GlobalPlatform: Automotive Activities
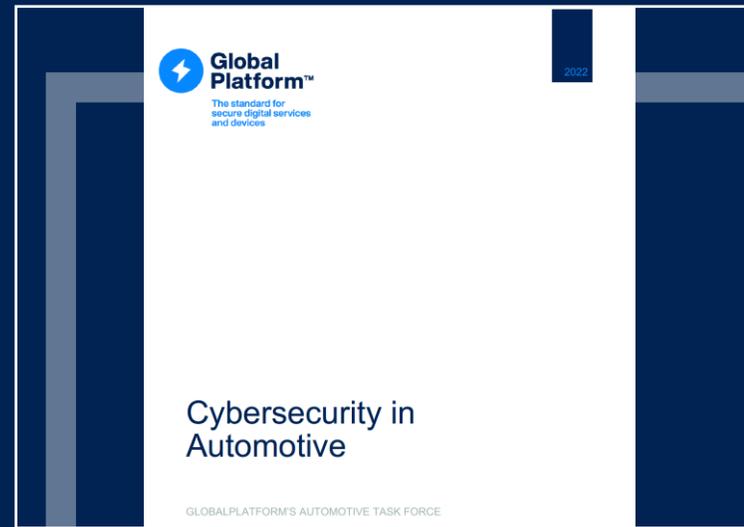
GlobalPlatform Automotive Activities: First Year

Cybersecurity Vehicle Forum

22 Use Cases GlobalPlatform Relevant

35 Use Cases Reviewed

Prioritised 6 lowest hanging fruit

Automotive Task Force
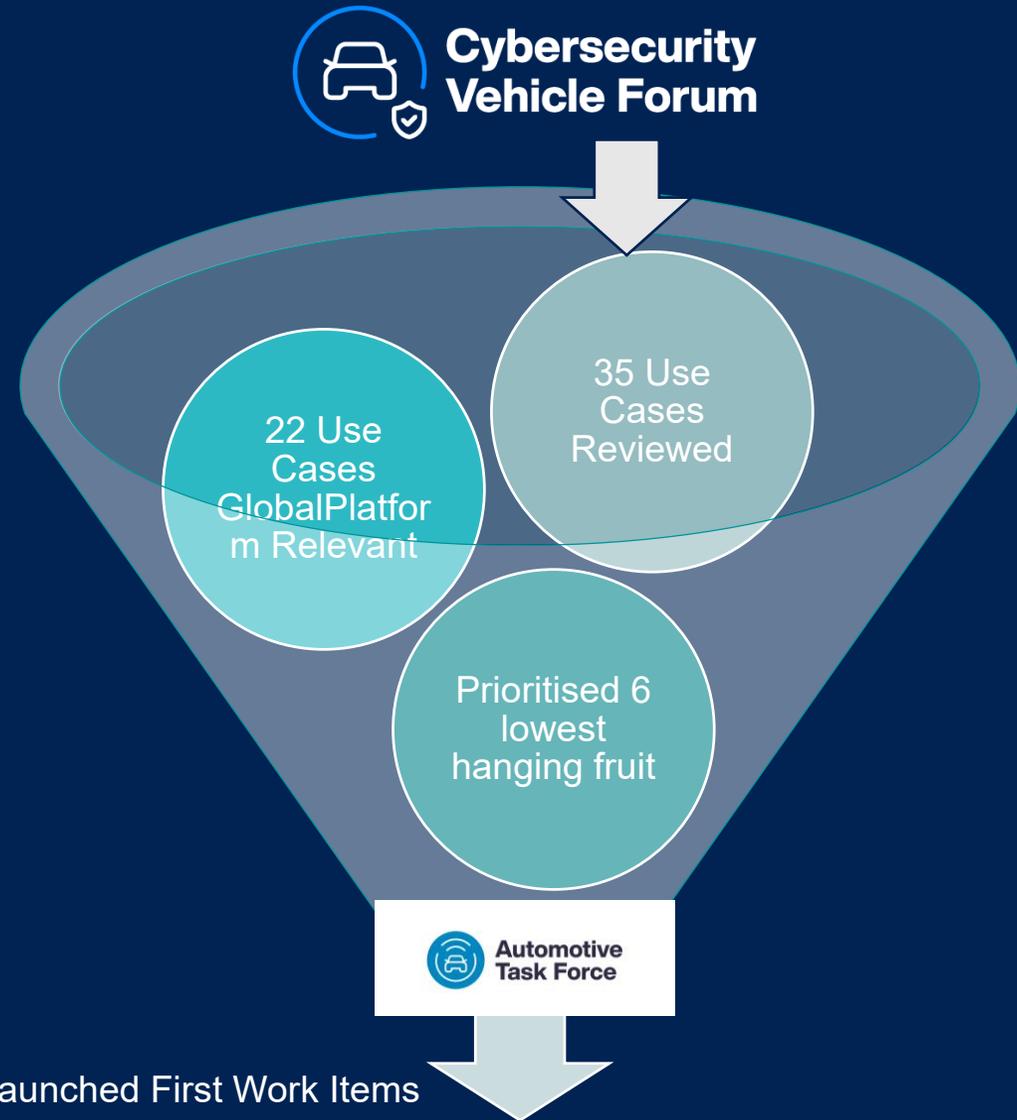
Launched First Work Items

