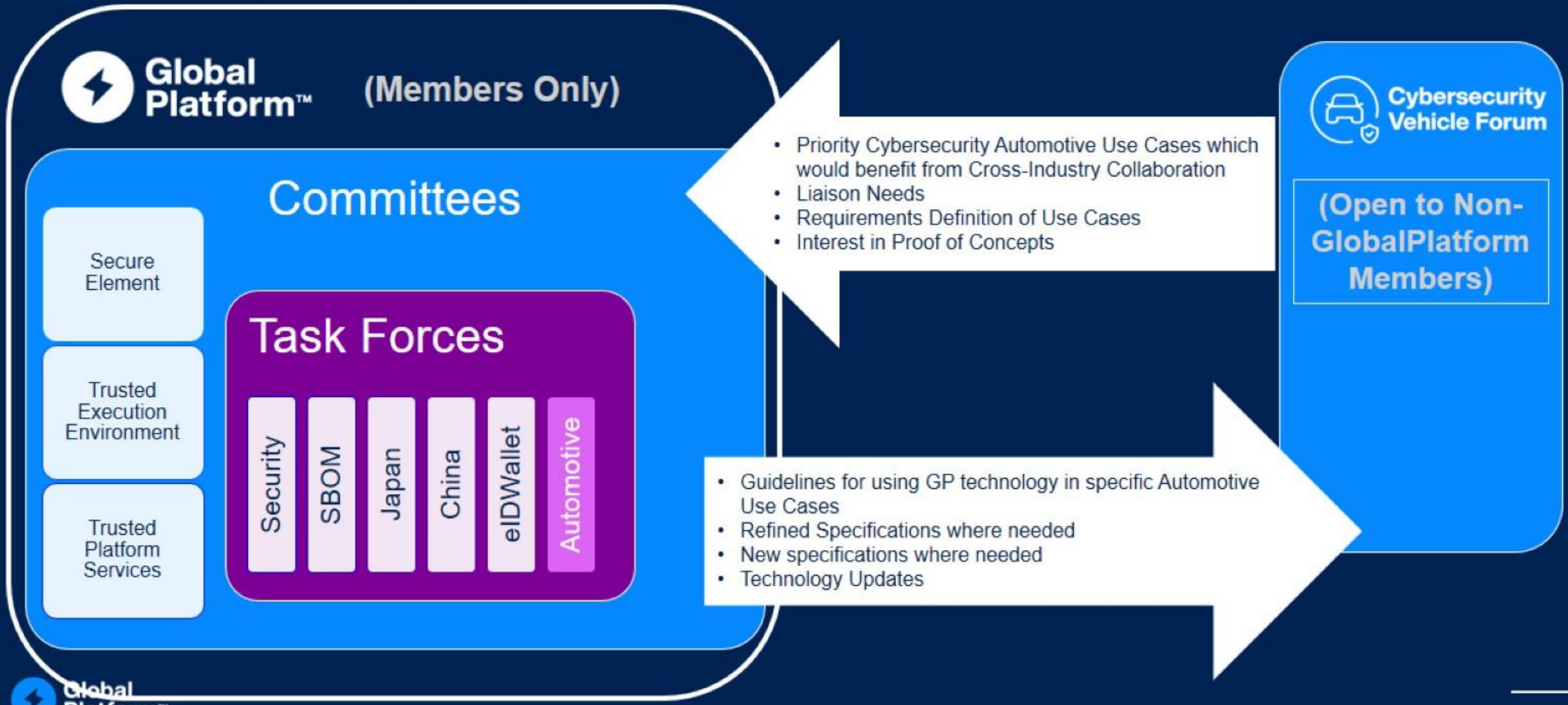
Global Platform™

Automotive in GlobalPlatform

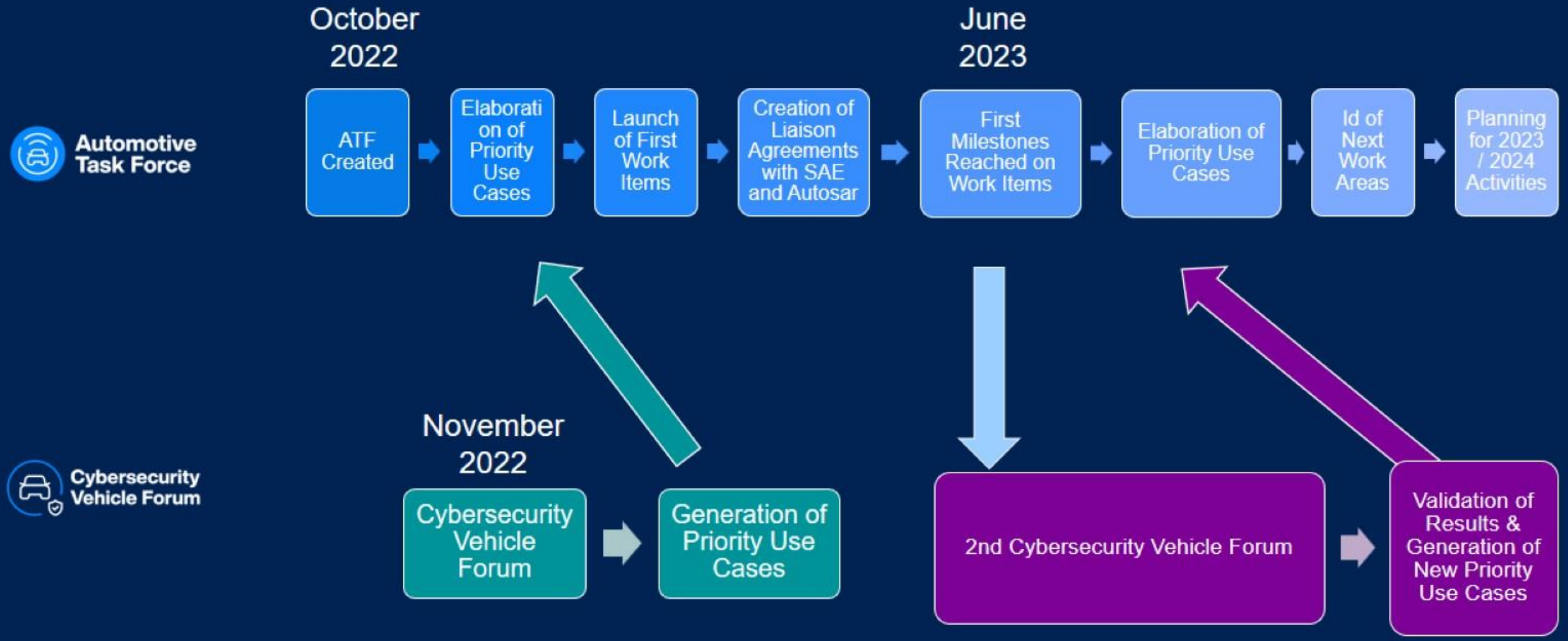
Francesca Forestieri
Global Platform Automotive Lead

Cybersecurity Vehicle Forum

GlobalPlatform's Engagement On Automotive



First 8 Months



Current Automotive Work Items

Choosing Solutions

- Guidelines on Roots of Trust and Trust Anchors
- Aligning GlobalPlatform with SAE Hardware Protected Security Environments J3101

Trusted Platform Service Tools for Automotive

- Standard APIs supporting communication across secure components

Demonstrating Compliance in Security for Automotive

- SESIP Evaluation Methodology
  - To generate artefacts for ISO 21434 demonstrating that products adhering to best practices in cybersecurity for automotive

Future Proofing

- Management of Post Quantum Migration

Global Platform™

Cybersecurity Vehicle Forum

Next Meetings

20th June Detroit/ Plymouth

- Prior to ESCAR USA & Uptane

September 14th – Tokyo Japan

- Timed during Automotive World Congress, Tokyo Japan

October 27th - YiZhuang, Beijing, China

- Timed during the China SAE Annual Conference**

November 14th - Hamburg, Germany

- Before European ESCAR

GlobalPlatform Strategy: How to Generate Industrial Impact

Alignment with Automotive "Standards" Alignment

- SAE
- ISO
- Autosar
- Car Connectivity Consortium
- JasPar?
- China SAE?
- Asia-Pacific Connected Vehicles Industry Association (ICCE)
- Smart Car Association Open Alliance (ICCOA)

Mapping of Alignment

- Identification of Areas where Specifications Need Updating to Reflect Automotive Specific Requirements
- J3101 Hardware Protected Security Environments Recommended Practice
- Autosar APIs

Develop Automotive Configuration

- Secure Element
- Trusted Execution Environment

Positioning of GlobalPlatform

- As a generator of artefacts on best practice alignment in support of ISO 21434
- Test Suites for J3101 compliance for SE and TEE
- SESIP as a security evaluation methodology

Possible Future Automotive Work Streams

- **Faster Deployment of GlobalPlatform Secure Components in Automotive**
  - Automotive Configuration
    - SE
    - TEE
  - Post Quantum Migration Discussions
- **Developing Open Source Facilitating GlobalPlatform Solution Usage**
  - Creating Trusted Platform Service Tools for Automotive
    - Standard APIs supporting communication across secure components
- **Tailored Services to Support Automotive Market**
  - Functional Certification & Test Suites for J3101
  - Training
- **Integrating GlobalPlatform Certification Tools into Vehicle Approval Processes**
  - SESIP Security Evaluation Methodology
    - To generate evidence for ISO/SAE 21434 demonstrating that products adhering to best practices in cybersecurity for automotive
  - GlobalPlatform Certification

Global Platform™

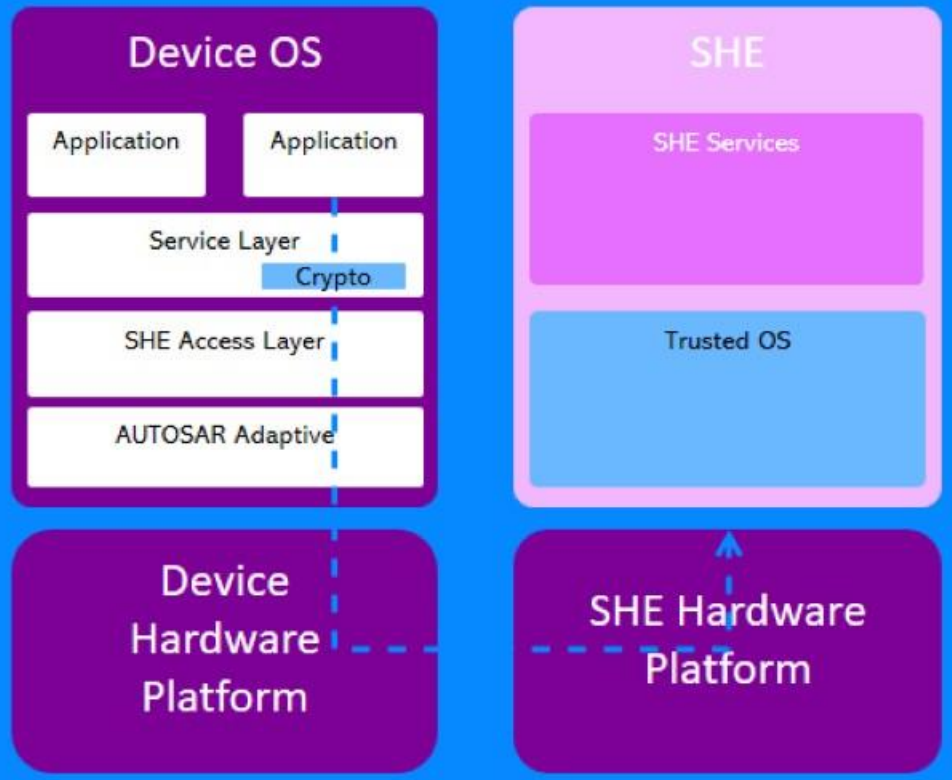
Recent Activities:

GlobalPlatform Secure Component Compliance to J3101

Gil Bernabeu
Global Platform CTO

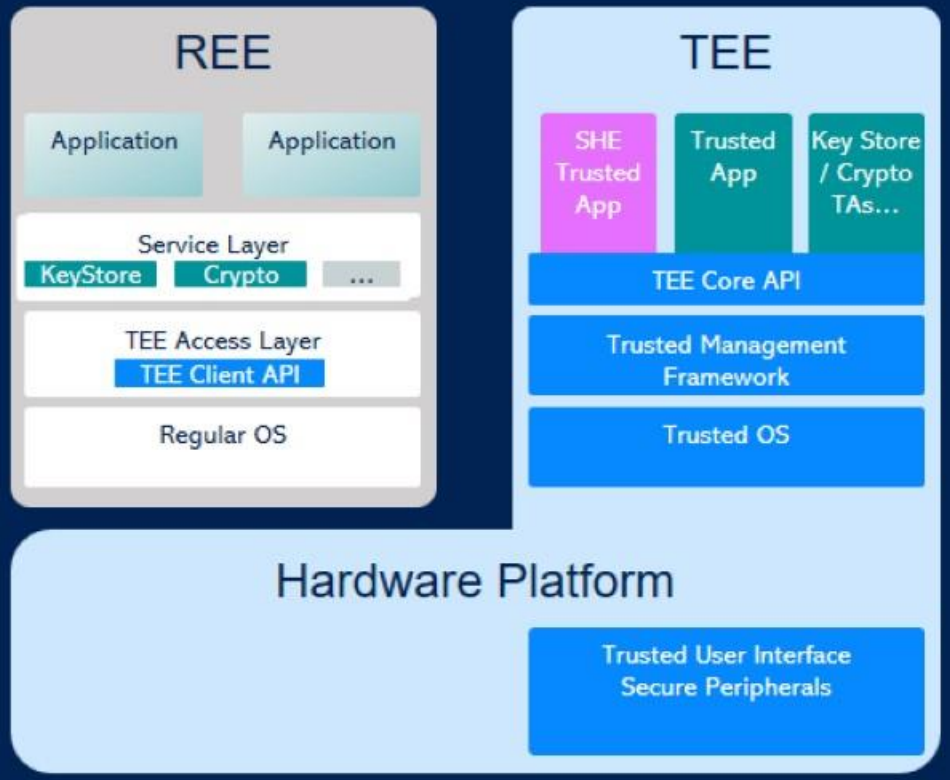
Automotive Task Force

Traditional Automotive Hardware Protected Environments (SHE++)



Traditional SHE Usage from AutoSAR

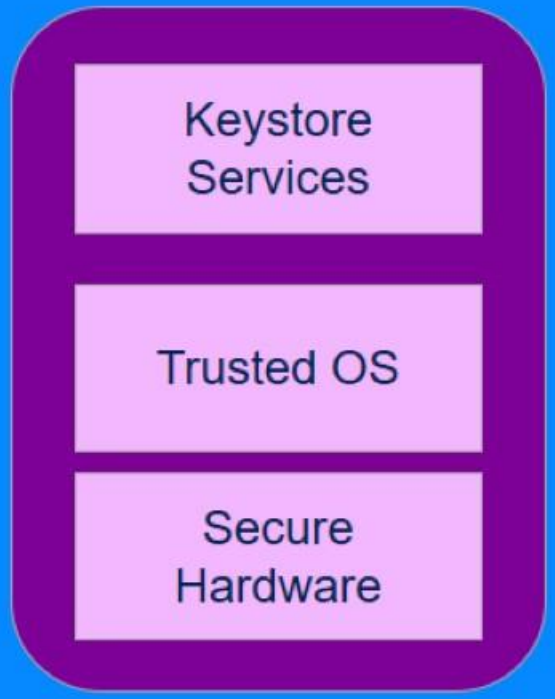
Evolution to GlobalPlatform Trusted Execution Environment



GlobalPlatform Trusted Execution Environment

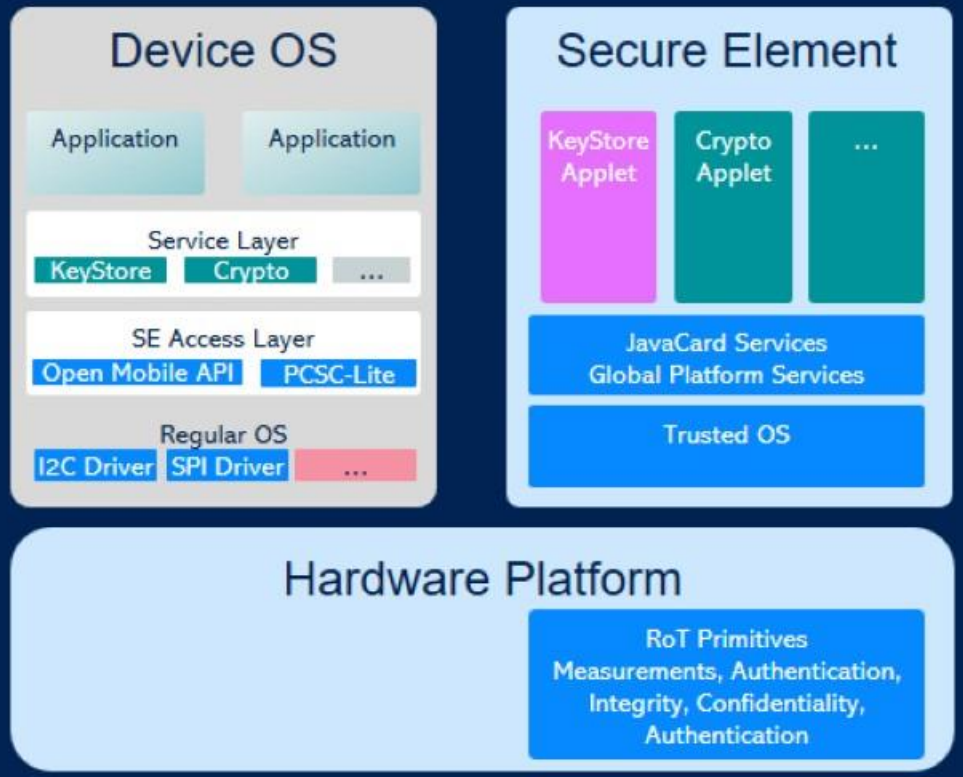
Global Platform™

Traditional Automotive Hardware Protected Environments (HSM)



Traditional HSM

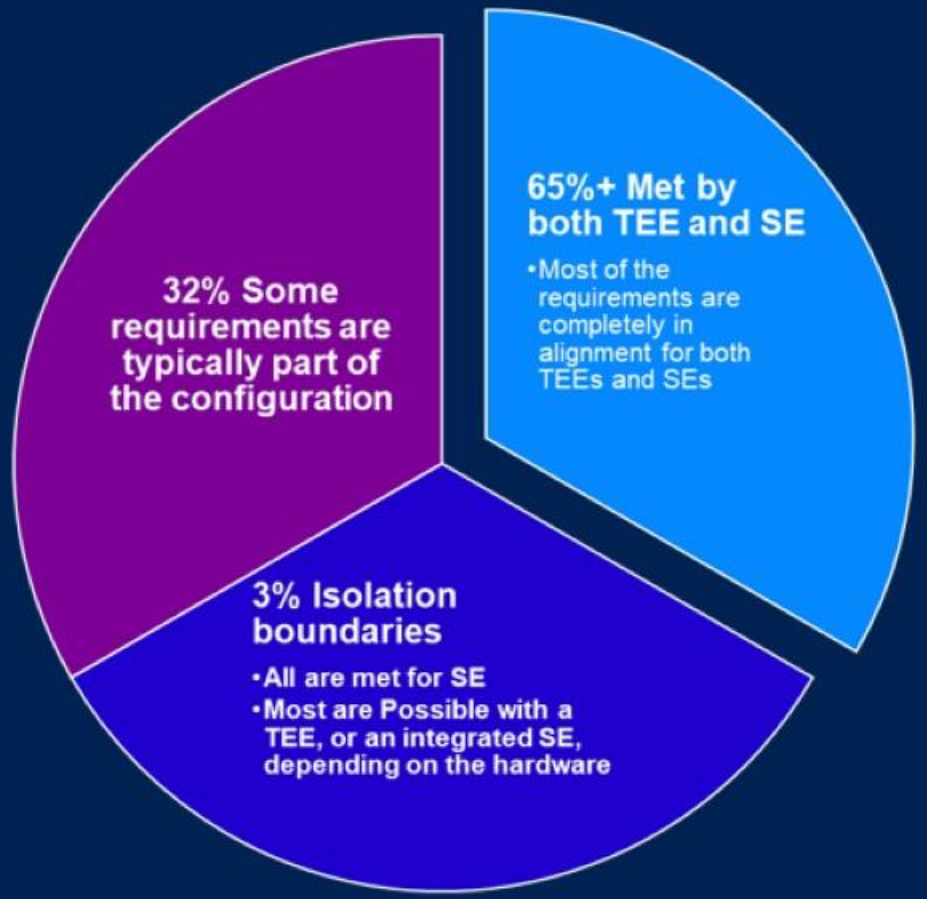
Evolution to GlobalPlatform Secure Element



