life.augmented

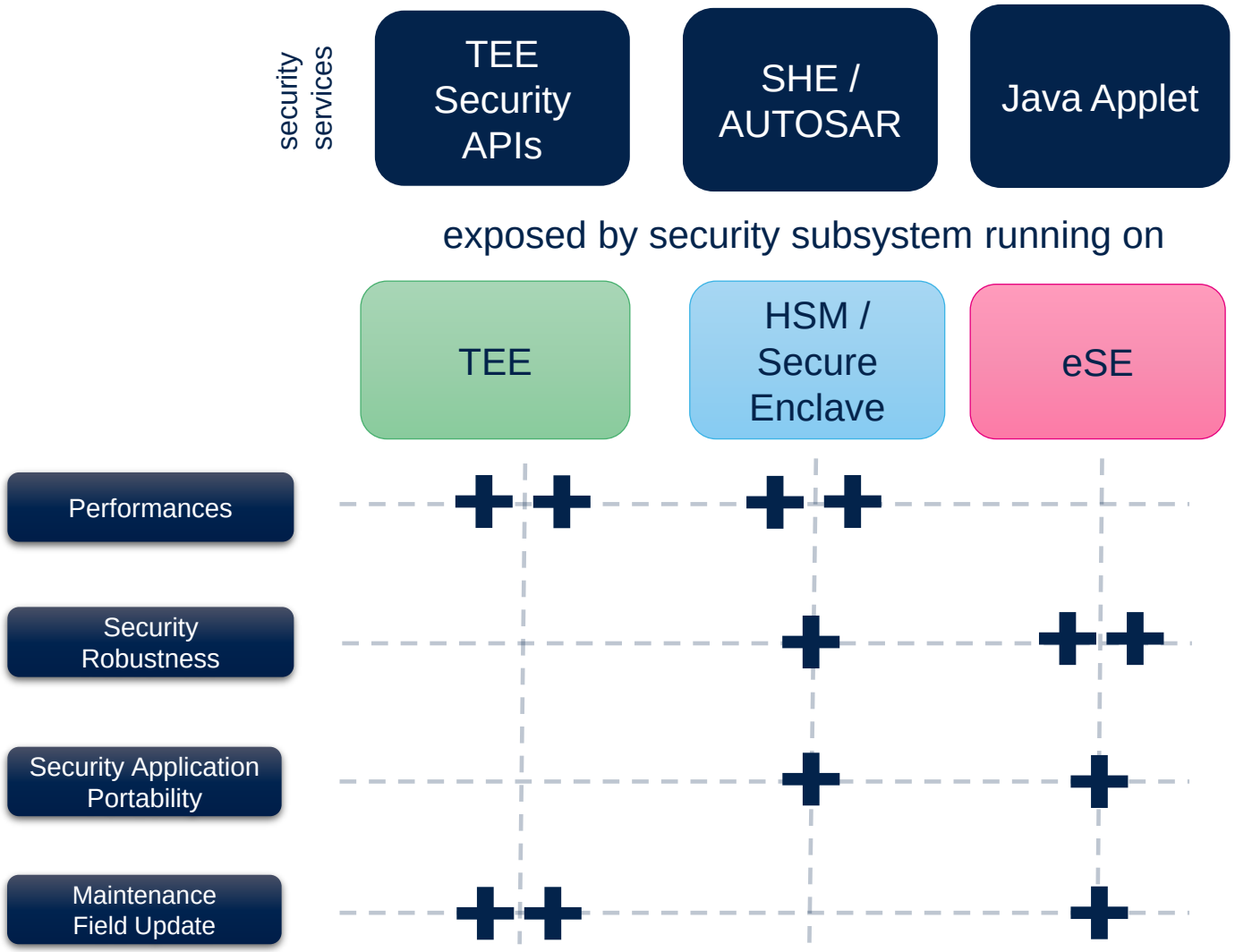
GlobalPlatform ATF Toolbox
Security Convergence