- Standards Alignment:
  - SAE International Hardware Protected Security Mapping J3101
    - Autosar Coordination
- Guidelines on Trust Anchors
  - Security and Trust in Automotive Systems

Global Platform™

GlobalPlatform Whitepapers

Global Platform™
The standard for secure digital services and devices

2022

Cybersecurity in Automotive

GLOBALPLATFORM'S AUTOMOTIVE TASK FORCE

Global Platform®
The standard for secure digital services and devices

COMING SOON!

GlobalPlatform Technology

Trust & Security in Automotive Systems

White Paper
September 2023
GP_WPR_146

Global Platform™

Cybersecurity:
Compliance with UNECE 155 & 156

ISO /SAE 21434 **+** SAE J3101 Hardware Protected Security Environments **=** Cybersecurity Vehicle Management
- Compliance with UNECE 155/156
- Demonstration of Best Practices

Global Platform™

SAE Hardware Protected Security Environments J3101: Common Security Use Case Requirements

Profile	Key Protection 6.2	Cryptographic Algorithms 6.3	Random Number 6.4	Critical Security Parameters 6.5	Algorithm Agility 6.6	Interface Control 6.7	Secure Execution Environment 6.8	Self-Test 6.9
Confidentiality	X	X			?		X	X
Integrity	X	X		X	?		X	X
Availability	X	X			?	X	X	X
Access Control	X	X	X		?	X	X	X
Non-Repudiation	X	X	X	X	?		X	X

NOTE: If algorithm agility is not supported, the profile shall be classified as "limited use" (7.6).

Hardware Protected Security Environments (J3101): Application Use Cases

IPR Protection

Satisfying the requirements of the IP protection use case requires implementation of the base confidentiality profile (7.1).

Secure Diagnosis at the ECU Level

Implementation of the secure ECU diagnostics use case requires implementation of the following profiles:

- Base Confidentiality (7.1):
- Base Integrity (7.2):
- Access Control (7.4):

Additionally, the following profiles should be considered depending on the system implementation:

- Base Availability (7.3):
- Assurance Level (7.7):

Secure Logging

To satisfy the minimum, fundamental secure logging requirements of authentication and non-repudiation, three profiles are required:
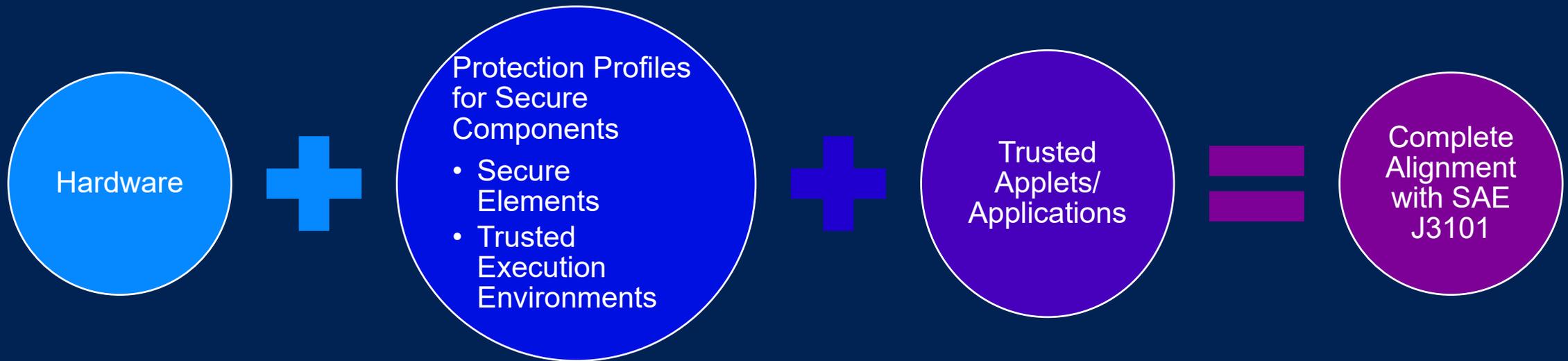
- Base Confidentiality (7.1)
- Base Integrity (7.2)
- Non-Repudiation (7.5)