GlobalPlatform Secure Element

Global Platform™

Analysis of J3101 Alignment with GP Specifications

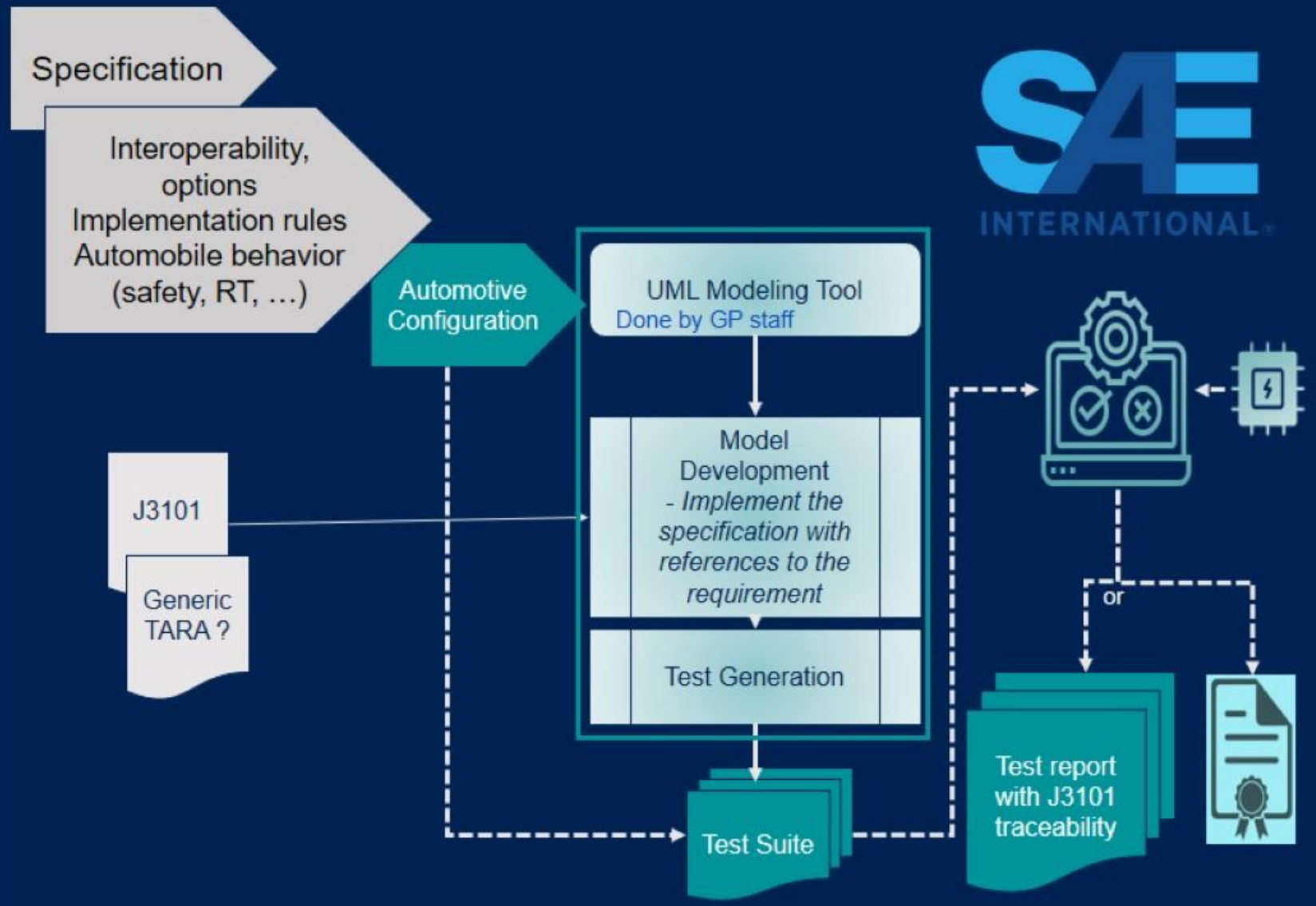


16% GP Specs more exacting

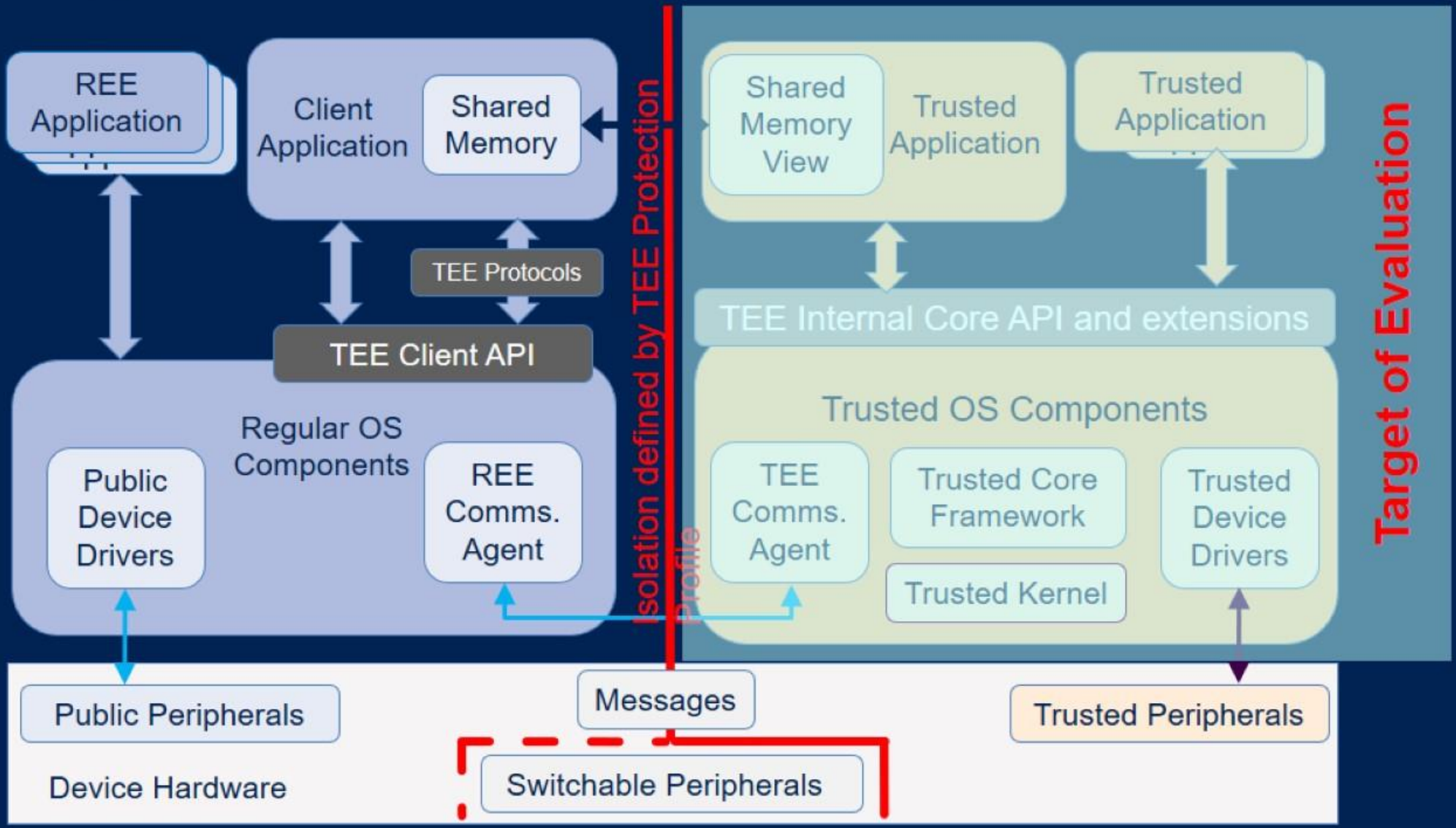
- Requirement Areas where GP specifications require significantly more stringent behaviour

Demonstrate Compliance to J3101:

GlobalPlatform Automotive Configuration for SE and TEE



The Target of Evaluation (TOE) (1 of 2)



The Target of Evaluation (2 of 2)

Includes	**Any hardware, firmware and software** used to provide the TEE security functionality, including debug mechanisms (specified in the Debug module)
	The guidance for the secure usage of the TEE after delivery
Does not include	The trusted applications
	The Regular Execution Environment (REE)
	The client applications

TOE Security Functionality (1 of 2)

TEE initialization process using assets bound to the SoC, that ensures the authenticity and integrity of the TEE code running in the device (implementation-dependent)

Authentication of TEE firmware and of TAs

Isolation of the TEE services, the TEE resources involved and all the TAs from the REE

Isolation between TAs and isolation of the TEE from TAs

Trusted storage of TA and TEE data and keys, ensuring consistency, confidentiality, atomicity and binding to the TEE

TOE Security Functionality (2 of 2)

Random number generator

Cryptographic algorithms

- Specified by the implementer in the Security Target
- Chosen from those in the GlobalPlatform APIs and/or algorithms used to provide security functionality, e.g. Trusted Storage

Monotonic TA instance time

Advanced TEE (rollback protection over resets)

- *Monotonic persistent time*
- *Full integrity protection of TA data, code, keys and TEE data*

Security Requirements (1 of 2)

Identifiers and device binders

- TEE identifier, unique and non-modifiable.
- TEE storage root of trust, unique, integrity- and confidentiality-protected, used to bind the stored data and keys to the TEE.
- TEE debug authentication key, integrity- and confidentiality-protected, used to authenticate for granting TEE debug access

TEE initialization code and data, integrity-protected

TEE runtime assets

- TEE firmware, authentic, integrity-protected, including protection against rollback
- TEE rollback detection data, used to detect rollback to previous versions of trusted storage
- TEE persistent data, authentic, integrity- and confidentiality-protected, bound to the device; includes TEE keys and TA properties
- TEE runtime data , integrity- and confidentiality-protected, includes random numbers generated by the TEE.

Security Requirements (2 of 2)

TA assets

- TA code, authentic, integrity-protected
- TA data and keys managed by the TA using TEE services, authentic, integrity- and confidentiality-protected, processed with atomicity, bound to the device.
- TA instance time, monotonic during TA instance lifetime including low-power states.
- TA persistent time, monotonic over TEE reset or TA shut-down.

Crypto assets

- RNG, unpredictable random numbers with sufficient entropy
- Other assets defined for each specific evaluation

Global Platform™

Recent Activities:

Guidelines on Trust Management in Automotive

Francesca Forestieri
Global Platform Automotive Lead

Automotive Task Force

Trust for Secure Automotive Services

Trust for Secure Automotive Services:
Roots of Trust, Chains of Trust, and Trust Anchors

Objectives

- How GlobalPlatform technologies support the evolving requirements in trust management of automotive

Target Audience:

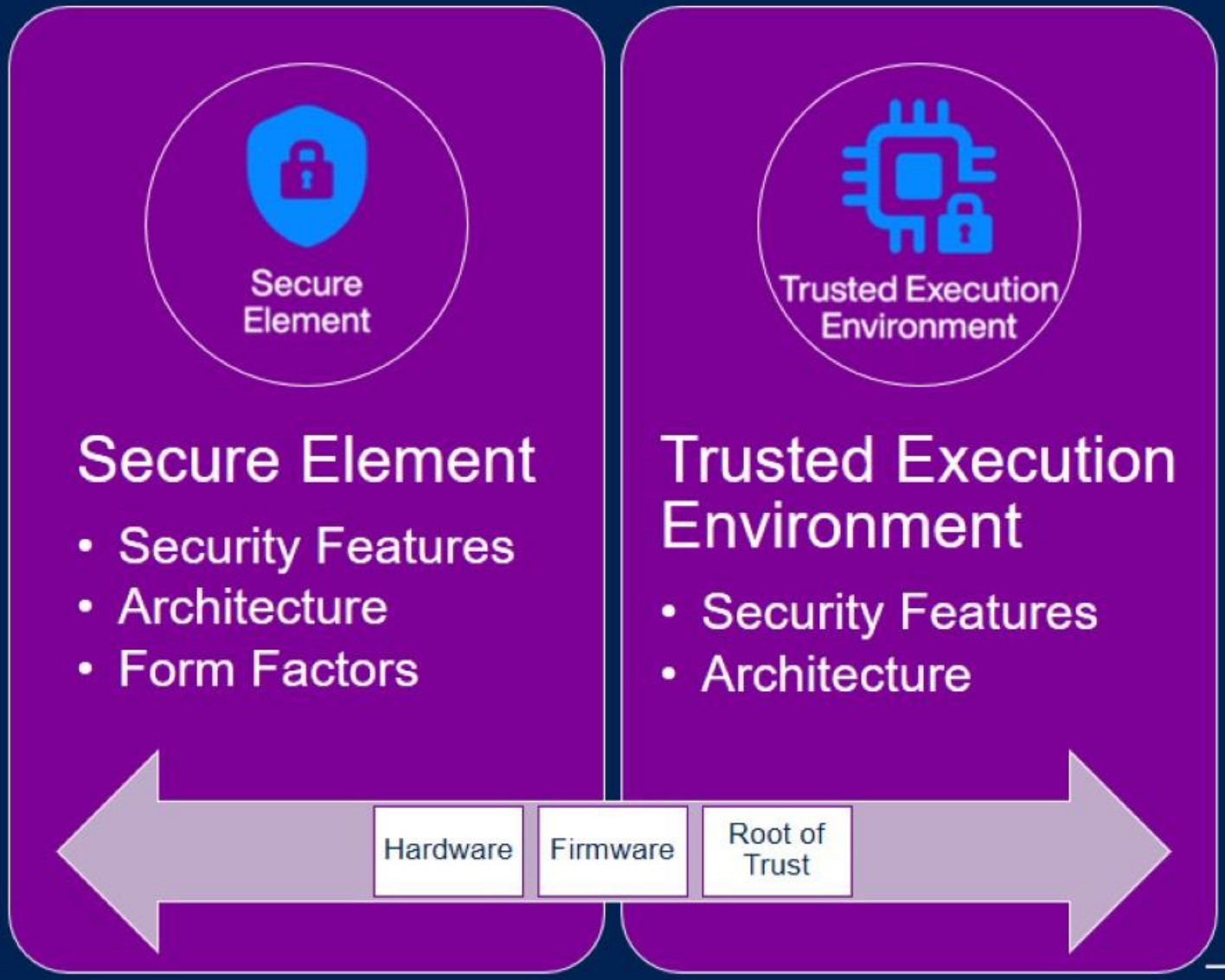
- Automotive Value Chain
- Secure digital services and device producers

Whitepaper Table of Contents

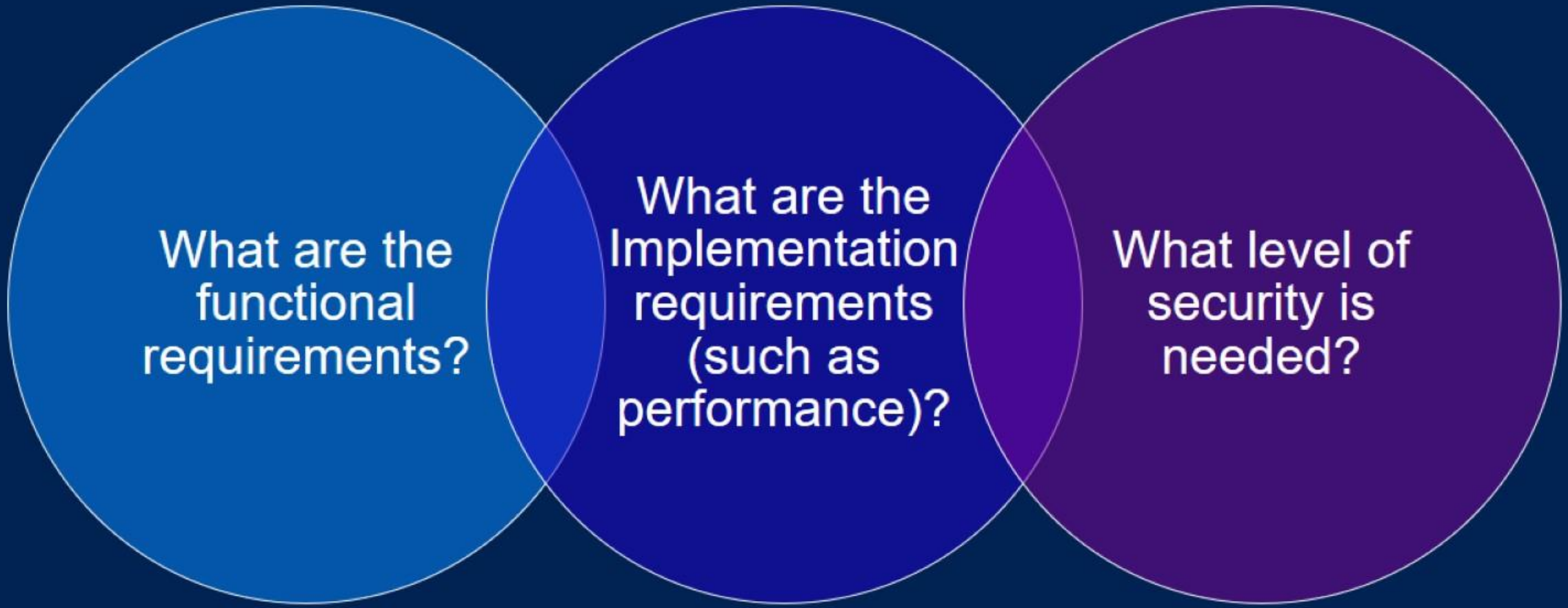
GlobalPlatform Security By Design

GlobalPlatform Solutions Supporting Trust Management

Trust Anchors



Selecting Secure Components

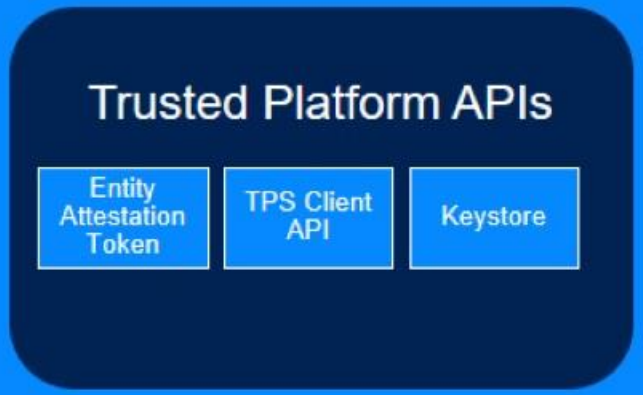


Comparing Trust Anchors: Pros and Cons

			SE		TEE	
			OS	Applet	OS	Trusted App
Functional Requirements	General Purpose or Special Purpose		General	Special Purpose	General	Special Purpose
	Root Of trust		Yes	Yes	Yes	Yes
	Key Management		Yes	Yes	Yes	YEs
	Application Management		Yes		Yes	
	Life cycle and Ownership management		Yes		Yes	
	Communication services		Yes		Yes	
	Over the Air Updates		Yes		Yes	
	Additional Secure Services Supported			Yes		Yes
	Standardized APIS		Yes	Yes	Yes	Yes
	Functional Certification		Yes (GP)	Multiple	Yes (GP)	Some
Implementation requirements	Performance	Security	Tamper resistant		Hardware protection	
		How many cores	Mono core		CPU/Multi Core	
		How much memory	Small		Large	
		How much power	Small		Flexible	
Level of Security	Protection Profile	Scope	SE PP (OS) based on HW PP		TEE PP & mCU-RoT PP (SW and HW boundary)	
		Security Target template	Yes		Yes	
		Attack (incl. Side channel)	Catalogue is managed by SOG-IS - Jhas		Catalogue is managed by GlobalPlatform	
	Robustness	VAN level	Minimum EAL4+ with AVA_VAN.5 (High attack resistance for HW and SW)		Minimum EAL2+ with AVA_VAN_AP.3 (Enhanced-basic attack resistance for HW and SW)	
	Certification		Yes (GP simplified and CC)		Yes (GP simplified and CC)	

Global Platform™

Additional Security Resources 1/2



Device Access to Secure Services

Trusted Platform Services

Provides universal access to secure services between Rich EE and device application

Enables Trust between a device and IoT Service Provider

- Allows a Service Provider to:
  - Determine what a device is and how it is configured
  - Provisions key material to a device
  - Establishes how a device should behave

Provides data confidentiality, integrity and privacy as appropriate

Interoperability with Proprietary Solutions possible

Additional Security Resources 2/2

SESIP: *Security Evaluation Methodology*

CEN/ CENELEC Standard EN 17927

SESIP

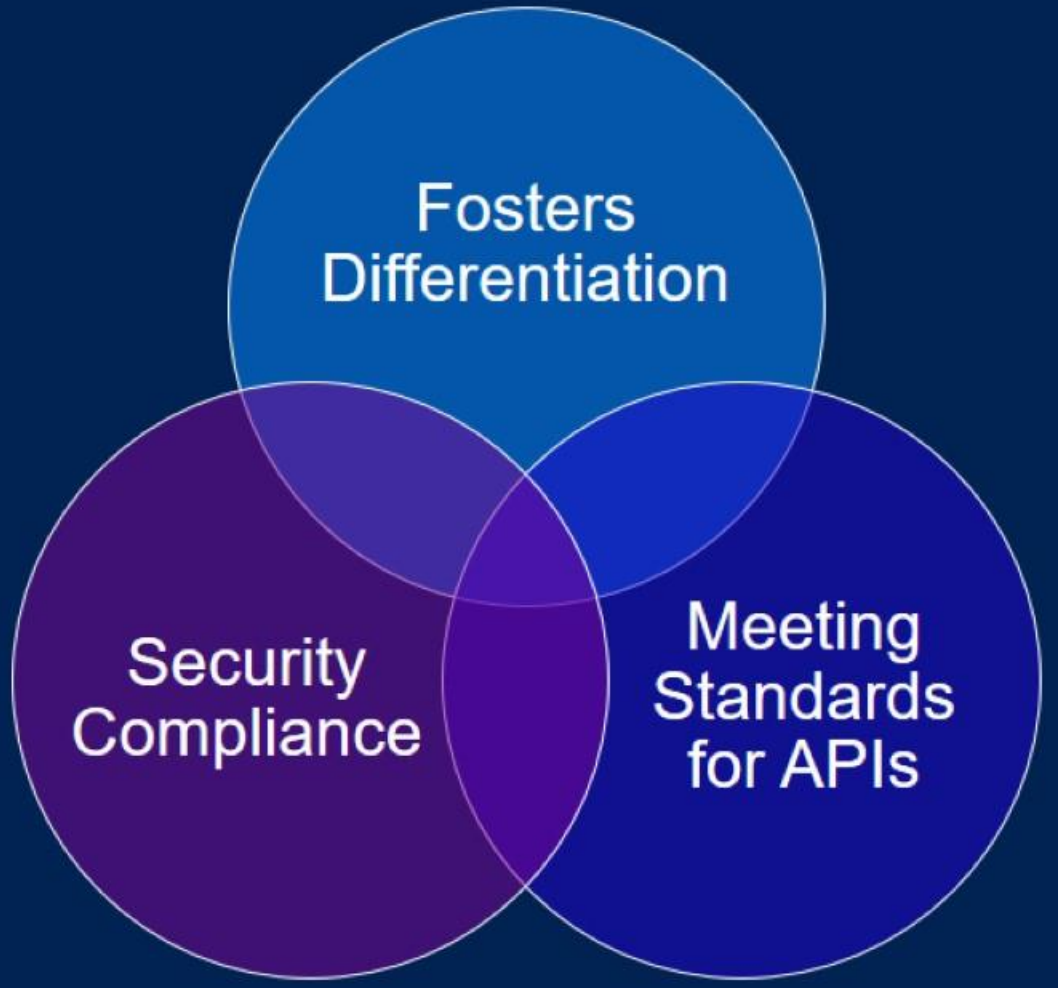
Designed to not require security expertise for use

Address Device/ Component Security

Provide Vulnerability Assessment

Conclusions

GlobalPlatform Supporting Automotive Security Deployments



Global Platform™

Hardware Protected Security Environments

Philip Lapczynski, Renesas

HARDWARE PROTECTED SECURITY ENVIRONMENT

ANALYZING APIS IN THE CONTEXT OF SAE J3101

Philip Lapczynski
Renesas Electronics America, Inc
Automotive Core Technology – Security (ACTS)
2023-06-20

BIG IDEAS
FOR EVERY SPACE

RENESAS

RENESAS
BIG IDEAS FOR EVERY SPACE

Whoami

Phil Lapczynski

Principal Engineer - Automotive Security
2017-present: Renesas Electronics America, Inc.
2006-2017: Led bootloader and OTA team at Vector North America

Other Activities:

- Uptane Advisory Group Member and GSoC Mentor
- SAE Vehicle Electrical Hardware Security Task Force Member
  - Sponsor for J3101-1 Information Report
- SAE Vehicle Electrical System Security Committee Member
- Auto-ISAC Product Working Group Member
- CyberTruck/CyberAuto Challenge Mentor / Instructor
- University of Detroit Mercy - Adjunct professor for Secure Vehicle Embedded Systems course (VCE 5400)

HOW TO BUILD A ROOT OF TRUST WITHIN EMBEDDED SYSTEMS?