To satisfy additional security objectives which could be specified for certain usages of secure logging, the following additional profiles may be required and should be considered based on the context provided above:

- Base Availability Profile (7.3)
- High Assurance Level Profile (7.7)

GlobalPlatform Alignment with Hardware Protected Security Environments J3101

Hardware

+

Protection Profiles for Secure Components
- Secure Elements
- Trusted Execution Environments

+

Trusted Applets/ Applications

=

Complete Alignment with SAE J3101

What does this mean for Tier 1s?   *#1/2*

New version

Customer specific

SC App

Answers to J3101
Security Certified

Secure component

Hardware

SC App

Secure component

Hardware

Focus on update

Already done

What does this mean for Tier 1s? #2/2

SC App

New hardware version

Secure component

Answers to J3101
Security certified

Hardware

Value added
SC App

Secure component

Hardware

Already
done

Focus
On SC
update

Global Platform™
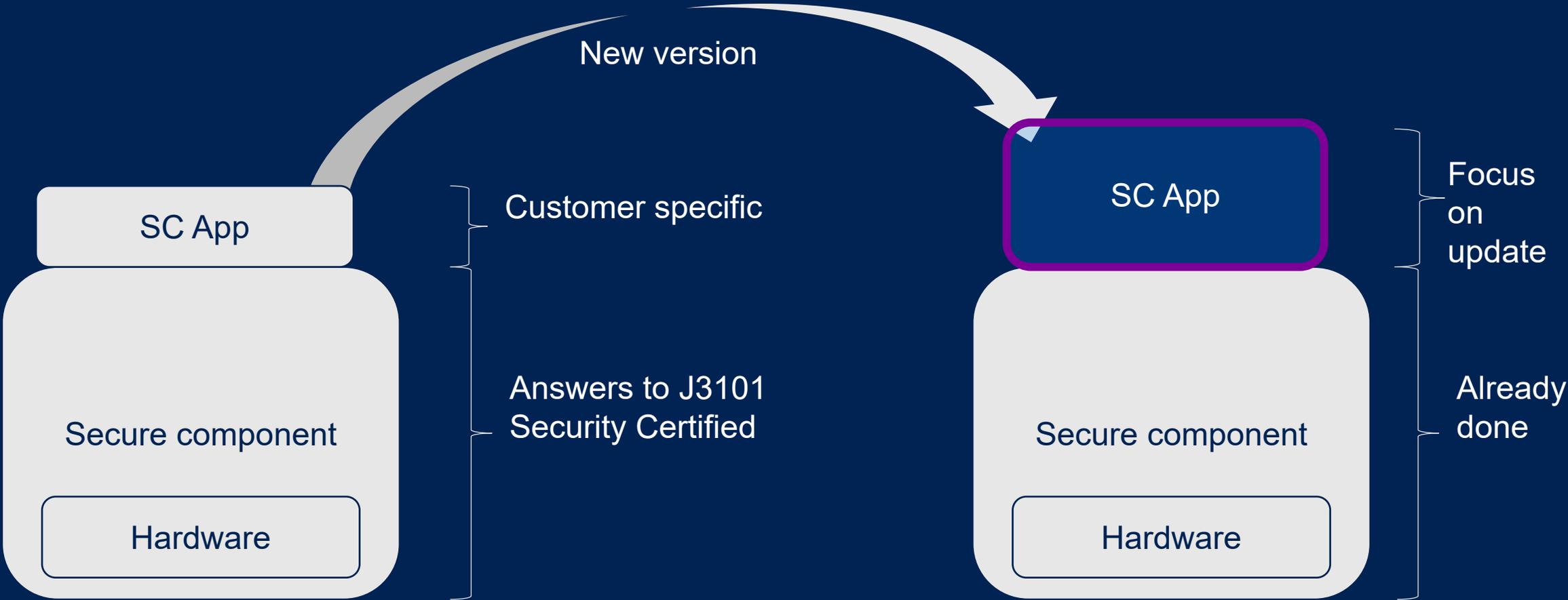
Analysis of J3101 Alignment with GP Specifications