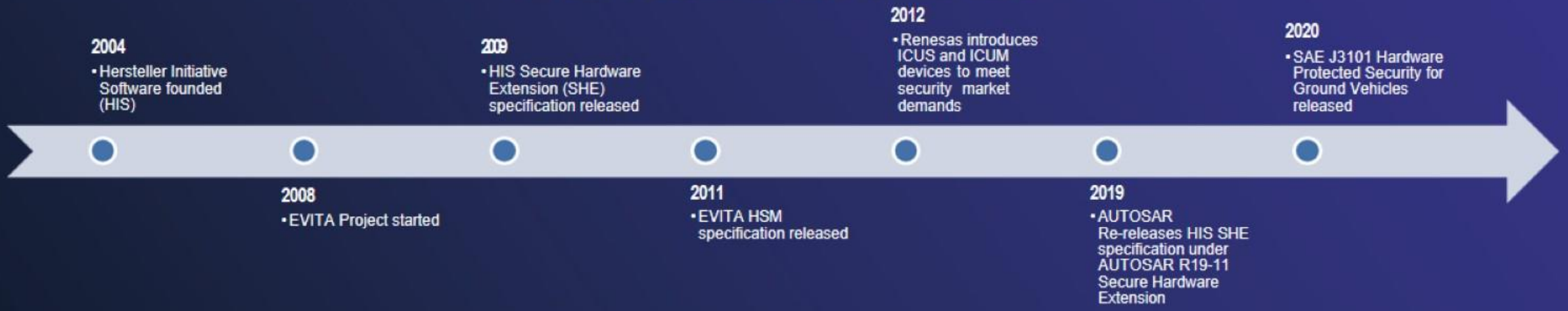
RENESAS

HARDWARE PROTECTED SECURITY ENVIRONMENTS

HARDWARE PROTECTED SECURITY ENVIRONMENT HISTORY

Automotive hardware protected security environments have been evolving for over a decade. First introduced by the **Hersteller Initiative Software (HIS)** group, the **Secure Hardware Extension (SHE)** has become the baseline set of requirements for automotive security peripherals. **EVITA HSM** and **SAE J3101** build and expand on the concepts released in the HIS SHE spec.

Timeline of automotive security standards



SAE J3101 – HARDWARE PROTECTED SECURITY ENVIRONMENT

Released in February 2020, SAE J3101 took a new approach to automotive hardware security, focusing on defining primary and application use cases and defining the requirements needed in an HPSE to fulfill these goals.

Primary Use Cases

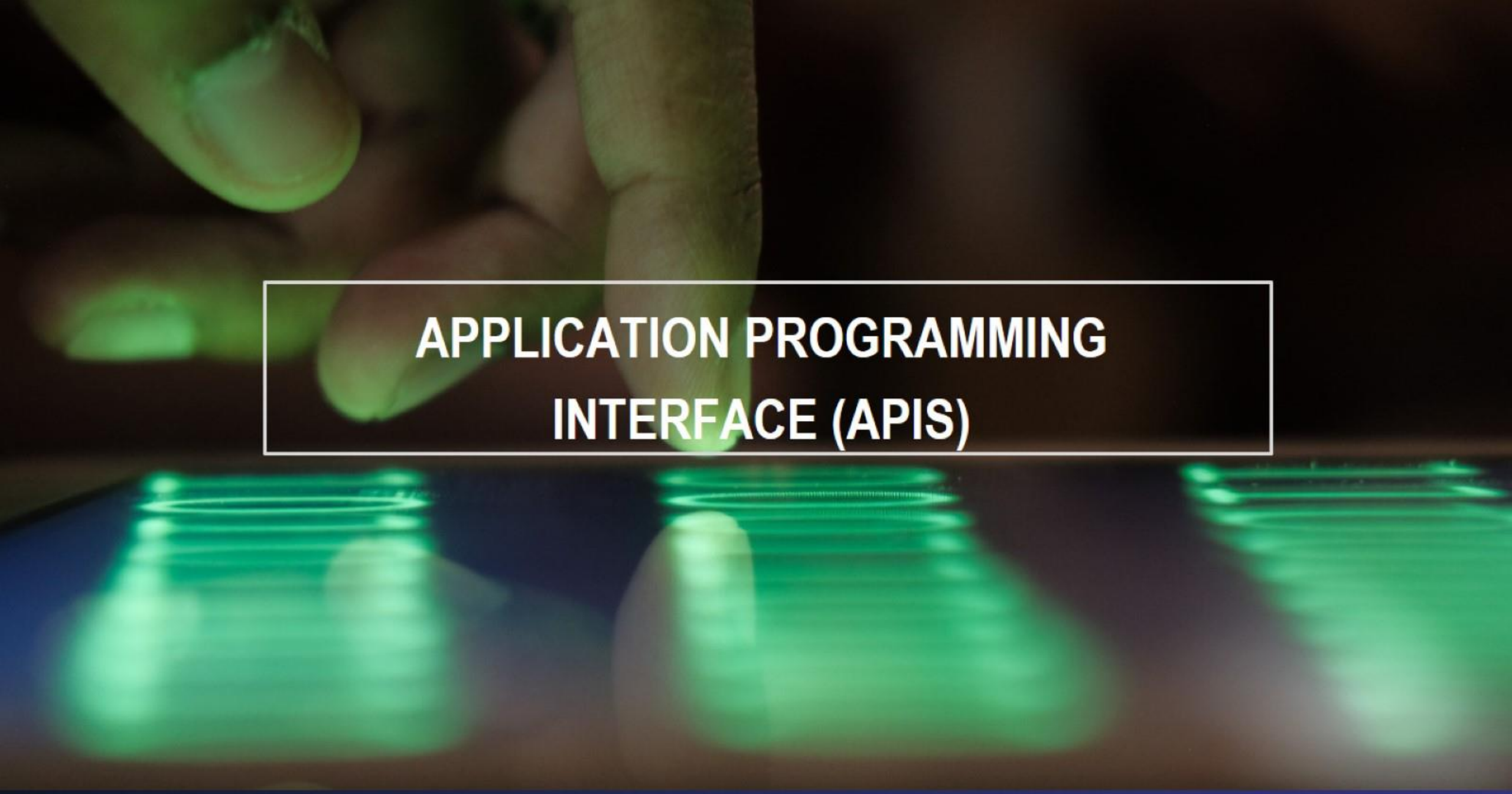
- Authenticated boot
- Authenticated update
- Secure in-vehicle messaging
- Access mechanisms
- Secure storage

Application Use Cases

- Intellectual property protection
- Secure diagnostics
- Secure logging

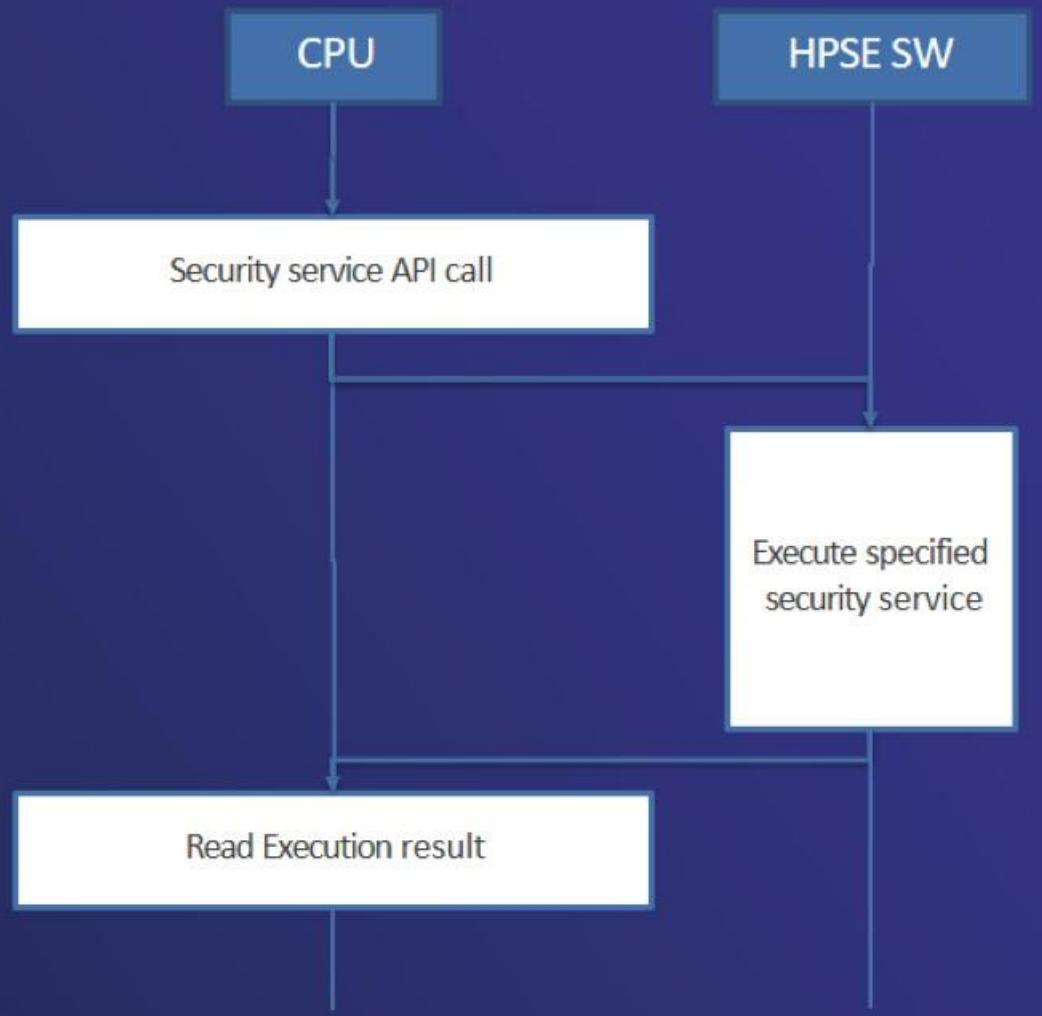
Common Requirements

- Cryptographic key protection
- Cryptographic algorithms
- Random number generator
- Secure nonvolatile data
- Algorithm agility
- Interface control
- Secure execution environment
- Self-tests

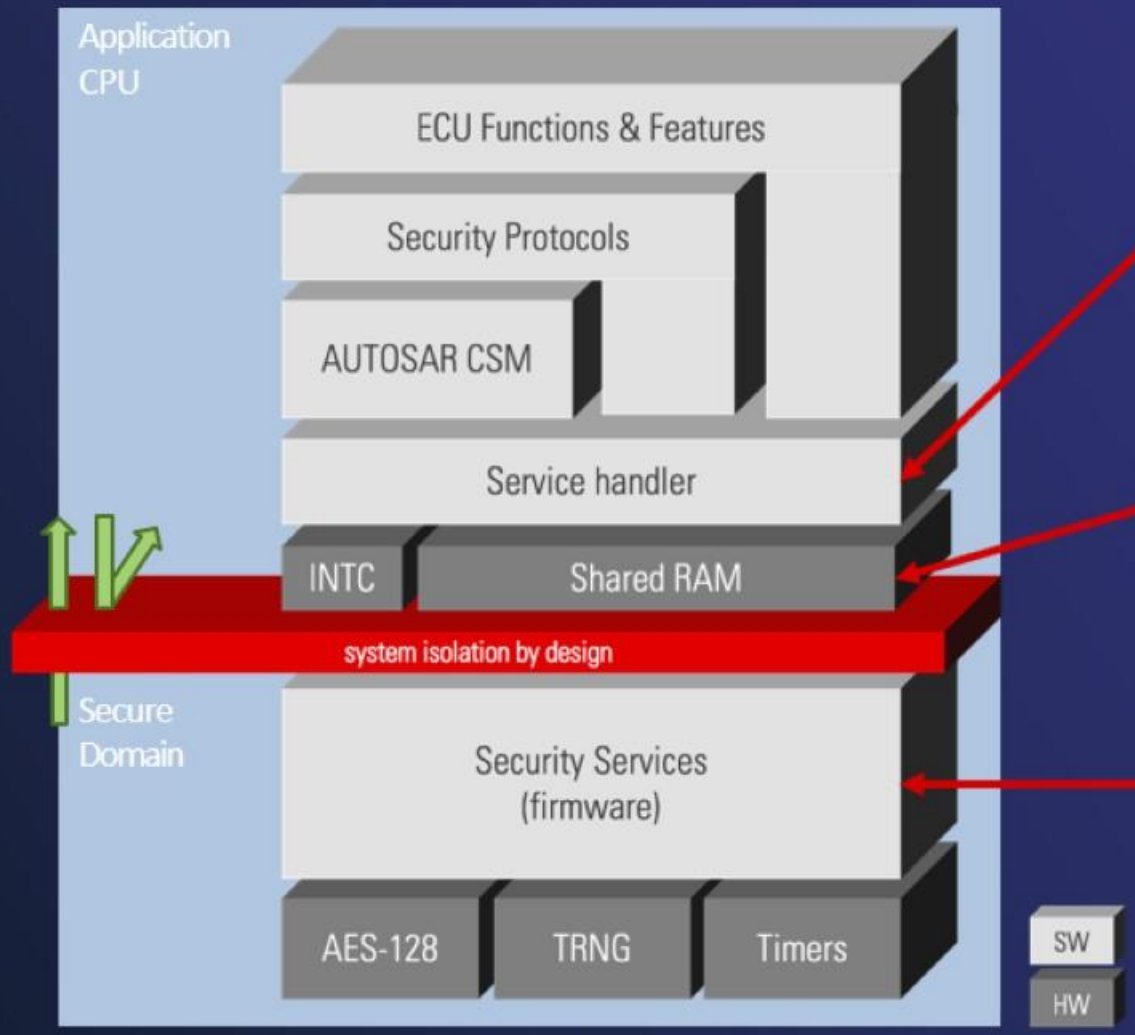


HPSE OPERATION CONCEPT

- ICUM is security sub-system that consists of CPU and cryptographic engine that can access a shared security mailbox
- The host CPU makes a service API call and triggers an interrupt in the ICUM firmware



HPSE FIRMWARE: SYSTEM OVERVIEW

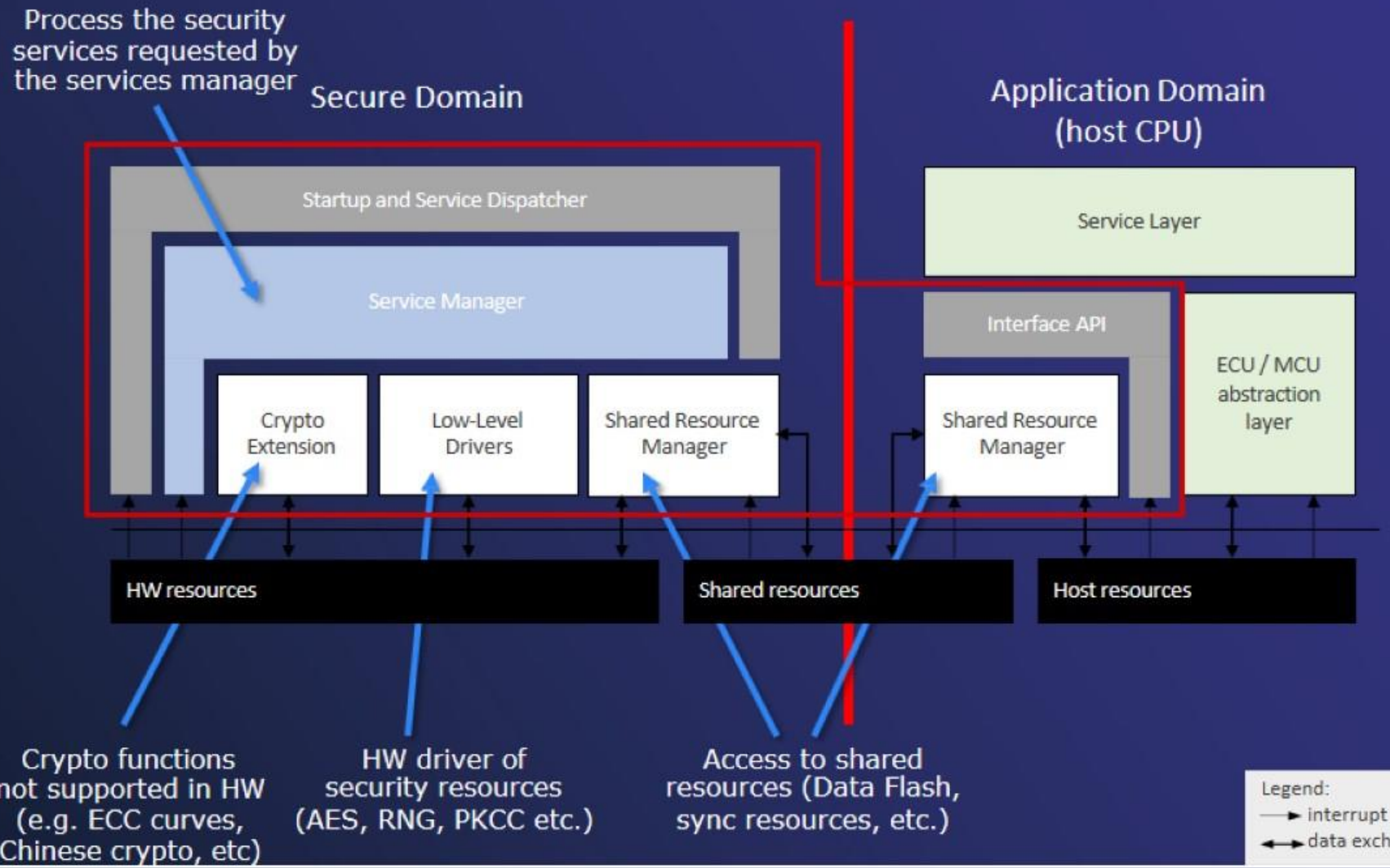


Application API to handle the service requests and response

Used to:
- Post security service requests
- Retrieve results after processing

The core of the security services

HPSE FIRMWARE ARCHITECTURE



SAE J3101-1 INTRODUCTION

WIP 2022-10-25

Gap Analysis Report: SAE J3101 API Requirements and AUTOSAR Classic Platform Crypto API Version R21-11 J3101-1

The scope of the report is a gap analysis between J3101 requirements that require an API and the API functions described in common automotive security APIs. AUTOSAR Crypto Driver R21-11 was chosen as the first interface to analyze.

Currently unavailable for purchase at this time

This Standard is currently a WIP.

Related Info

Issuing Committee: Vehicle Electrical System Security Committee

Rationale: In order to understand the existing software API landscape for J3101 devices, the SAE Vehicle Electrical Hardware Security Task Force completed a series of gap analysis on several common automotive relevant crypto APIs. The intent is to understand the coverage of J3101 requirements by existing APIs and highlight the gaps in coverage.

Related Topics:

ELECTRICAL SYSTEMS

Also known as: SAE J 3101-1

RENESAS

RATIONALE

The purpose of this information report is to…

- Provide an analysis and summary of the coverage of J3101 requirements by existing Application Programming Interfaces (APIs)
- Identify areas of coverage within these APIs
- Highlight any gaps in coverage that need to be addressed
- Inform and guide future development efforts in this area.

METHODOLOGY – REQUIREMENTS CATEGORIZATION

All J3101 requirements were extracted into a tabular database for analysis. Requirements were categorized into 4 categories related to software API:

Category	Description
API Impact	This requirement impacts API design choices
API Required	This requirement requires dedicated API support
Implementation Specific	This requirement may need support within an API, however it may be specific to an individual implementation of an HPSE or API design
Internal	This is a requirement internal to the HPSE firmware or hardware. No external API required

METHODOLOGY – API ANALYSIS

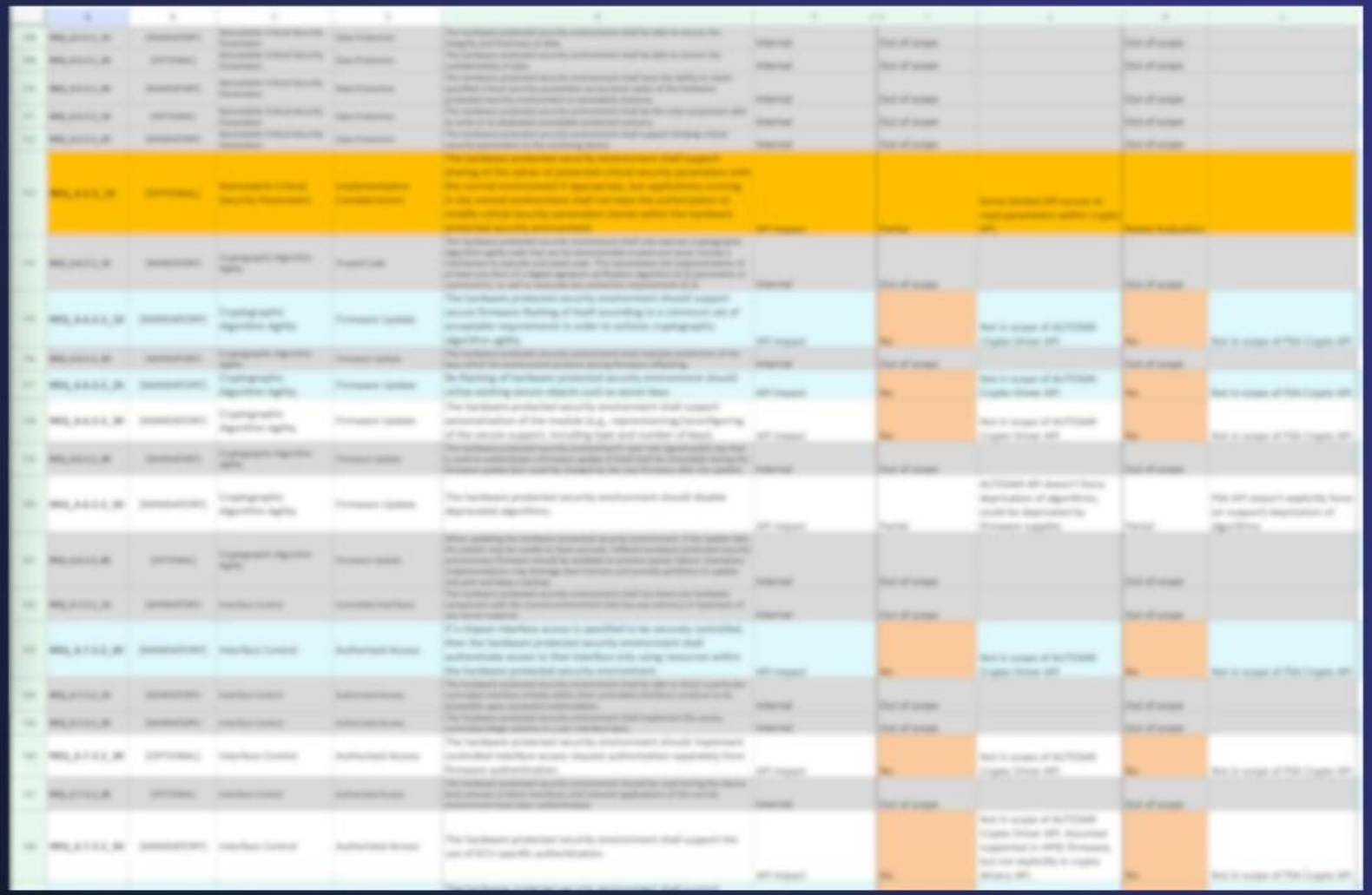
The committee working group analyzed each J3101 requirement against the assessed specification categorizing the API coverage into the following 3 categories: Yes, Partial, and No. The categories are described in the following table.

Requirement Category	Description
Yes	This J3101 requirement is fulfilled by the assessed specification
Partial	This J3101 requirement is partially fulfilled by the assessed specification. The details of this choice are included in the comments section for each requirement.
No	This J3101 requirement is not fulfilled by the assessed specification.

METHODOLOGY – ASSESSED API SPECIFICATION

Initial assessed API specification was AUTOSAR Classic Platform Crypto API Version R21-11

METHODOLOGY – REQUIREMENTS ASSESSMENT



Reviewed each J3101 requirement in the context of the assessed API

J3101 REQUIREMENTS ANALYSIS

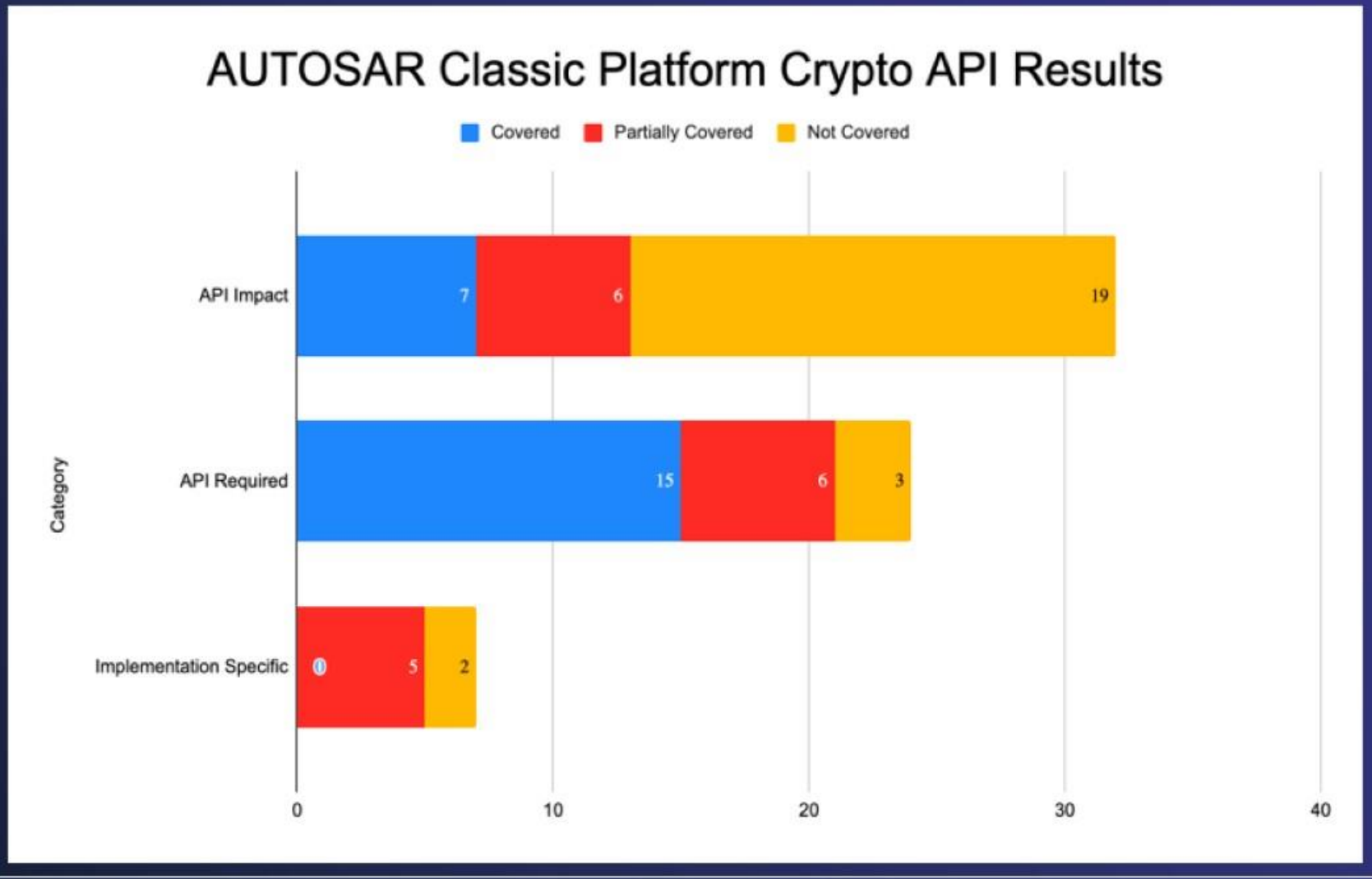
- 33 API Impact
- 25 API Required
- 7 Implementation specific
- 94 Out of API scope

INTERPRETING RESULTS

In the case of non-covered requirements, the report intends to give practical guidance on why the requirement was deemed non-covered. For example, REQ_6.2.3.7_100 was deemed not covered with the comment that “Device lifecycle is out of scope of the AUTOSAR [crypto] API. To implement a device lifecycle, additional logic is needed.”

In the case of partially covered results, an effort is taken to describe the covered (or non-covered) parts of the requirement.

ANALYSIS RESULTS



BALLOTING

We are currently in the process of bringing J3101-1 up for feedback and voting from the TEVEES18 parent committee.

NEXT STEPS

We intend to update the J3101-1 information report to add additional analyzing APIs. Next, we will be focusing on Global Platform APIs.

Global Platform™

ISO 21434

John Krzeszewski, Eaton

Current ISO/SAE JWG status & potential synergies with GlobalPlatform

John T. Krzeszewski

June 20, 2023

Powering Business Worldwide

Agenda

- Common Criteria for automotive (ISO/IEC AWI 5888)
- SAE/ISO Joint Working Group (JWG)-projects & status
  - Summary
    - Cybersecurity Assurance Level (CAL)
    - Verification and validation
    - Targeted Attack Feasibility (TAF)
- Possible synergies with GlobalPlatform (GP)

ISO/IEC AWI 5888 JWG6 5888 - Common Criteria for automotive

ISO/IEC 5888 summary

- Goal is application of common criteria for automotive
  - Leveraging ISO/IEC 15408 framework (intended for IT)
- Stalled due to disagreement in scope between ISO & IEC
  - Initial proposals included most automotive systems
  - Subsequent proposed to limit scope
    - Suggest only applying if significant benefit and not duplication of effort
      - E.g., existing CC profiles, GlobalPlatform, etc.
- Project will most likely be halted

Powering Business Worldwide

Current development status - SAE/ISO JWG

- Three projects (2 joint ISO-SAE, 1 joint ISO-IEC)
  - ISO/SAE PWI 8475
    - Cybersecurity Assurance Level (CAL) & Targeted Attack Feasibility (TAF)
      - Next working draft ~ early July
      - Committee draft: July 2024
      - Publicly Available Specification (~November 2024)
  - ISO/SAE PWI 8477
    - Verification and validation
      - NWIP approval (end of August 2023)
      - Technical Report (~December 2024)

Powering Business Worldwide

Cybersecurity Assurance Level (CAL)

Powering Business Worldwide

CAL summary

- Expanding the CAL concept as defined in ISO/SAE 21434
- Topics-current state
  - Determining which RQs can be scaled and how
  - Clarification/relationships between CAL, TAF and existing frameworks such as EAL, ASIL
  - Enhancing how CAL is derived
    - i.e., common methodology; stability of CAL value
  - Composition and decomposition
  - Communications in the supply chain
  - Collaborative development

Powering Business Worldwide

ISO/SAE PWI 8477 V&V

ISO/SAE PWI 8477 V&V summary

- Content that was intended to be included in ISO/SAE 21434 annex
- Intended to be released as a “Technical Report” (informational only)
- Topics-current state
  - Defining verification and validation
  - Verification that CS requirements are adequate
  - Verification that implementation conforms with CS requirements
  - Verification of assumptions/claims
  - Relationship between V&V and CS requirements, risk, activities
  - Example V&V methods
  - Discussion of pros/cons of various types of testing
  - Application to off-the-shelf, reused & out-of-context components

Powering Business Worldwide

Targeted Attack Feasibility (TAF)

Motivation for TAF

- As a result of the TARA, the risk treatment decision for certain threats will be to ‘reduce the risk’
  - How do you specify the required strength of counter-measures?
  - How do you know if the counter-measure strength is ‘sufficient’?
  - How do you communicate this within the supply chain?
- Thus, the motivation for TAF…

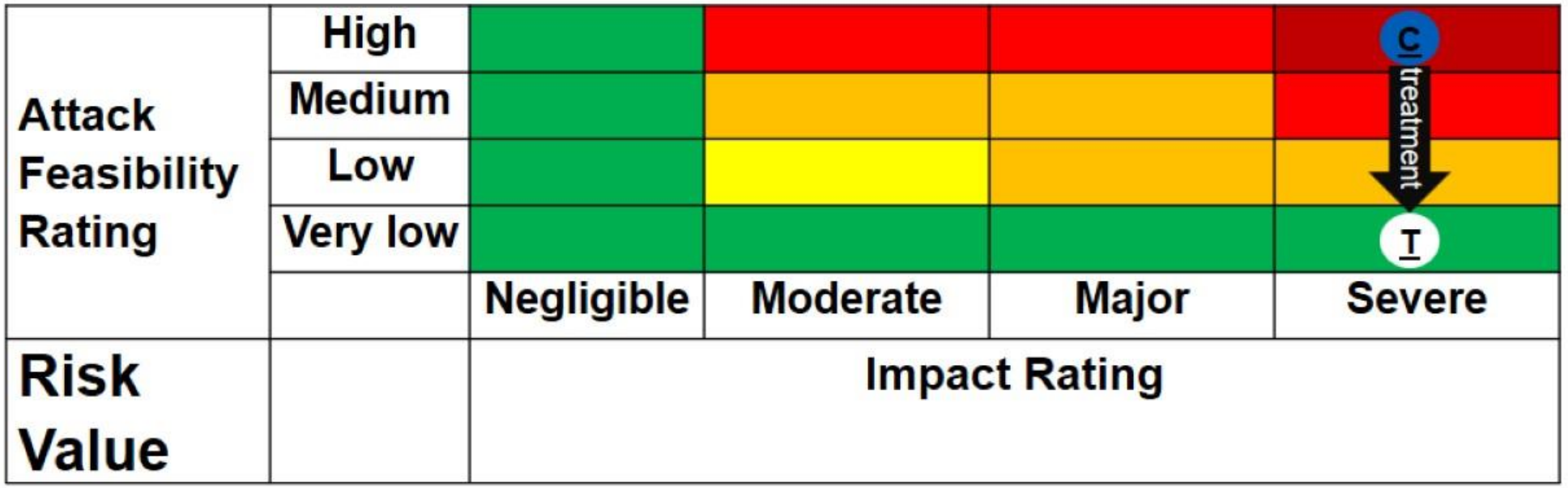
What is TAF?

- Based on attack feasibility as defined in ISO/SAE 21434
  - ‘attribute of an attack path describing the ease of successfully carrying out the corresponding set of actions’
- Current Attack Feasibility
  - Attack feasibility, considering current counter-measures, but before risk treatment
    - A factor to be considered when deciding risk treatment
- Targeted Attack Feasibility (TAF)
  - The target level of attack feasibility after implementation of countermeasures in order to control residual risk
    - TAF and impact determine residual risk

Powering Business Worldwide

TAF selection

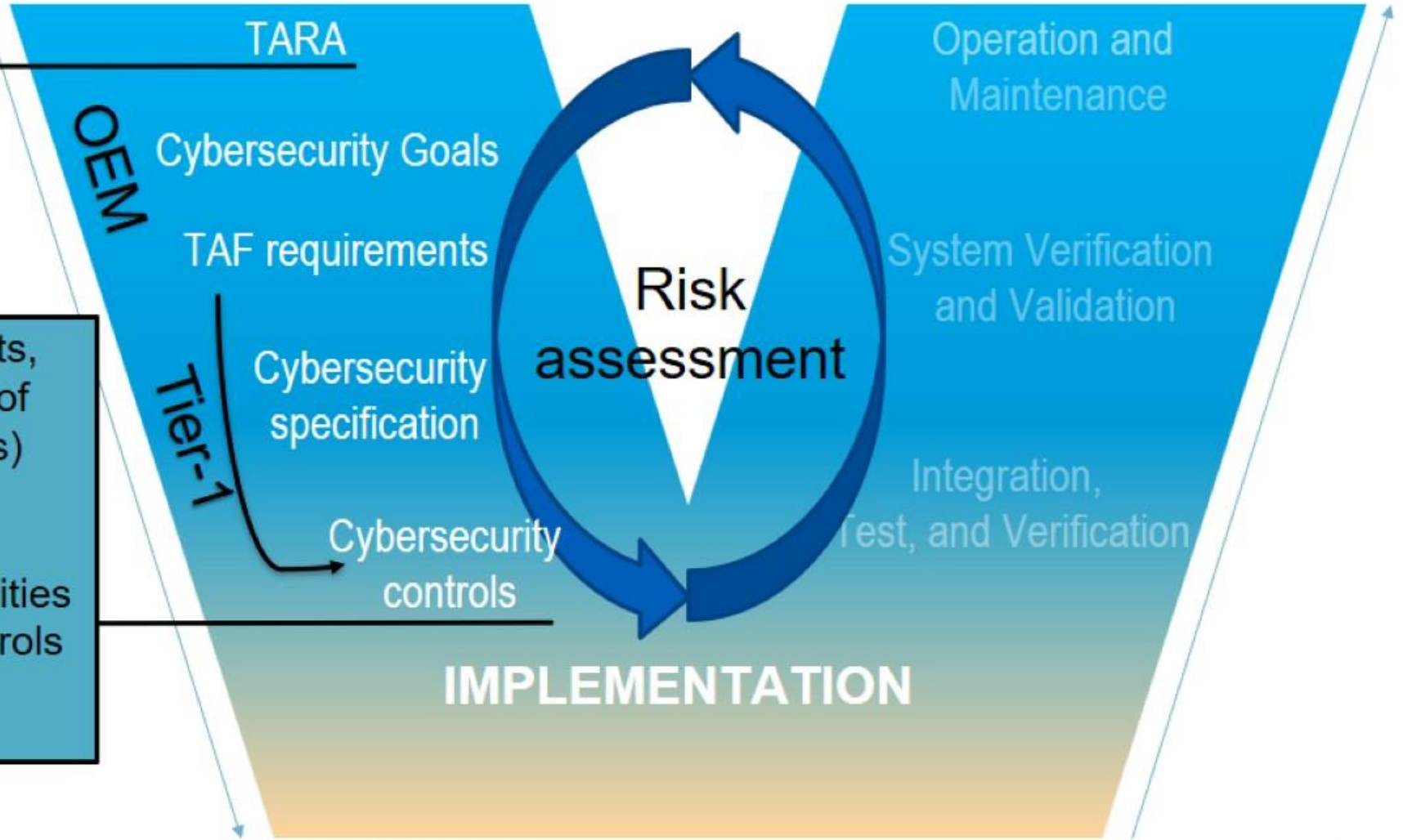
- The intent is to lower current attack feasibility
  - Selection of method to mitigate the risk could also reduce impact
  - Target level is communicated with supplier
    - See illustration below, where “C” is current, and “T” is targeted attack feasibility



Potential application of TAF during design phase

- "TARA"=> output Risk value, relative to threat/damage scenario (Impact and Attack feasibility)
- Derive CS goals and associated TAF
- Determines how to layer the protections (DiD)

- Refine & verify CS requirements, architecture, design: selection of controls (considering interfaces)
- Allocation of requirements to architectural elements
- Identify and manage vulnerabilities
- Selection of cybersecurity controls due to TAF (strength, depth)



EATON
Powering Business Worldwide

TAF summary

- Topics-current state
  - TAF to be used to determine controls (technical)
  - TAF can be used to describe strength of controls
  - TAF can be used for out of context development
  - Method(s) to derive TAF
  - Decomposition and composition options
  - Relationship with CAL
  - Supply chain or internal communications
- TAF will be informative content of PWI 8475 CAL/TAF

Powering Business Worldwide

Potential synergies with GP

- Methods for determining attack feasibility for TAF
  - Leveraging Security Evaluation Standard for IoT Platforms (SESIP)
    - 3.4.1 Limited Physical Attacker Resistance
    - 3.4.2 Physical Attacker Resistance
- Standardized security requirements/architectures
- Roadmap for post-quantum cryptography

Powering Business Worldwide

Questions?

Thank you!

John Krzeszewski, MSEE, GSEC

Senior Specialist, Functional Safety and Cybersecurity

johntkrzeszewski@eaton.com

Powering Business Worldwide

Global Platform™

SESIP Evaluation Methodology and Automotive

John Boggie, NXP

SESIP AND AUTOMOTIVE

John BOGGIE
Head of Cybersecurity Certification

SECURE CONNECTIONS FOR A SMARTER WORLD

BRIEF OVERVIEW OF EACH CERTIFICATION TYPE 3/3

- SESIP (EN 17927)
  - Security Evaluation for Secure IoT Platforms EN 17927: SESIP is a certification standard developed to allow re-use of security testing across complex connected products. It provides a technology agnostic approach (lego-box) to allow technology to define a set of security requirements and common security vulnerability assessment and testing approach. It is built around the security services provided by all layers of a system from sub-component to final product. It is written in easy to understand language and provides a cost/time effective approach to security validation and testing.

ISO/SAE 21434

ISO/SAE 21434 – MANDATORY THREAT AND RISK ANALYSIS

- TARA Threat Analysis and Risk Assessment requires to be performed by each security component in the Automotive Supply Chain up to and including the OEM
- It requires:
  - Secure development Process
  - Item Definition defining threats and risks
  - Incident management and resolution

READY FOR ISO/SAE 21434 COMPLIANCE CLAIM AT PRODUCT LEVEL

- ISO/SAE 21434 defines cybersecurity process, and it is typically tied to a company development process
- In SESIP, one can further claim the process has been applied for a particular product
  - SESIP EN 17927:2022 CEN/JTC 13

6.2 Secure development

6.2.1 Requirement

For the development of the platform, the secure development process specified in <standard/specification> has been applied to the platform.

6.2.2 Value

The inclusion of this package claim in a SESIP Security Target or profile allows the generation of evidences that secure development requirements from a referenced specification/standard have been applied to the platform under evaluation.

Example: application of security-by-design process from a specification/standard e.g. ISO/SAE 21434:2021.

6.2.3 Considerations

Complete the variable parts of this SPP as follows:

- The specification or standard to be implemented by the environment and applied to the platform.

ISO/SAE 21434 and SESIP

ASSET DEFINITION

- SESIP Methodology lists the main assets of a Connected Platform

Asset	Protections
User data (local)	Privacy concerns are essential. Protections of integrity, authenticity, and confidentiality must be provided.
User data (authentication data)	Confidentiality is required for secrets. Secondary data (like counters) must be appropriately protected (integrity, confidentiality).
Data in transit (internet)	Confidentiality and integrity are often essential, as are authenticity and authentication of the other party.
Data in transit (local)	Integrity is often essential. Confidentiality is not a systematic requirement. Authenticity and authentication of the other party are less common.
Code, including platform code and application code	Integrity and authenticity are strong requirements. Confidentiality is optional.
Product identity	Integrity and unicity are required.
Configuration and system data	Integrity and authenticity are required.
Life cycle related data	Integrity is required.