Hardware Isolation Boundaries (met by SE, Possible with a TEE)
3%

Addressed by Trusted Applications/Apps
32%

GlobalPlatform Full Alignment through TEE and SE Protection Profiles
65%
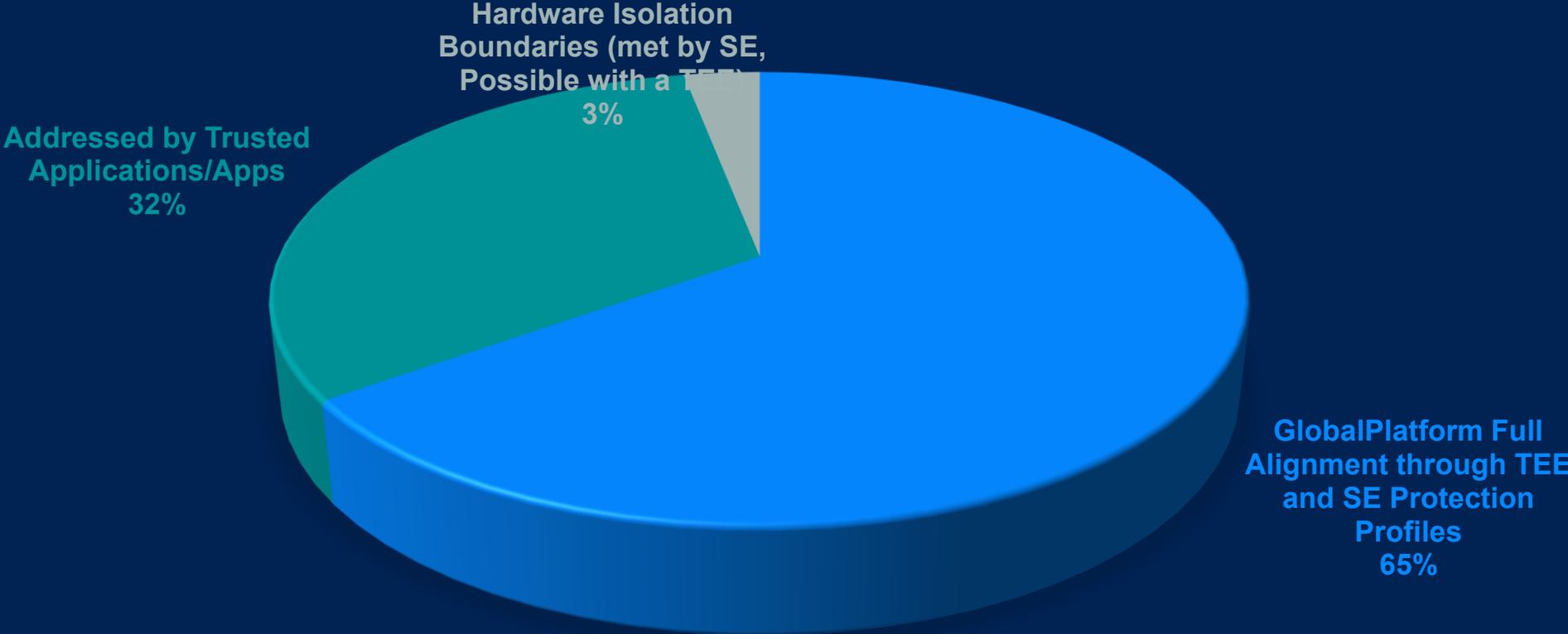
Building Alignment with Standards

Create an Automotive Configuration → Define Requirements for compatibility with AUTOSAR → Identification of Regional Requirements for Automotive Configuration → Align Automotive Configuration → Develop Test Suites for Demonstrating Compliance?

Is there an opportunity to coordinate with Japanese organisations on this work?