SESIP ALREADY COVERS ISO/SAE 21434 INFORMATIVE REQUIREMENTS IN APPENDICES

- ISO/SAE 21434 Annex E: Cybersecurity assurance levels (CAL)

Example of Annex E CAL4 (Highest level)	SESIP
Search for vulnerabilities by exploratory methods	Yes; by definition of SESIP methodology
Cybersecurity assessments are carried out by a person who is independent	Totally independent; 3rd party certification
Independence of verification of cybersecurity concept and design activities	Security target is assessed (ASE); Process application can be covered by independent 3rd party (SPP)
Independence of verification of the implementation and integration of components	Covered by independent 3rd party (ADV)
Independence of cybersecurity validation	Covered by independent 3rd party evaluation
Independence of cybersecurity assessment	Covered by independent 3rd party evaluation and certification
Functional testing	Covered (ATE)
Vulnerability scanning	Covered (AVA)
Fuzz testing	Can be covered (AVA)
Penetration testing	Covered (AVA & Pentesting)

SESIP ALREADY COVERS ISO/SAE 21434 INFORMATIVE REQUIREMENTS IN APPENDICES

- ISO/SAE 21434 Annex G2: Guidelines for the attack potential-based approach
- SESIP Rating table separates Identification and Exploitation phase
- Results should be interchangeable

Table G.6 — Example aggregation of attack potential

Elapsed time		Specialist expertise		Knowledge of the item or component		Window of opportunity		Equipment	
Enumerate	Value	Enumerate	Value	Enumerate	Value	Enumerate	Value	Enumerate	Value
≤1 day	0	Layman	0	Public	0	Unlimited	0	Standard	0
≤1 week	1	Proficient	3	Restricted	3	Easy	1	Specialized	4
≤1 month	4	Expert	6	Confidential	7	Moderate	4	Bespoke	7
≤6 months	17	Multiple experts	8	Strictly confidential	11	Difficult/ none	10	Multiple bespoke	9
>6 months	19								

Table B-1: Attacks Rating

Factors	Identification	Exploitation	Notes
Elapsed time			
< one hour	0	0	
< one day	1	3	
< one week	2	4	
< one month	3	6	
> one month	5	8	
Not practical	*	*	
Expertise			
Layman	0	0	
Proficient	2	2	
Expert	5	4	
Multiple Expert	7	6	
Knowledge of the TOE			
Public	0	0	Critical or higher can only be claimed if all sites with access to that information are included in the scope of the evaluation at ALC_DVS.2 level (i.e. SESIP5).[1]
Restricted	2	2	
Sensitive	4	3	
Critical	6	5	
Very critical hardware design	9	NA	
Access to TOE			
< 10 samples	0	0	
< 30 samples	1	2	
< 100 samples	2	4	
> 100 samples	3	6	
Not practical	*	*	
Equipment			
None	0	0	
Standard	1	2	
Specialized	3	4	
Bespoke	5	6	
Multiple Bespoke	7	8	
Open samples			
Public	0	NA	Sensitive or higher can only be claimed if all sites with access to such open samples are included in the scope of the evaluation at ALC_DVS.2 level (i.e. SESIP5).[2]
Restricted	2	NA	
Sensitive	4	NA	
Critical	6	NA	

MCU/MPU PROFILE – GENERIC PRODUCT TYPE THREAT ANALYSIS

Assets	Threats	MCU/MPU profile coverage
Sensitive data End-user information (identity, other personal information, related keys/password) Environment data (e.g. road traffic information, environment measurements) Internal sensitive data (configuration data, keys, life cycle state)	**Modification [and disclosure] of sensitive data while stored** ➔ Impersonation leading e.g. to access to internal or external restricted services ➔ Privacy concerns ➔ Diffusion of wrong environment information ➔ Access to sensitive data and/or restricted services	Secure [Confidential/External] Storage – protections of sensitive data Secure KeyStore – protections of user crypto data e.g. keys, password Secure Debugging – protection of data access through debug interfaces Residual Information Purging – ensures erasure of sensitive data when needed (e.g. to ensure privacy in case of Field Return, Factory Reset, Decommissioning of the device) [Physical Attacker Resistance – protection against physical intrusions as simple probing]
	Modification [and disclosure] of sensitive data during manipulation ➔ Same potential impacts as above	All features – each claimed feature include the protection of assets related to the security feature [Software Attacker Resistance: Isolation of Platform – additional protections against software attacks using untrusted local code] [Physical Attacker Resistance – protections against local attacks]
	Modification [and disclosure] of sensitive data during exchanges with external entity (e.g. remote server, secure element of the integrating SoC) ➔ Diffusion of wrong environment information	Secure Communications – protections of the overall establishment of communications including related keys (generation/derivation, exchange, storage, binding, etc.)
Code	**Modification or replacement of stored code** ➔ Deletion of parts of original code ➔ Execution of attacker code replacing original code ➔ Disabling of part or all security features, access to sensitive data	Secure Initialization of Platform / Secure Update – check code authenticity and integrity before running Secure Update – allow security breaches fix All features– protection of security features execution
	Modification code at execution ➔ Bypass of parts of the code ➔ Execution of attacker code illegally loaded in memory ➔ Disabling of part or all security features, access to sensitive data and/or restricted services	[Software Attacker Resistance: Isolation of Platform – protection against malicious interactions with executing code through local untrusted code] [Physical Attacker Resistance – protections against local attacks disrupting code execution e.g. HW fault injections]

MCU/MPU PROFILE - THREAT ANALYSIS

Assets	Threats	MCU/MPU profile coverage
Life-Cycle	**Modification of MCU/MPU life-cycle state verification** + See modification of sensitive data for threats against life cycle state while stored and at runtime ➔ Access to restricted life cycle state, giving access to restricted features e.g. debug/test ➔ Access to sensitive data and/or restricted services	Secure Initialization of Platform – include control of boot modes/tests access depending on life cycle [Secure Attestation of Platform State – can include MCU/MPU life cycle state for external check] [Software Attacker Resistance: Isolation of Platform – protection against malicious interactions with executing code through local untrusted code]
Secure services Cryptographic services	**MCU/MPU weak cryptographic services** ➔ Generation of weak cryptographic material ➔ Disclosure of cryptographic secrets ➔ Access to sensitive data and/or restricted services	Cryptographic Operations, Cryptographic Key Generation, Cryptographic KeyStore, Cryptographic Random Number Generation - ensure cryptographic services following secure crypto rules [Software Attacker Resistance: Isolation of Platform – protection against malicious interactions with executing code through local untrusted code] [Physical Attacker Resistance – protections against local attacks disrupting code execution e.g. HW fault injections, disclosing involved cryptographic keys or secrets]
MCU/MPU identification	**Modification of MCU/MPU identification** **Non unique MCU/MPU identification** ➔ Unexpected use of non-certified MCU/MPU	Verification of Platform Identity – check if right type and version of the MCU/MPU

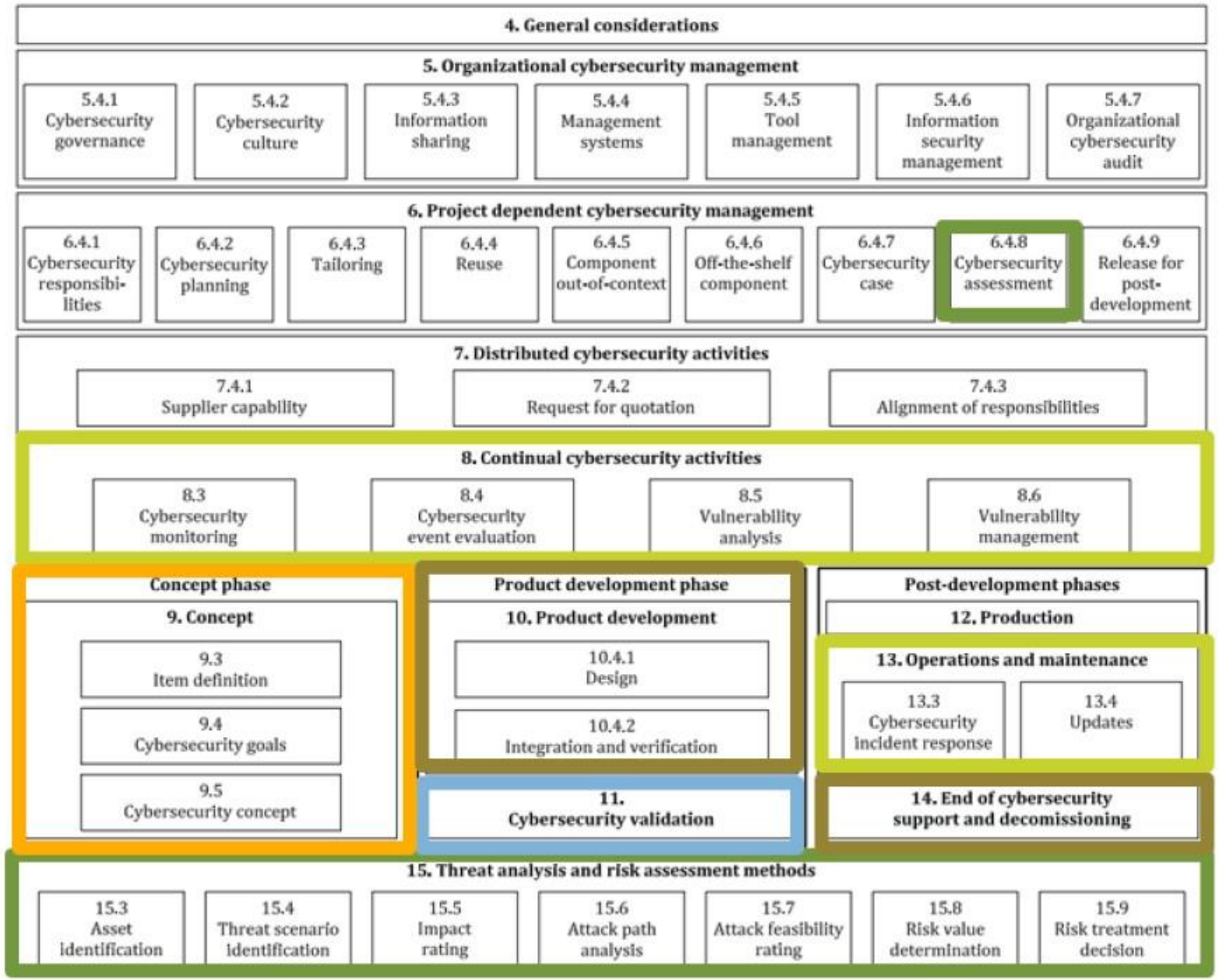
MCU/MPU PROFILE - THREAT ANALYSIS SUMMARY

- **Details on considered attacks**

– Remote attacks (by default)
  - Remote logical attacks (e.g. ill formed messages targeting remote services as FW/SW update, environment measurements/probing, ranging calculation, etc.
  - Remote side channel attacks (e.g. timing attacks, cache attacks)
  - Remote hardware attacks (e.g. clkscrew)

– Local attacks (if applicable i.e. use cases depending)
  - Local logical attacks (e.g. via USB interfaces)
  - Local side channel with “basic/standard” material (e.g. power/EM/clock measurements)
  - Local hardware attacks with “basic/standard” material (e.g. voltage/clock glitching, EMFI, simple probing)

SESIP EVALUATION PROVIDES ISO/SAE21434 COMPLIANCE EVIDENCE



SESIP requires clear Security Target and Claims

SESIP can assess development process and product feature

SESIP verifies Security Claims and provide assessment

SESIP methodology is for Threat Analysis and Risk Assessment

SESIP requires Incident Management

NXP Semiconductors usage of SESIP for Automotive

AUTOMOTIVE NXP CERTIFICATIONS

CAVP – NIST
Cryptographic Compliance

ESV – NIST
Random Number
Compliance – SP800 90B

SESIP Certification

ISO/SAE 21434 Process
Certification

TISAX (ISO 27001)
Trusted Information Security
Assessment Exchange

BRIEF OVERVIEW OF EACH CERTIFICATION TYPE 1/3

- NIST Certifications
  - Cryptographic Algorithm Validation Program (CAVP): The NIST CAVP program provides validation testing of NIST approved cryptographic Algorithms, i.e. each algorithm implemented in our products is validated that it complies with the NIST standard. Each algorithm receives a separate certificate.
  - Entropy Validation Server (ESV): ESV is the process where an accredited lab submit compliance and testing proof to NIST to show compliance to SP 800-90B (Random Number Generator)
- TISAX
  - Trusted Information Security Assessment Exchange: Provided by the ENX Association, TISAX is a Automotive specific variant of the Information Security Management System (ISO 27001). TISAX asses a companies security practices and how the organization deals with information and data protection. It includes management buy-in, disaster recovery and how the organization handles security incidents.

BRIEF OVERVIEW OF EACH CERTIFICATION TYPE 2/3

- ISO/SAE 21434
  - ISO/SAE 21434: Specifies engineering requirements for cybersecurity risk management regarding concept, product development, production, operation, maintenance and decommissioning of electrical and electronic systems in road vehicles, including their components and interfaces. It requires a company to:
    - Perform Risk Assessments - Identify potential security vulnerabilities
    - Address these vulnerabilities as part of the product design/development
    - Test to show the risks have been mitigated

    UN R155 and UN 156 made this mandatory across the Automotive supply chain from July 2022

AUTOMOTIVE NXP CERTIFICATIONS –SESIP PROVIDES A PROOF POINT FOR THE OTHER CERTIFICATION STANDARDS

AUTOMOTIVE NXP CERTIFICATIONS – WHAT THE SESIP CERTIFICATE COVERS

Certificates proving that the Cryptography is implemented correctly

Proof that the random number generator complies to a industry standard

Certificates provided by US Government

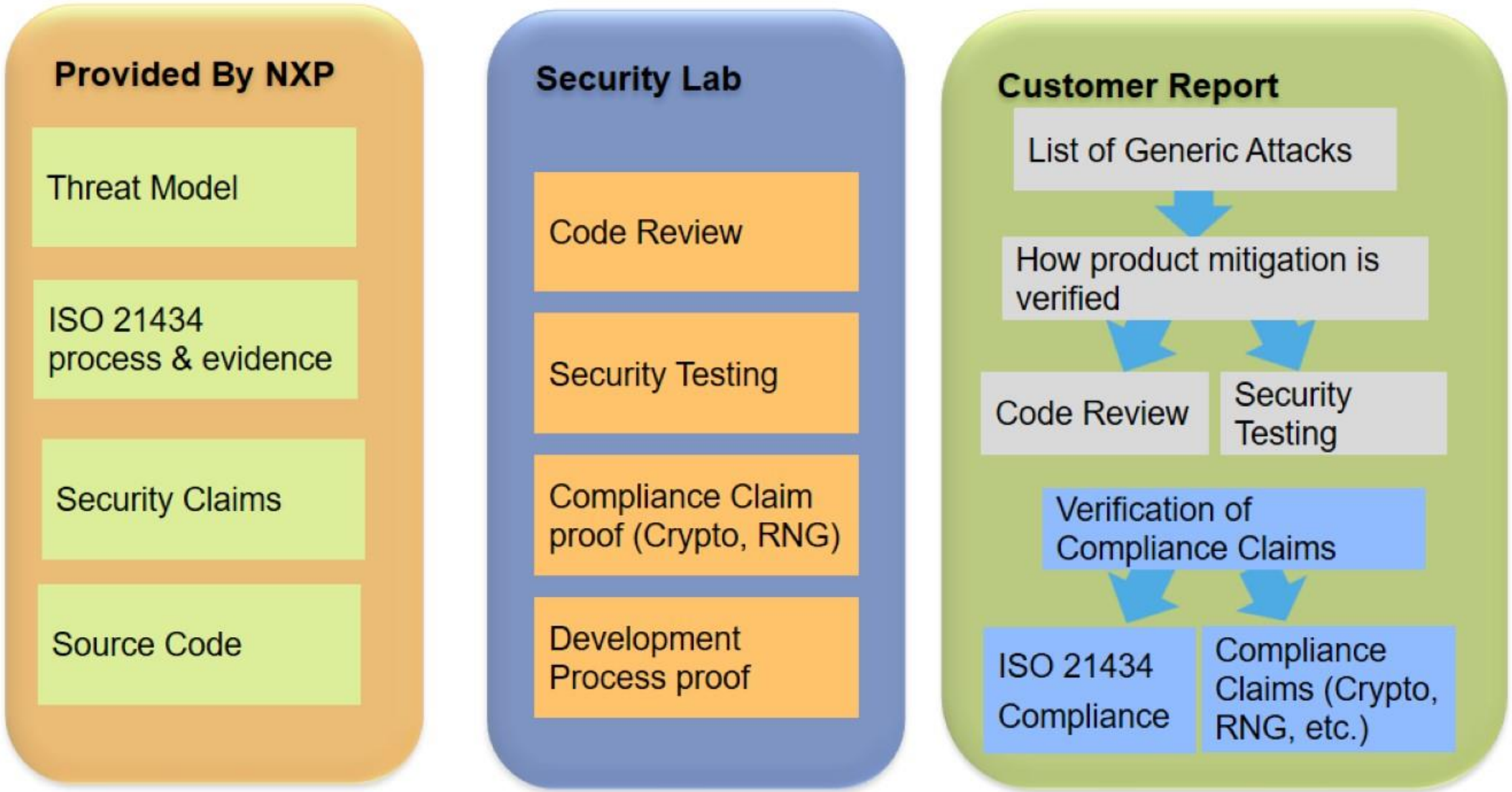
The Device has been defined using a common threat model and details of how it mitigates these threats.

Proof that the ISO 21434 certified processes and procedures were followed for the product's development cycle

Details how security sensitive information is handled within NXP

Proof that the Device follows the Product Security Response Incident Team (PSIRT) Process

NXP USAGE OF SESIP



IN SUMMARY

- SESIP provides evidence that the product security claims are tested and verified
- Verification and testing is performed by an external highly experienced test lab
- The certificate is awarded by a third part independent party
- A report can be delivered to customers all the way to the OEM and can be then shown as an artifact in their TARA
- SESIP already covers requirements coming from government legislation

Test Labs

- SGS Brightsight
- Riscure
- TUV Informationstechnik
- APPLUS
- Serma
- Dekra (preliminary accreditation)
- UL (preliminary accreditation)
- ATSEC (preliminary accreditation)

SECURE CONNECTIONS
FOR A SMARTER WORLD

Global Platform™

An Overview of V2X Security Challenges

William Whyte, Qualcomm

Qualcomm

Plymouth, MI

2023-06-20

Securing V2X communications: the role of trusted components

William Whyte, Senior Director, Technical Standards, Qualcomm Technologies Inc.

wwhyte@qti.qualcomm.com

2021 traffic crash data

(National Highway Traffic Safety Administration[1])

42,915

people killed in motor vehicle traffic crashes on U.S. roadways —highest since 2005

10.5%

Increase in fatalities since 2020

13%

Increase for pedestrians

5%

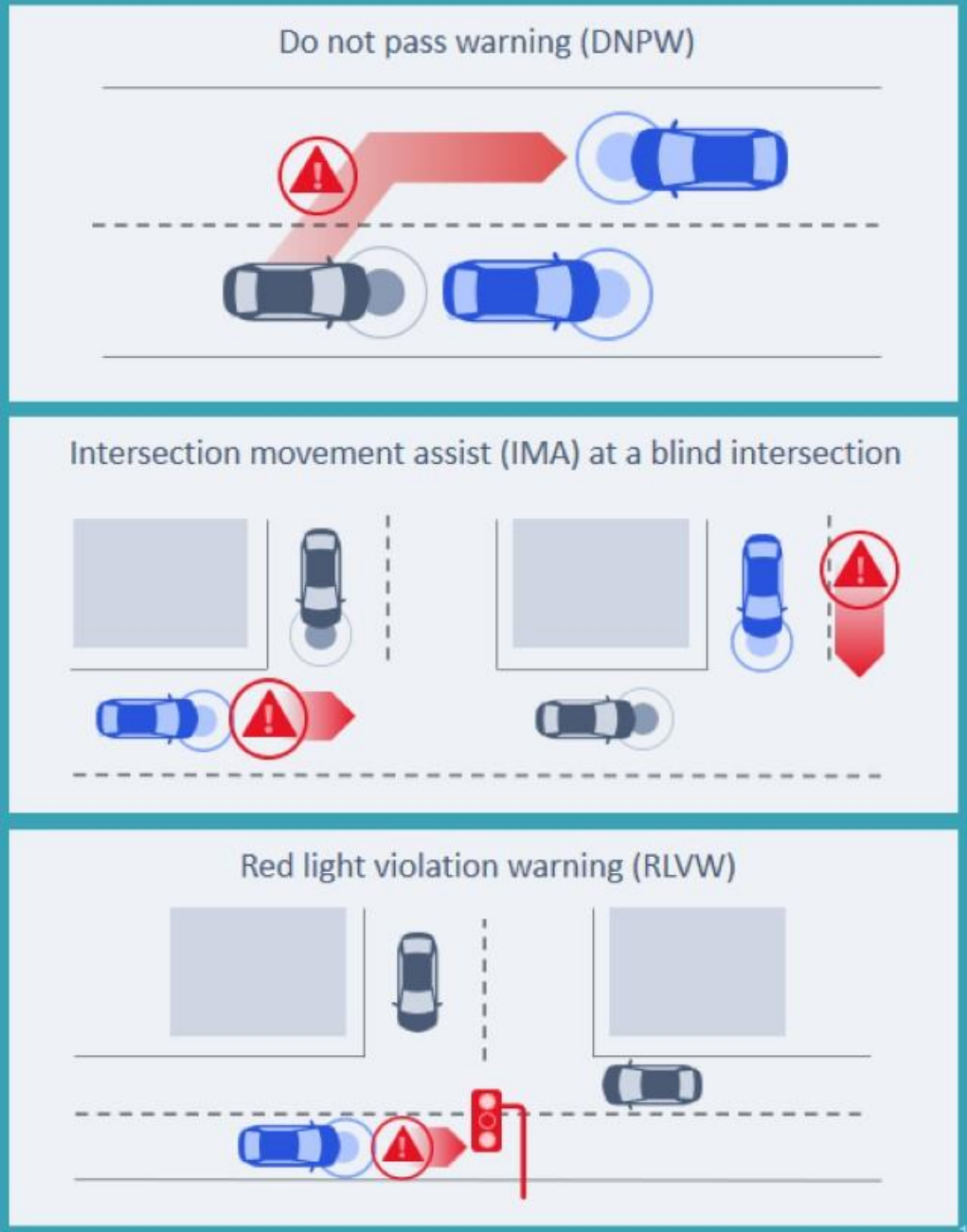
Increase for pedal cyclists

1. NHTSA

2. Independent analysis based on the following reports: i) NHTSA, "Preliminary Regulatory Impact Analysis FMVSS No. 150 Vehicle-to-Vehicle Communication Technology for Light Vehicles," (2016), ii) Kareen El Beyrouty et al., "Support Study for Impact Assessment of Cooperative Intelligent Transport Systems" (2018), iii) U.S. DoT, "Benefit-Cost Analysis Guidance for Discretionary Grant Programs" (2020).

Vehicle-to-Anything (V2X)

- V2V Safety
  - Intersection Movement Assist
  - Emergency Brake Light notification
  - Forward Collision warning
  - Sensor Sharing
- V2I Safety and Mobility
  - Red Light Violation Warning
  - Signal Prioritization and Preemption
- V2V Efficiency
  - Truck platooning
  - Maneuver Coordination
- V2X can address 80% of non-impaired collisions
- But these messages must be **trustworthy** and **reliable**



What's special about V2X security?

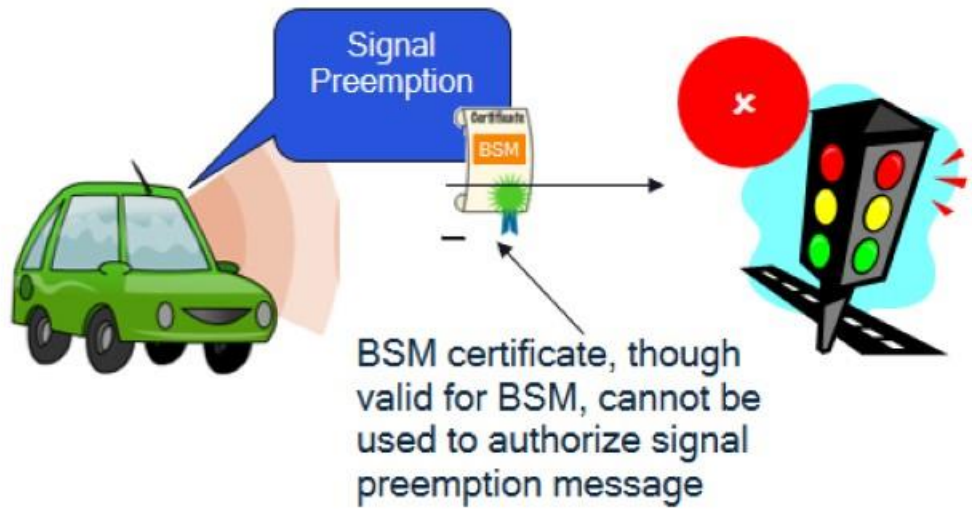
- Trusted Web communications
  - Connection to eCommerceGiant.com
  - Unicast
  - Online, can request more information for validation if necessary
  - Identity-based - server cert contains DNS ID
- V2X / ad-hoc networking
  - Many-to-many communications
  - Need to be able to make real-time decisions locally
    - Limited bandwidth
    - Low-latency network connectivity not assured
  - Different actors in different roles
    - Typically the identity of the actor isn't important, the role is
  - Concern about privacy
  - Limited connectivity for security / system management updates

V2X Communications Security with IEEE 1609.2: Goals

- Allow receivers to make trust decisions about received messages in real time with minimal increase in packet size
  - Ordinary car **can** send Basic Safety Message / Cooperative Awareness Message and have receivers accept it
  - Roadside Unit (RSU) **cannot** send BSM / CAM and have receivers accept it
  - Ordinary car **cannot** send signal preemption and have receivers accept it
  - Public safety (police) car **can** send signal preemption and have receivers accept

Approach: IEEE 1609.2 certificates

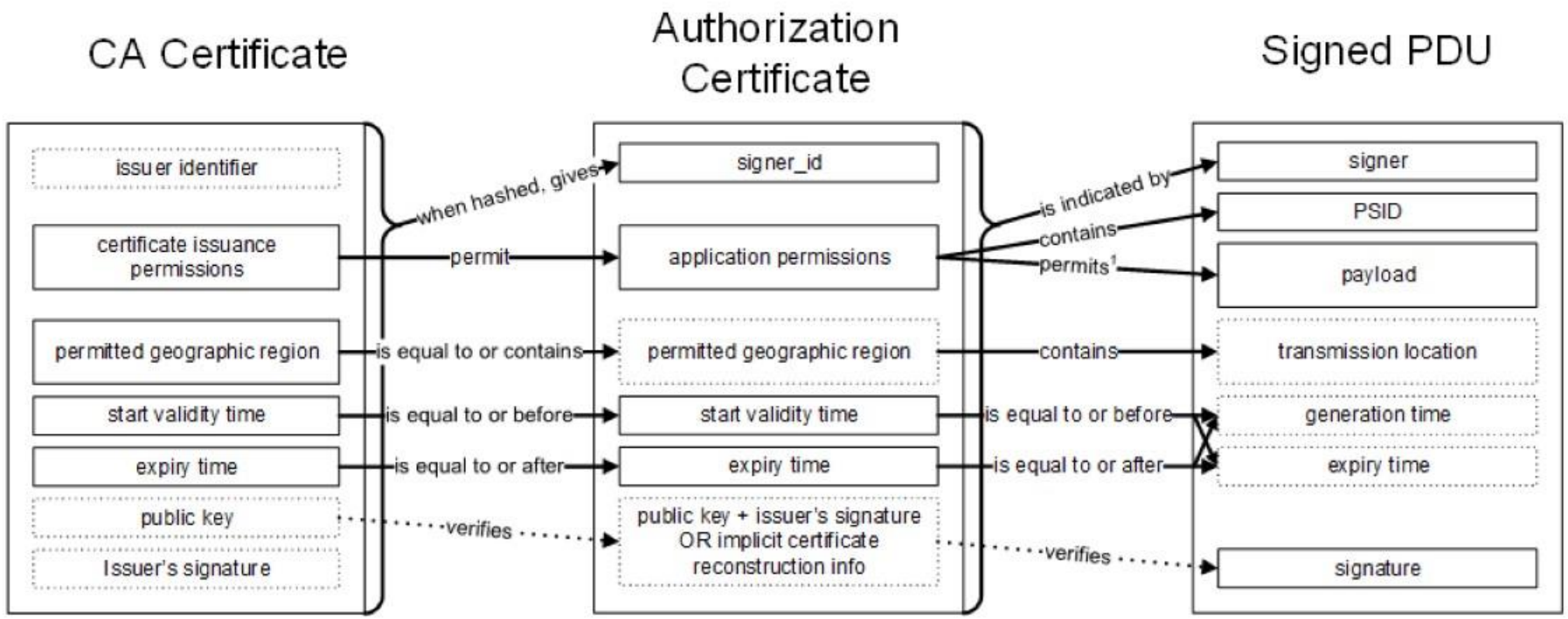
- IEEE 1609.2 defines secure message and certificate format
- Certificate states permissions and other attributes of sender; receiver checks that sender has the permissions they need to carry out the actions
  - Permissions are encoded as Provider Service ID (PSID, known as ITS-AID internationally) and Service Specific Permissions (SSP)
- PSID system is extensible to support arbitrarily many future applications
  - New applications apply for PSID from registry, define own SSP semantics
- 1609.2 used in US, Europe (ETSI profile), China (CCSA harmonized standard), Korea, Australia, …



Source sample text

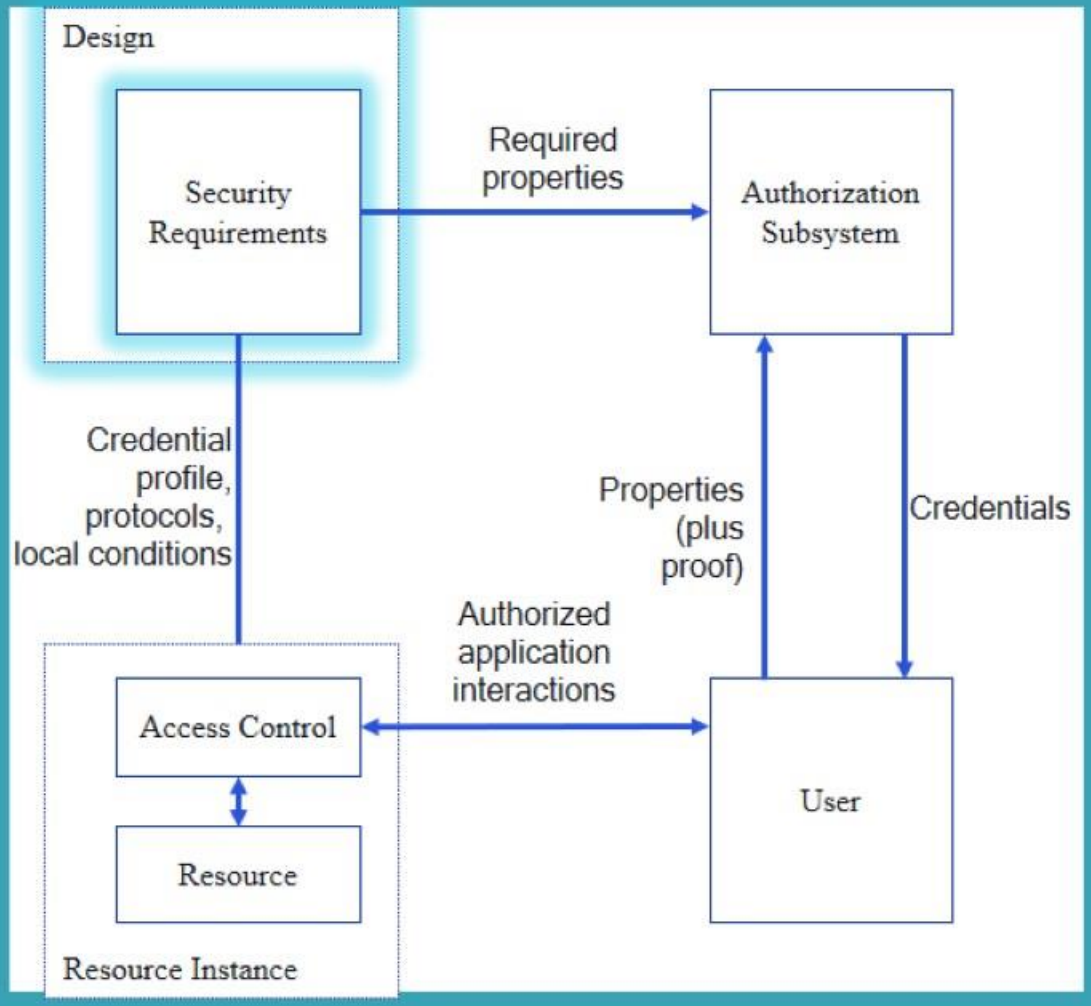
Consistency

- 1609.2 completely defines consistency conditions between certificates and messages, and between a CA certificate and a certificate that CA issued
- A message is only valid if all consistency checks are passed
  - Dotted boxes = optional fields; if present, they too must be consistent



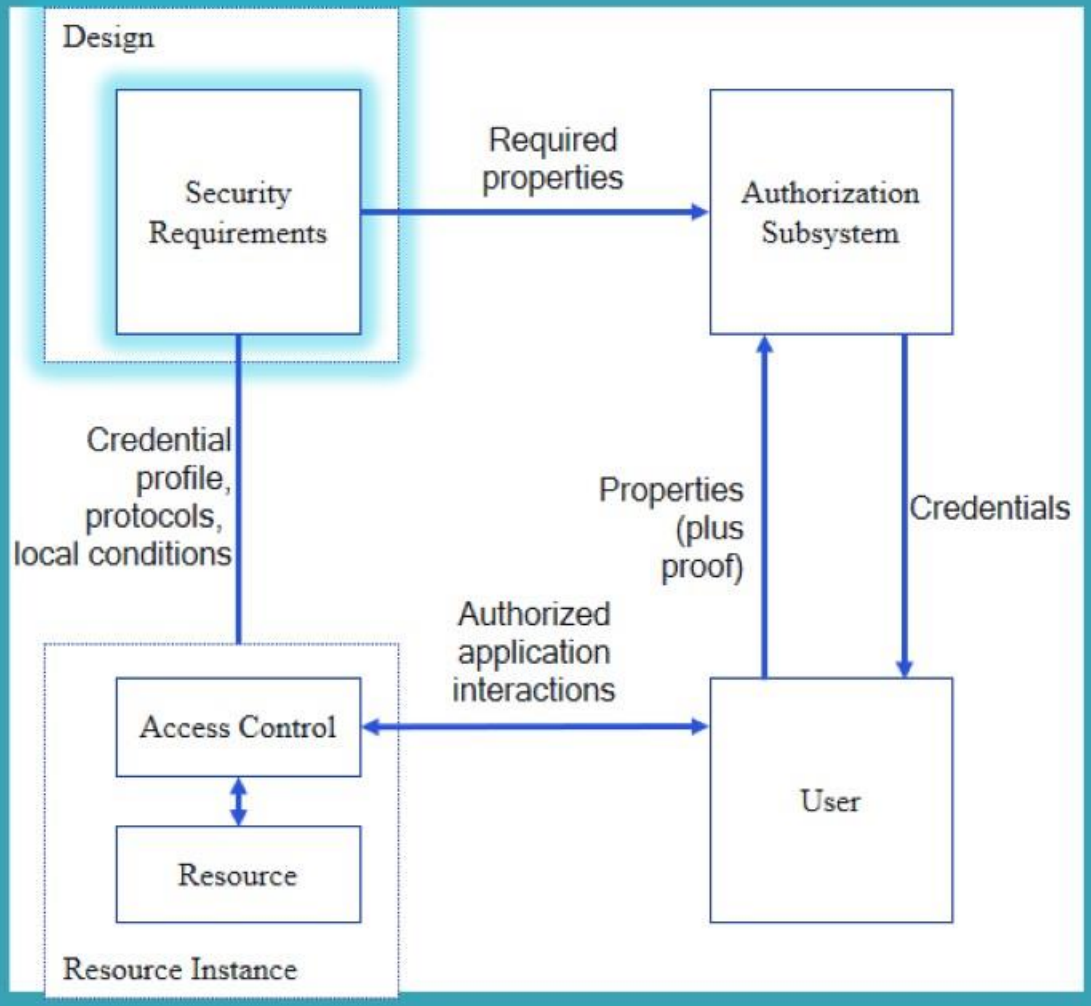
Security Requirements for BSM

- PSID 0x20 is reserved for “vehicle to vehicle safety and awareness”
  - https://standards.ieee.org/products-services/regauth/psid/index.html shows this as associated with appropriate SAE standards



Security Requirements for BSM

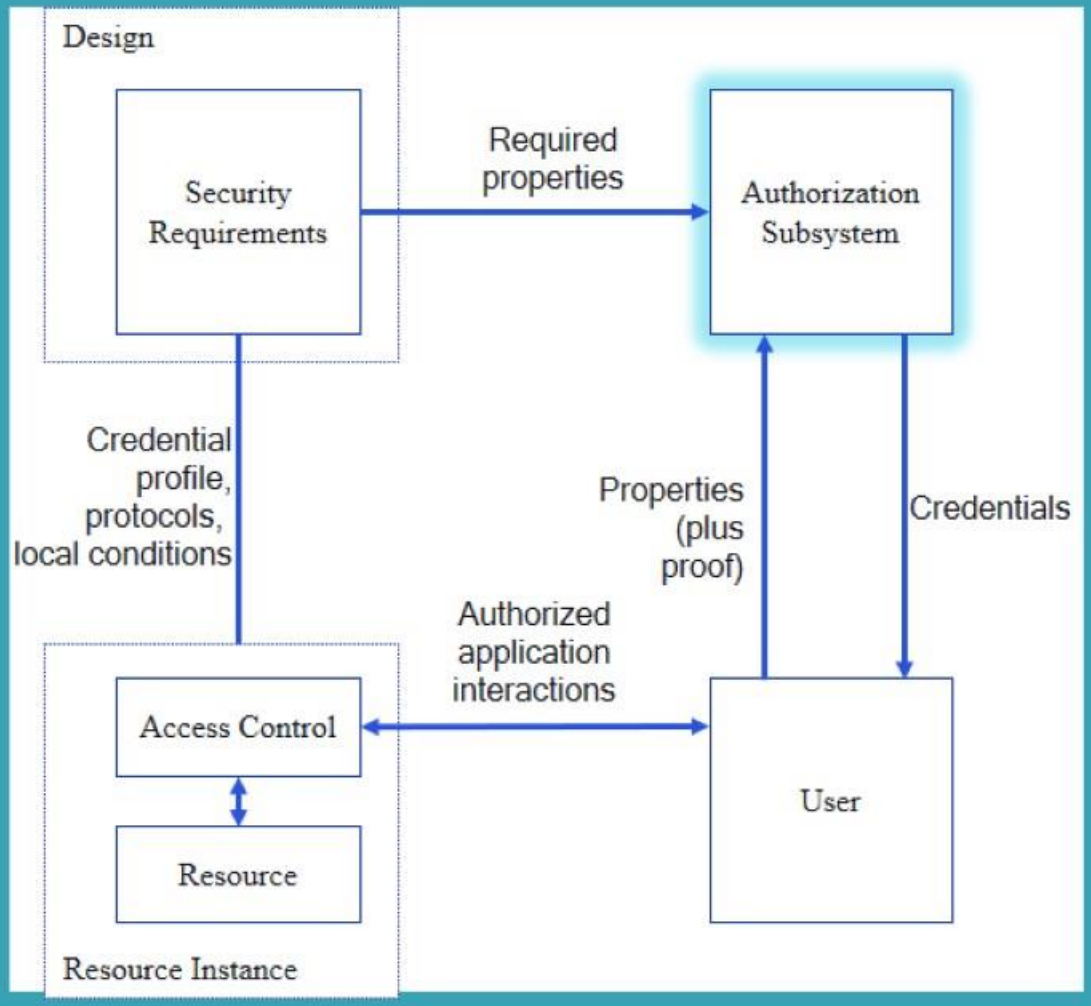
- PSID 0x20 is reserved for “vehicle to vehicle safety and awareness”
- The SAE standards (J2945/1, J3161/1, J3161/1A, J3161/1B, J2735) specify the over-the-air parts of the application
  - Information fields to be included in the message (ASN.1)
  - Performance requirements on sender
  - Security requirements
    - Identify “roles” within the application with security implications
    - For example, use of emergency vehicle fields
    - The Service Specific Permissions field in the certificate can be used to indicate whether the certificate holder has permissions for those roles



Source sample text

Worked example: BSM

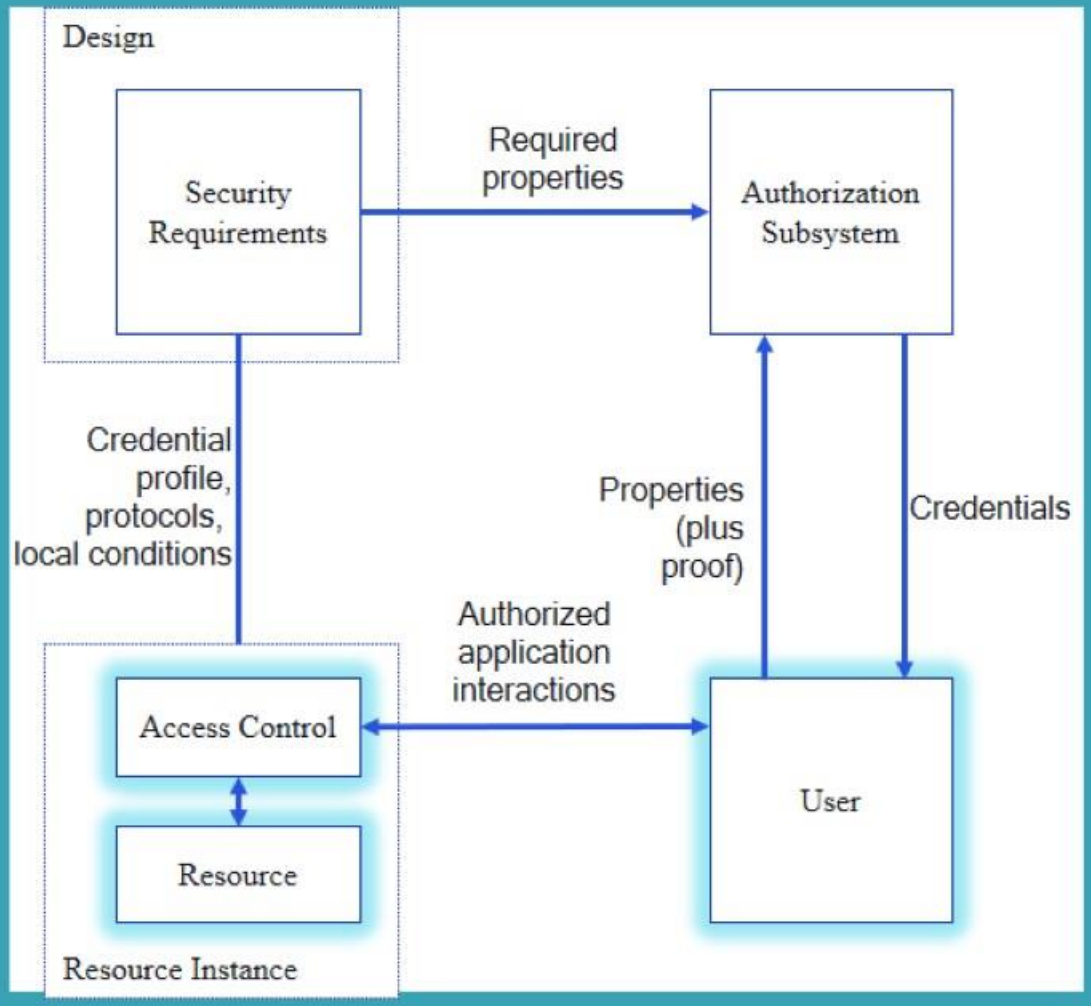
- PSID 0x20 is reserved for “vehicle to vehicle safety and awareness”
- The SAE standards specify the over-the-air parts of the application
- A Policy Authority specifies requirements that the host device must satisfy to be issued with certificates
  - These are published in a Certificate Policy and Security Policy and can include requirements for third party certification
    - Security certification by an accredited test lab following a standardized evaluation process
    - Functional/performance certification by a conformance test body
  - A device that meets these requirements is issued with certificates
  - The fact that a device can sign with a particular certificate indicates that it has satisfied all the policy requirements to get those certificates → messages from the device are **reliable** and **trustworthy**



Source sample text

Worked example: BSM

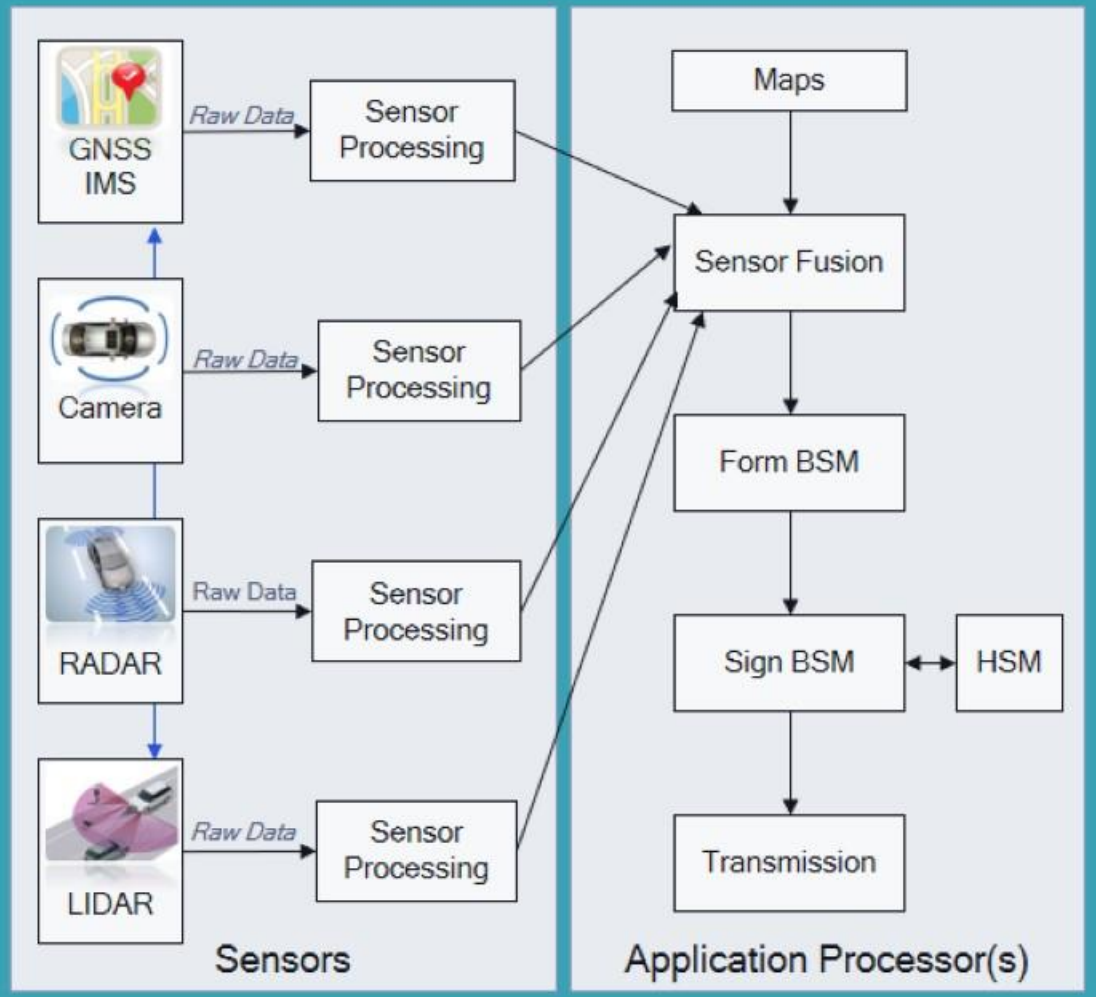
- PSID 0x20 is reserved for “vehicle to vehicle safety and awareness”
- The SAE standards specify the over-the-air parts of the application
- A Policy Authority specifies requirements that the host device must satisfy to be issued with certificates
  - The device demonstrates that it satisfies those requirements and obtains certificates
- The sender signs the message and makes the certificate available to the receiver
  - (Typically by including it in the sent PDU)
- The receiver checks that the PSID in the certificate matches the PSID in the message and that any “role activities” are permitted by the SSP
  - And that all other consistency conditions are met, etc



Source sample text

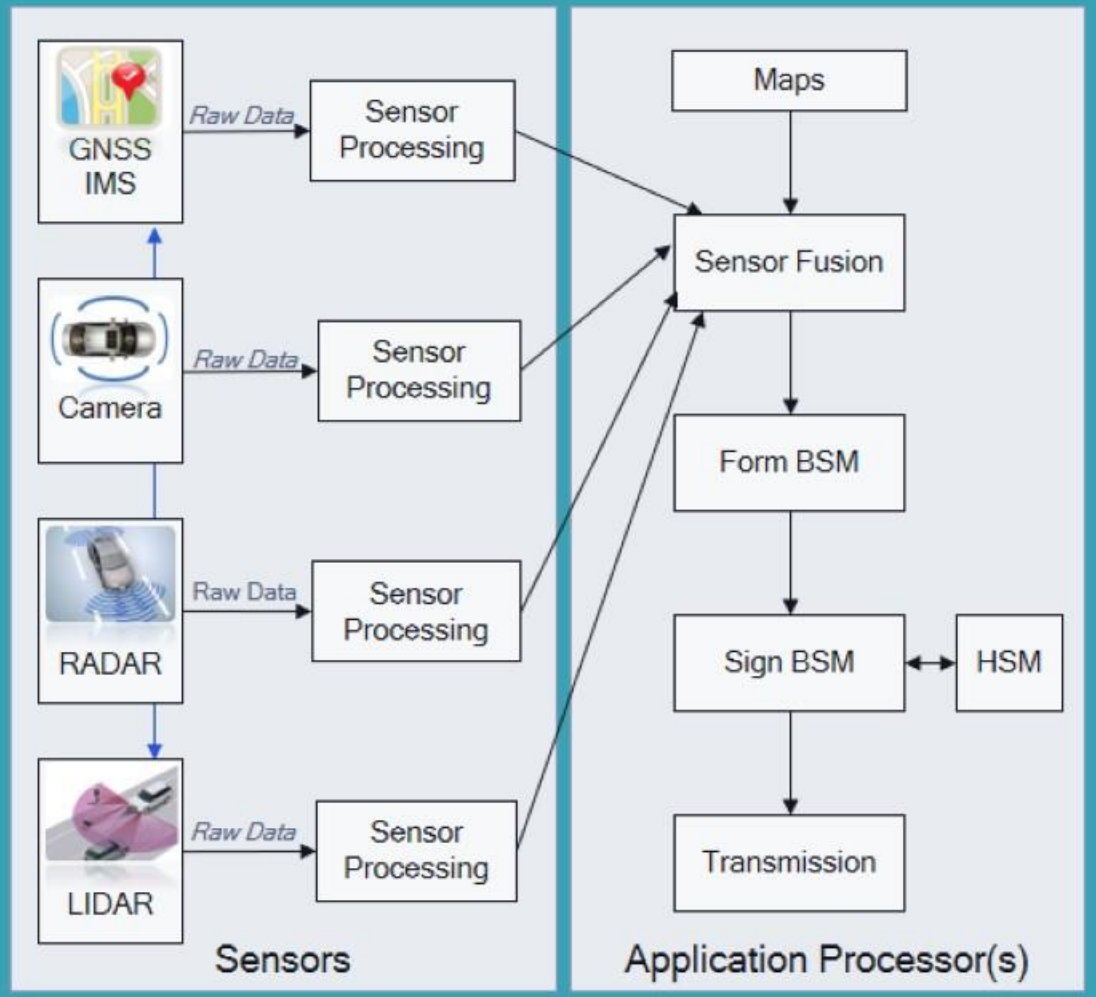
Formation of a BSM

- BSM is formed based on multiple sensors
  - Inertial Measurement System, GNSS, …
  - Sensors must be trustworthy
  - Connection from sensors to application processor must be trustworthy
- Individual sensor inputs are fused (potentially with non-sensor data) to give data about vehicle's dynamic state
  - Software that carries out fusion must be correct
    - Secure boot / secure software update / verification & validation
  - Non-sensor data must be trustworthy
- Dynamic state information is used to form BSM
  - Software and config files used to form BSM must be correct
    - Secure boot / secure software update / verification & validation
- BSM is signed
  - Platform must protect against bad signing requests getting to the HSM (HSM will sign anything - not realistic to require user authentication for each signature)
    - Control which processes have access to the HSM and control update of those processes' software and config
    - Protect physical connection between application processor and HSM
  - HSM must be secure and protect keys



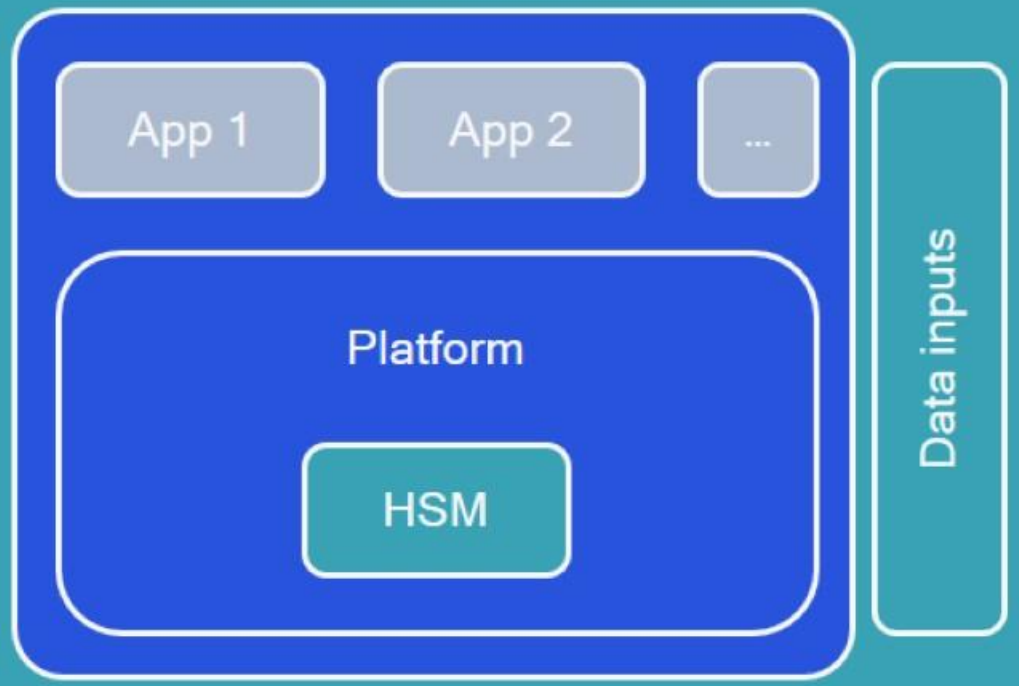
Formation of a BSM

- BSM is formed based on multiple sensors
  - Inertial Measurement System, GNSS, …
  - Sensors must be trustworthy
  - Connection from sensors to application processor must be trustworthy
- Individual sensor inputs are fused (potentially with non-sensor data) to give data about vehicle's dynamic state
  - Software that carries out fusion must be correct
    - Secure boot / secure software update / verification & validation
  - Non-sensor data must be trustworthy
- Dynamic state information is used to form BSM
  - Software and config files used to form BSM must be correct
    - Secure boot / secure software update / verification & validation
- BSM is signed
  - Platform must protect against bad signing requests getting to the HSM (HSM will sign anything - not realistic to require user authentication for each signature)
    - Control which processes have access to the HSM and control update of those processes' software and config
    - Protect physical connection between application processor and HSM
  - HSM must be secure and protect keys



Certification and security boundary

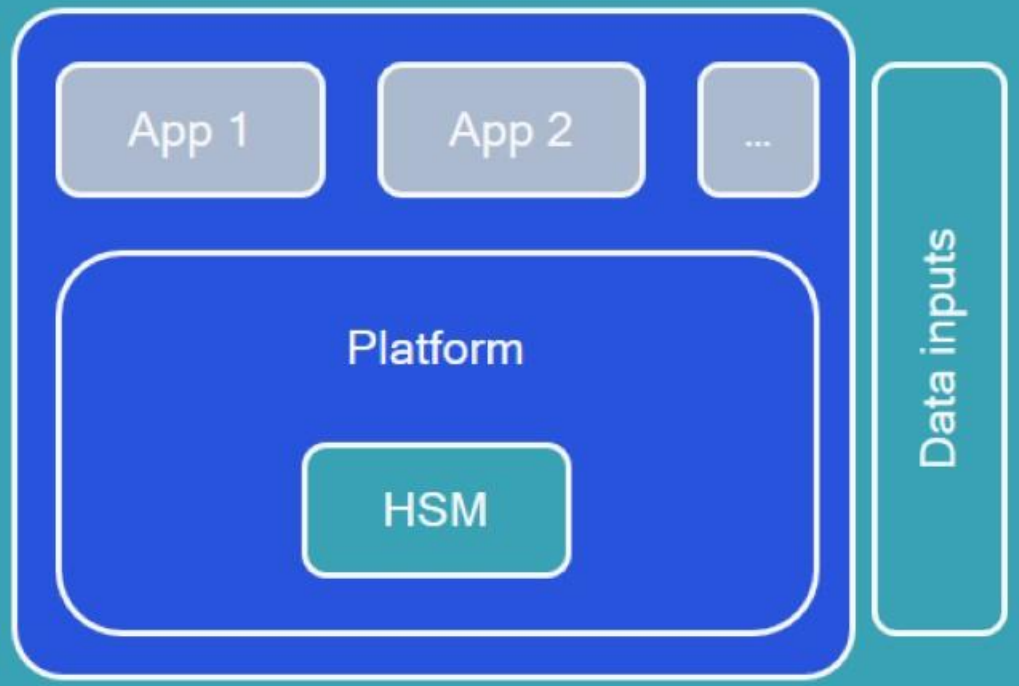
- Security certification of V2X devices is complex due to multi-application setting, variety of architectures in use, …
  - Determine appropriate security boundary
  - Determine appropriate evaluation process
    - OEMs are concerned about expense of Common Criteria
  - As V2X devices migrate from standalone to integrated into the TCU all these considerations become more difficult
- **Potential opportunity for Global Platform:**
  - **Define secure components that meet requirements in different regions**
  - **Use of GP APIs for HSM interface**



Source sample text

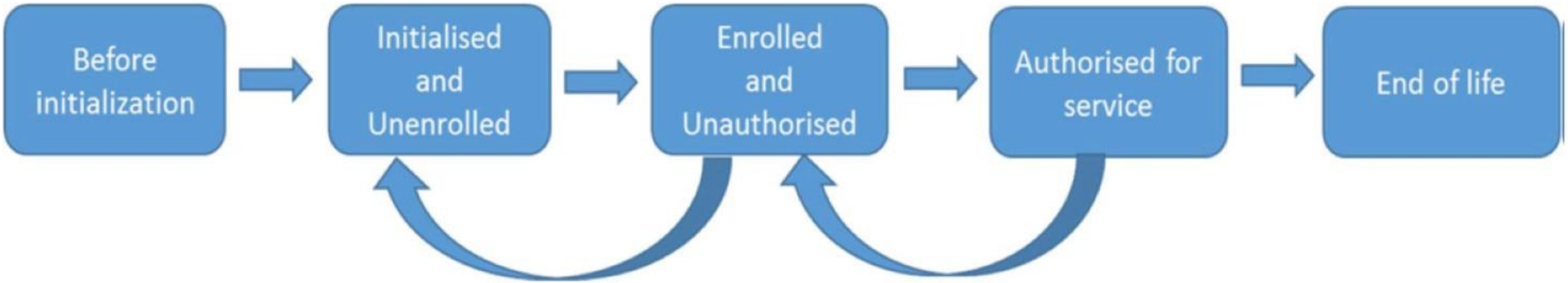
Certification: regional requirements

- EU
  - Published HSM protection profile (https://www.car-2-car.org/fileadmin/documents/Basic_System_Profile/Release_1.6.0/C2CCC_PP_2056_HSM_V1.0.pdf): some certified HSMs
  - PP for "V2X box" under development
  - EU Security / Certificate policy requires deployers to carry out a TARA where the impact of outputting incorrect messages is "medium"
  - No application conformance / performance requirements specifically for access to security credentials
- US
  - Informal "HSM + Platform" spec available, no formal validation available
    - HSM cannot be FIPS 140 certified due to spec inconsistencies but can be "FIPS 140 equivalent"
  - Intersections required to carry out TARA, integrated OBUs not currently required to do so
    - Expectation is that certification reqts will be ratcheted up over time
  - Requirements for security credentials include conformance / performance
    - Currently the credential issuance process is the only place in the system where this can be enforced
- China
  - China OBU Equipment Profile standard and RSU Profile standard close to completion
  - No standard WI on CC Protection Profile for C-V2X



Source sample text

Certificate lifecycle and possible GP intercept

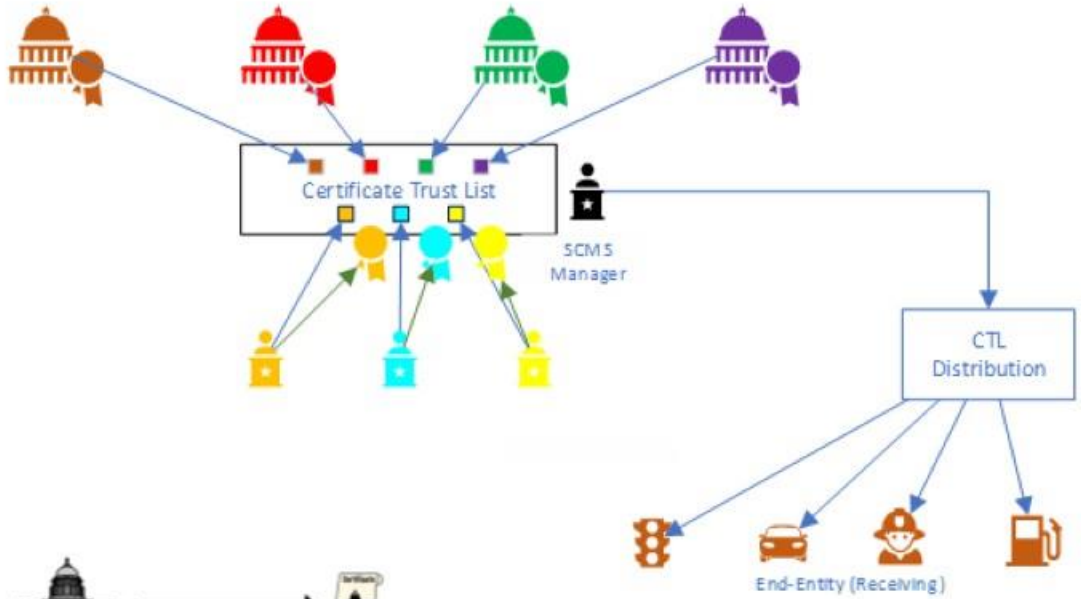


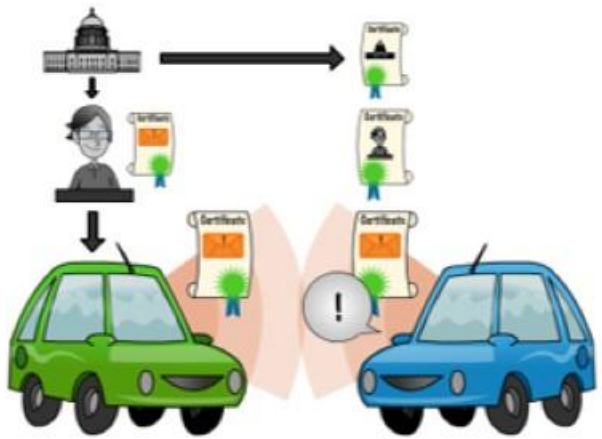
- End Entity is provisioned to become initialized (non-SCMS activity)
- EE interacts with Enrollment CA to become enrolled
- EE interacts with RA using enrollment cert to get authorization certs
- Authorization certs are used to authorize V2X application communications

- Enrollment is the point at which the device's permissions are established
  - Permissions can change throughout device lifecycle if new applications are added, device is used in a different context, …
- Mechanisms are not fully standardized
  - Legacy mechanisms have scalability questions
- **Possible opportunity for GP following standards work: Attestation potentially useful to ensure device is in known good state at enrollment status change**

Trust anchor management and trusted execution environment

- Received messages are trusted if signed by a certificate that chains back through a chain of issuers to a trusted root CA
  - Root CA trust needs to be established outside the chain
    - E.g. Mozilla root cert store
- 1609.2.1:
  - SCMS Manager (i.e. Policy Authority) creates Certificate Trust List (CTL) of trusted Root CAs
  - N Electors sign the CTL; a CTL is trusted if there are m < N valid signatures; m, N are public system parameters
  - Each CTL also contains the Elector certificates to be used to verify the next CTL in the series
  - Elector certificates can expire and be rolled over robustly
    - No issues so long as no more than (N-m) are invalid at the time a new CTL is received
    - Current parameters: N = 5, m = 3
  - If one Elector cert rolls over every 2 years, a device can be turned off for 2*(N-m) years and still have m trusted Electors -> still become up to date
- EU, China use CTL with single signer rather than Electors
- **Trusted environment needed: Elector certs are stored on each participant device and must only be updated via trusted process:**
  - (or via "manager" reset)
  - **Possible opportunity for use of GP technologies / standards**





Conclusions

- Making a working V2X system in which receivers can have enough confidence in received messages to make use of them is very complex!
- Issues around data reliability, input from multiple sources, correct implementation, performance requirements, **and** system security
- Some form of certification is likely to be required, even in US, for devices to be trusted - unclear what certification regime will be used
- Significant requirements for hardware security, platform security, secure connections between components and solutions not yet fully standardized
- Opportunity for Global Platform technologies (SE, TEE) and processes (SESIP) to prove valuable in this context

Thank you

Qualcomm

Follow us on:

For more information, visit us at:

qualcomm.com & qualcomm.com/blog

Global Platform™

Management of Post Quantum Crypto

Olivier Van Nieuwenhuyze, STMicroelectronics

Global Platform™

June 20, 2023

Security TF PQC Migration

Olivier Van Nieuwenhuyze

Agenda

Introduction

Solutions

GlobalPlatform

GlobalPlatform Policies

Please be aware that this meeting is being held in accordance with **GlobalPlatform's Bylaws and GlobalPlatform policies issued thereunder,** including but not limited to:

- **Antitrust Policy**
- **IPR Policy**
- **Member Confidentiality Requirements**
- **Meeting Protocol and Guidelines**

Patent Call

"Please be aware that this meeting is being held under the GlobalPlatform Intellectual Property Rights Policy. If you do not have a copy of this policy, please contact (or inform) the chairperson during this meeting. You may also view and download a copy of the policy at the Membership section of the GlobalPlatform Website.

At this time, each person in attendance is required to inform the chairperson if they are personally aware of any claims under any patent applications or issued patents which would be likely to be infringed by an implementation of any specification or other work product which is the subject of this meeting. You need not be the inventor of such patent or patent application in order to inform GlobalPlatform of its existence, nor will you be held responsible for expressing a good faith belief which proves to be inaccurate."

Global Platform™

Introduction

Quantum Computing Threat

The Quantum Computer

QUBIT

BIT
Classical Computing

0
1

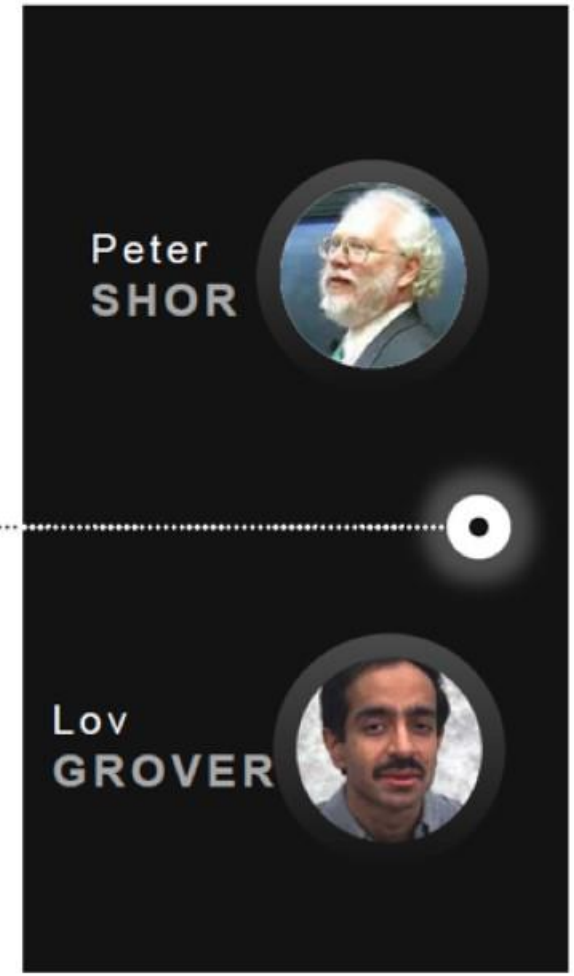
QUBIT
Quantum Computing

0
1

How Quantum Computer Impacts Cryptography?

CRYPTOGRAPHIC ALGORITHM TARGETED	TYPE	PURPOSE	IMPACT FROM LARGE SCALE QC
RSA	Public key	Signatures, Key establishment	No longer secure
Digital Signature Algorithm		Signatures, Key exchange	
ECDSA (Elliptic Curve DSA)			

CRYPTOGRAPHIC ALGORITHM TARGETED	TYPE	PURPOSE	IMPACT FROM LARGE SCALE QC
AES	Symmetric key	Encryption	e.g. longer keys needed
SHA-2, SHA-3	----------	Hash functions	e.g. larger output needed

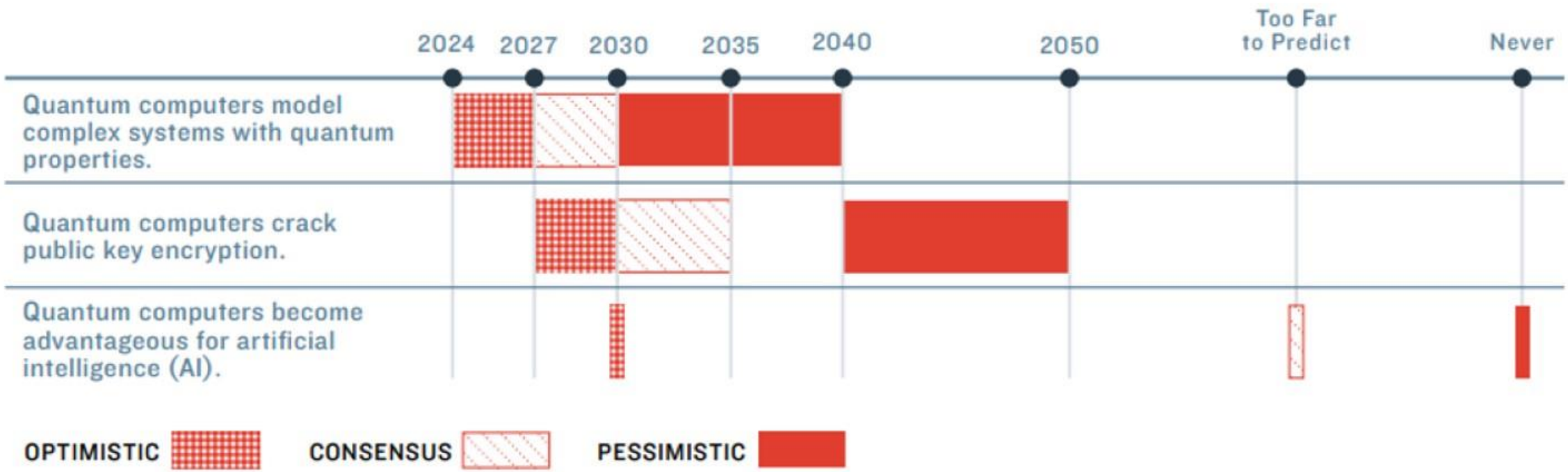


Is this really a problem ?

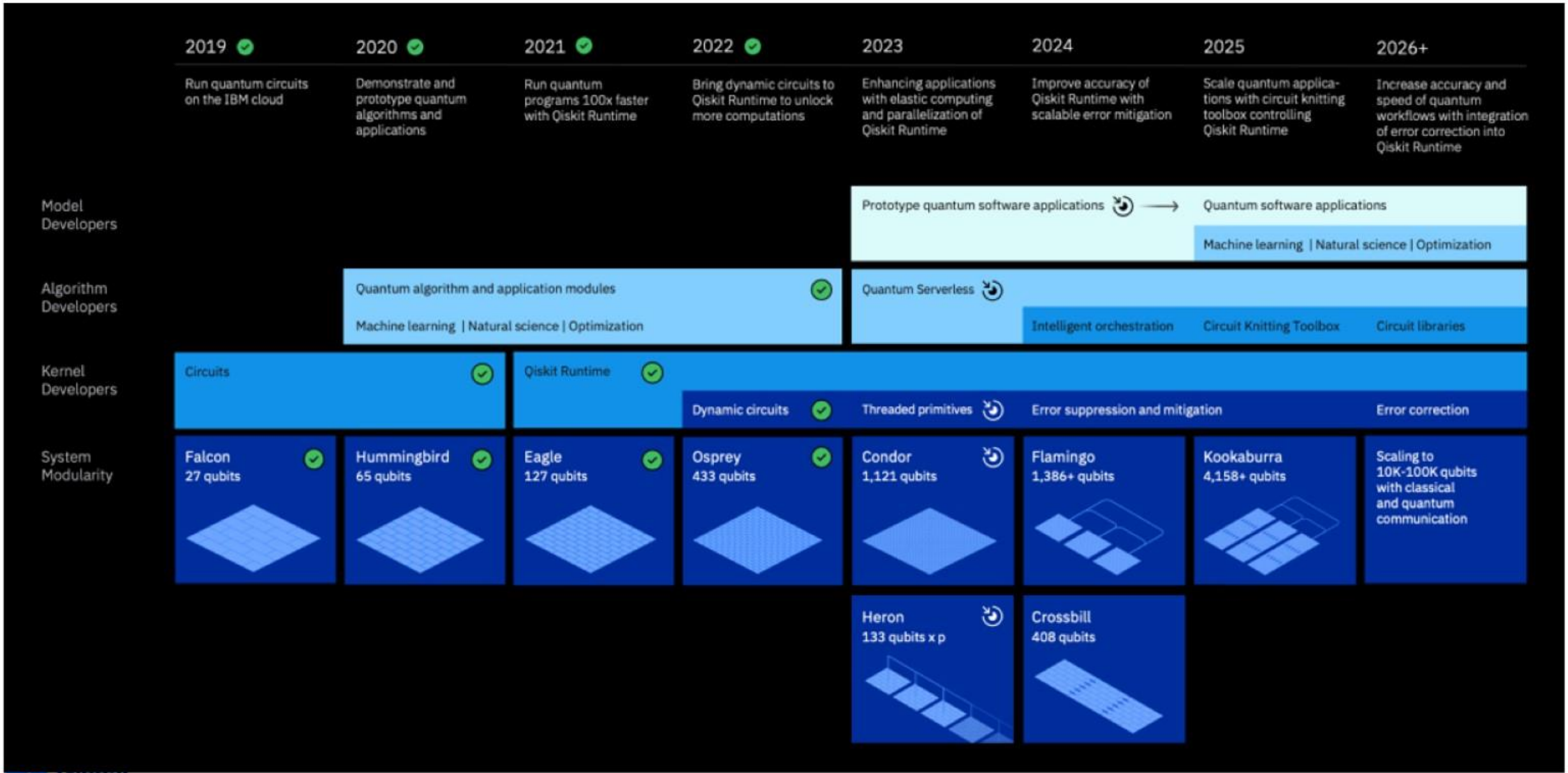
Significant effort to find solution

Time & difficulty to migrate/deploy the solution

Challenge start today as "*Store now, Decrypt later*" attack



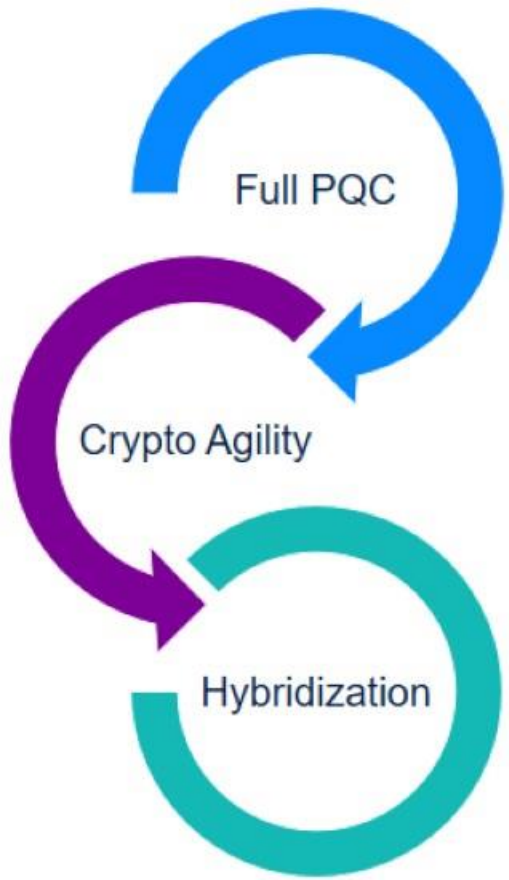
https://www.cisoforum.com/wp-content/uploads/2022/01/chinese-threats-quantum-era.pdf



https://www.ibm.com/quantum/roadmap

Solutions

Solutions



Organizations Standardizing PQC algorithms

Mainly

- NIST (See next slides)
- ISO SC27
- (ETSI CYBER QSC)

China organized a separated competition and already select several post-quantum algorithms.

- LAC and Aigis-Sig won the first prize in 2020.
- https://www.cacrnet.org.cn/site/content/854.html

Russia seems to have its own selection process too.

- No information.

NIST PQC Status

Final selection for standard (July 2022)

- **Crystals-Dilithium** for signature is the recommendation (strong security and excellent performance)
- **Falcon** (to be used when Dilithium signatures are too large) and Sphincs+ (hash-based)
- **Crystals-Kyber** for KEM (strong security and excellent performance)
- Draft standards expected for mid 2023, first PQC standards should be published in 2024 (FIPS & SP)

4th Round candidates for KEM, already including

- **BIKE** (most competitive performance) and **HQC** (strong security assurance, larger key size than BIKE), both based on structured codes, one of which could be standardized
- **Classic McEliece** (secure but too large public key size),
- and SIKE (small key and ciphertext sizes). INSECURE

NIST PQC Status Cont.

NIST issued in September 2022 a request for additional signature algorithms (deadline June 1, 2023)

- Not based on structured lattices (to diversify the portfolio)
- For certain applications, need of short signatures and fast verification

What Is Crypto Agility?

Introduced by

- ETSI in its 2014 white paper on quantum-safe cryptography and security
- as well as The National Institute of Standards and Technology (NIST) in its 2016 report on post-quantum cryptography.

Crypto agility allows for a system or application to migrate to alternate cryptographic algorithms without causing a significant disruption to the infrastructure, allowing security updates to be quickly deployed to fix broken algorithms or replace vulnerable ones.

In short, crypto agility offers the flexibility to meet the changing security needs of our connected world.

The Holy Grail!

Hybrid Cryptography

Hybrid cryptography, sometimes called composite cryptography,

- is a combination using one algorithm from the pre-quantum era, e.g.: RSA, and another algorithm from the post-quantum era, e.g.: one of the signature PQC algorithm from NIST PQC project.
- Thanks to this combination, the security is guaranteed by the security of each algorithm in its proper attack model.
- This level is comparable to the maturity level of RSA in the mid 90's

The maturity level of the post-quantum algorithms should not be overestimated.

- This level is comparable to the maturity level of RSA in the mid 90's

PQC will not become mature with the publication of NIST standards

Hybridization should facilitate the migration and keep backwards compatibility

Different approaches have been proposed and different view from National Agencies

- Hybrid solutions are requested by ANSSI (France) and BSI (Germany)
- Hybrid is encouraged by ENISA (EU) and ETSI (EU)
- Hybrid is discouraged by NSA (US), NCSC (UK) and CSE (Canada)

GlobalPlatform

Crypto Algorithms Recommendation – June 2021

Deprecated 80 bits (or less)	Legacy use 112 bits until 2023	Recommended 128 bits	Under scrutinization
			Reco for PQC 128 ~~/256 bits?~~ (unknown date)
DES 3DES with 2 keys SHA-1 RSA-1024 ECDSA-160 TLS 1.0 and TLS 1.1	3DES with 3 keys SHA-224 RSA-2048 ECDSA-224	AES-128 SHA-256 RSA-3072 EdDSA ECDSA-256 TLS 1.2 and TLS 1.3	AES-128 ~~/256?~~ SHA-256 ~~/384?~~ ?? ??

Global Platform™

GlobalPlatform Impact

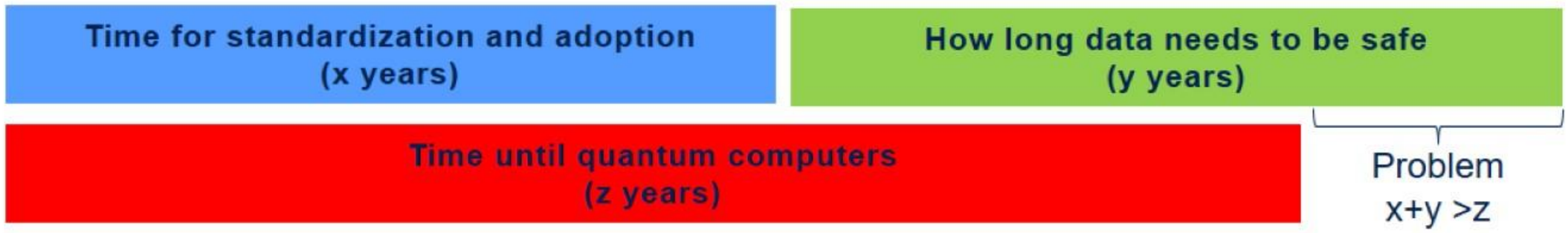
Some actors start asking questions, but the ecosystem is not ready to transition to PQC

Biggest problem is the embedded HW long lifetime

- Cars, Roadside Infrastructure, Charging stations

Main action point might be to deploy fully upgradable SE

Migration strategy – When



Can we extrapolate x, y and z?

- x roughly 2030
- y depends on the use case (telecom < bank < government ~ automotive < defense…) health?
- z? 2050? Never?

Secure Components

Secure Element

Only lattice-based algorithms
are practical on current SE!

Good news, this is what is being
standardized by NIST:

Dilithium and Kyber

Trusted Execution Environment

GP TEE is enabling
all the NIST final candidates
in TEE Internal Core 1.4 specification.

Memory size is typically not an issue in a TEE,
but PQC will be slower than
their classic cryptographic equivalents ….

A strategy for GP, discussion on-going

Hybrid cryptography, sometimes called composite cryptography,

Symmetric Cryptography
- SCP03 : OK, but envisage to double the Key Size

Asymmetric Cryptography needs to evolve
- SCP11 : NOK
- In principle, follow the NIST recommendation
- but also, other algorithms if needed (e.g.: country regulation)

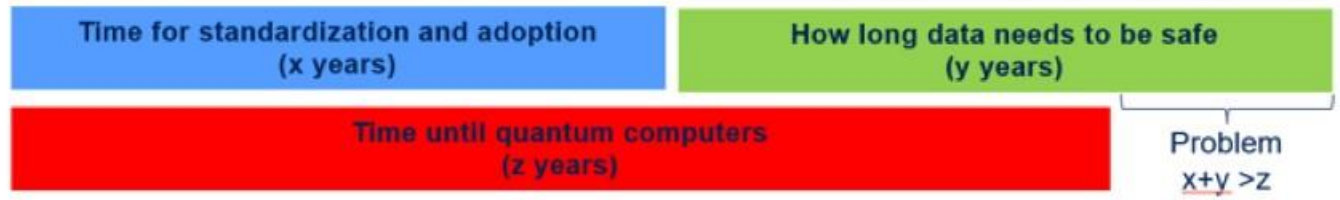
The maturity level of the post-quantum algorithms should not be overestimated.

Having Crypto Agility and OS Update
- SCP 04 is OK
- Be able to download new keys/algorithms with sufficient protection (e.g. to load AES-128 keys Need of 256 bits).

A strategy for GP, discussion on-going Cont.

What is our y?

- Think about lifetime of product, but also development time and certification duration



Support Hybrid Algorithm

- Full PQC
- Or Hybrid PQC (required by some countries)
- Whatever the case and our choice, the device must embed all solutions (classic and PQC), to be able to communicate with the other elements of the ecosystem until all are migrated. This will also ease use of hybridization.

Global Platform™

Regional Considerations

Automotive Task Force

GlobalPlatform: China Task Force

Goals

- Align GlobalPlatform technology with requirements from China,
- Expand GlobalPlatform technology adoption and the certification regime in China.
- Provide input to relevant specifications, compliance and certification programs to GlobalPlatform Committees.
- Identify relevant special Chinese compliance and certification programs within the Chinese market.

Current Priorities

- IoT security standardization, certification, requirements and use cases.
- Develop regional use cases beyond payments for TEE and eSE.
- Liaison with ChinaDRM Forum and the GSMA.

China: Automotive Activities

Developing Liaison Relationship with SAE China

Internal Focus on Automotive within China Task Force

- New Candidate for Vice Chair of China Task Force:
  - Assistant to Secretary General of SAE China
  - Vice President of CSAE Automotive Innovation and Strategy Institute

Regional Cybersecurity Vehicle Forum in China

- October 27th - YiZhuang, Beijing, China
  - In conjunction with SAE China Annual Conference

Input from this Cybersecurity Vehicle Forum for China CSVF?

GlobalPlatform: Japan Task Force

Goals

- Exchange information with Japanese / Asian industry associations and standardization bodies including:
  - Connected Consumer Device Security Council (CCDS),
  - Secure IoT Platform Consortium,
  - Next Generation IC Card System Study Group (NICSS),
  - Association of Radio Industries and Businesses (ARIB),
  - Japan Automotive Software Platform and Architecture (JASPAR),
  - Asian IC Card Forum (AICF) and the
  - Asia Pacific Smart Card Association (APSCA).

Current Priorities

- Continue to liaise with relevant industry associations, including NICSS, oneM2M and TCG.
- Collaborate with Japanese Bodies and identify opportunities to support the security requirements of embedded secure components including MPU.
- Analyze the IoT security requirements of other Japanese bodies in comparison with GlobalPlatform, including CRYPTREC Ciphers List and CCDS.

Japan: Automotive Activities

Creating Automotive Task Force in Japan

Outreach to Key Liaison Organisations:

- JasPar
- JSAE

Japan Cybersecurity Vehicle Forum

- Tokyo September 14th

Draft Agenda – 14th of September - Tokyo

10:00	Welcome
10:15	Presentation of Objectives of the Cybersecurity Vehicle Forum
10:45	Round Robin Introductions
11:15	GlobalPlatform • Overview • Trust Management with Secure Components • Secure Elements • Trusted Execution Environments
12:00	Lunch
13:00	Secure Evaluation Methodology Possible Automotive Certification for UNECE 155
13:20	GlobalPlatform Automotive Use Cases • Secure Components and eSE • Trusted Execution Environments
14:00	Incorporating Flexibility and Agility into Automotive Solutions: Post Quantum Crypto Migration
14:20	Coffee Break

14:50	Future Proofing: Automotive Crypto Agility
15:10	AUTOSAR Crypto API • Key Ownership • Key Access Policies • Key Management System
15:30	Japanese Standardization in Automotive • Software Isolation Security Measure Guidelines • Automotive Use Cases
16:00	Open Discussion • Biggest Opportunities to Support Secure Component Evolution to Fit Automotive Use Cases • Biggest Challenges with ISO21434 regarding product robustness • Understanding the utility of security evaluation methodologies as a support to ISO21434 • Japanese-Specific Market Requirements
16:45	Next Steps
17:00	End of Meeting

Global Platform™

Brainstorming Activities

Francesca Forestieri
Global Platform Automotive Lead

We Want Your Input on Areas for Cross Industry Collaboration

Needed guidelines in applying specifications to automotive use cases

Gaps in specifications directly addressing Automotive requirements

Needed additional specifications

Technology gaps

Areas where Proof of Concepts would be useful to demonstrate the technology in uses

We Want Your Input: Possible Outstanding Requirements

- GlobalPlatform Solutions
  - Secure Elements
  - Trusted Execution Environments
  - TPS APIs
  - Security Evaluation Methodology SESIP
- Certification
  - Functional Certification
  - Security Assurance Certification
- Standards Alignment
  - SAE 3101
  - ISO 21434
  - Autosar
  - C2X
- Liaisons
  - CCC
  - AutoIsac
- Upcoming Requirements
  - Post Quantum Crypto
  - Generation of Evidence for ISO21434
- Regional Questions
  - Europe
  - China
  - Japan
  - Other

New Use Cases for Automotive Security

Electrical Charging

Digital Car Key

Digital Media Protection

Protecting High Value IP (e.g. ADAS)

How to Best Cooperate Cross-Industry:

Better Mechanisms? Key Liaisons Missing?

Join Us!


Follow GP Specs
Leverage mature and interoperable specs
Rely on externally validated certification
Become a GP Member
Obtain early visibility of standards development as the evolve
Help shape the development of standards directly
Plan your roadmap
Leverage security evaluation methodologies

Global Platform™

The standard for secure digital services and devices

→globalplatform.org