Laurent TABARIES

STMicroelectronics – GlobalPlatform meeting

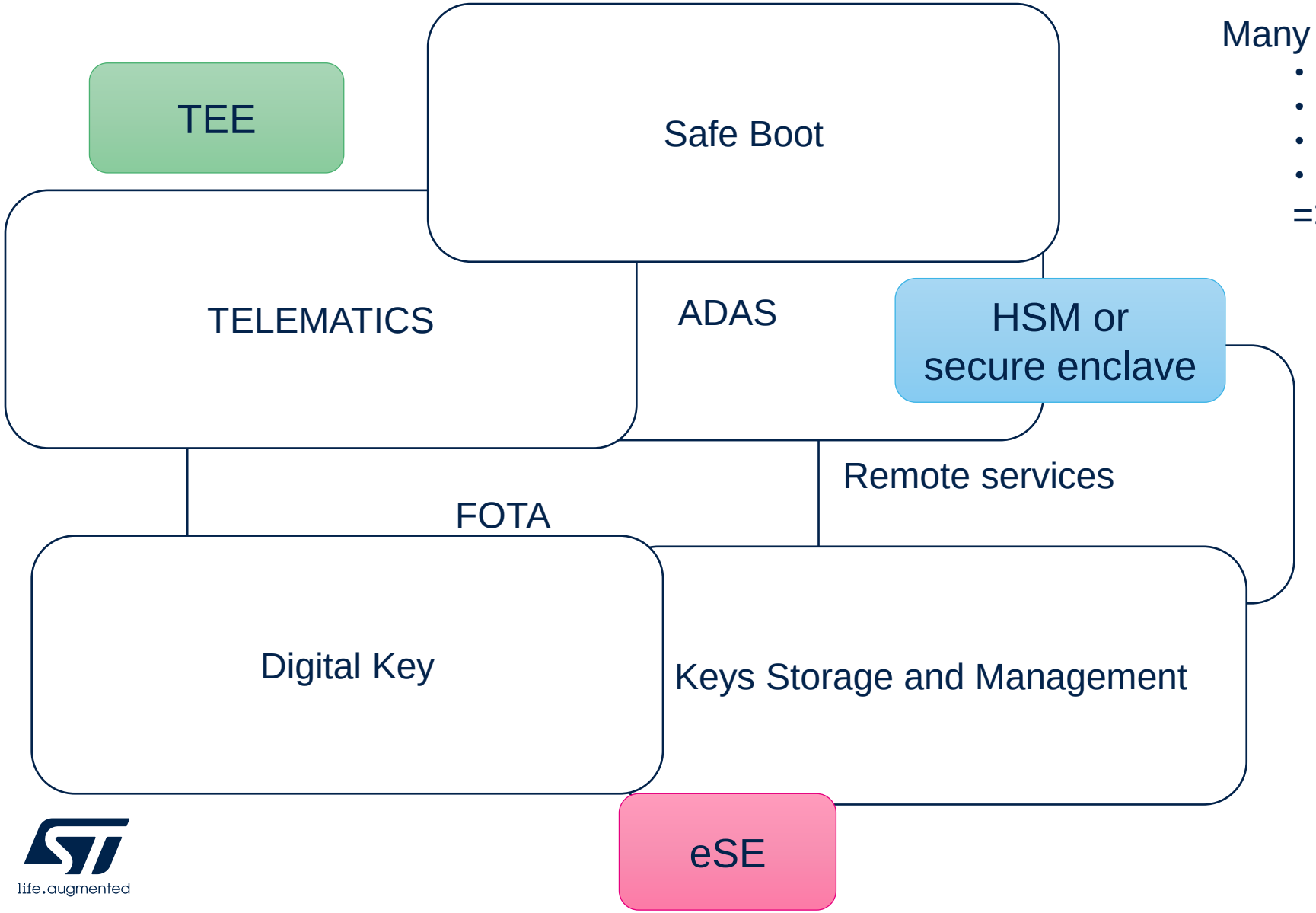
24th October 2024, Tokyo

Automotive security subsystem panorama



NB: This analysis is given as an high level overview and could be redefined according to a vote organized during any ATF meeting

Automotive security different use cases



Many use cases with different

- Definitions
- Expectations
- Constraints
- Environments

=> Non unique solution

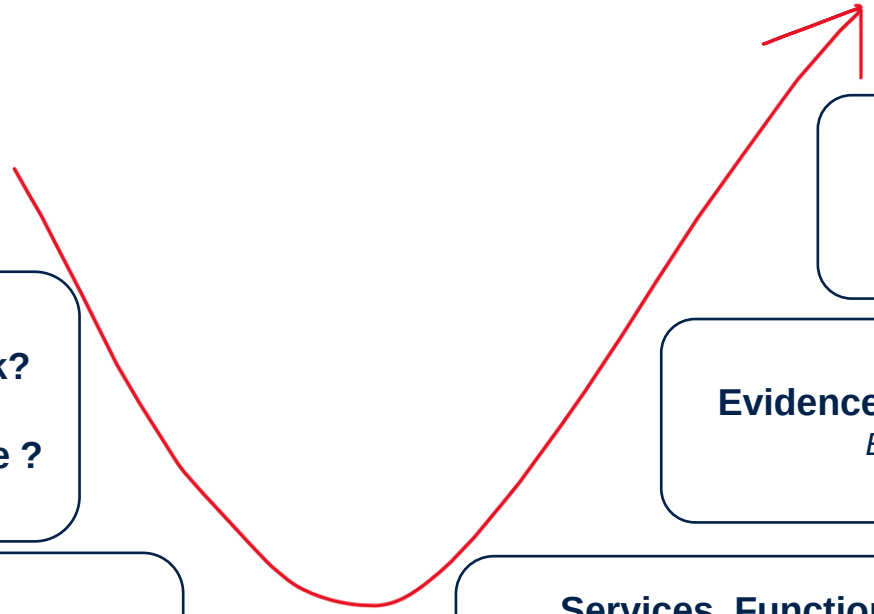
life.augmented

Use Cases “security needs” driven by

Standard (or Protection Profile) requirement
Ex: Qi, Digital Key CCC, V2X, GBA

Self assesment Analysis (use case dependant)
Security robustness : Remote or Board level Attack?
What is the asset to protect ?
Field update (patch or data perso) level of insurance ?
Ex: UWB Anchor or Lidar located in the bumper

System level integration with correlations ?
Ex : ADAS with mutiple sensors inter-connected with supervision or Battery Passeport with regular cloud connection



Easy deployment and usage
Ex: SCP or SPI GP T=1

Evidence of security level reached
Ex: SESIP level 3 or 4

Services, Functions and API availability combined with customization capabilty
Ex: Few custom functions for maintenance purpose or for proprietary legacy crypto scheme

What is the starting point, or what are the legacy constraints ?
Ex: solution EVITA with Autosar to implement new crypto function
What are the missing points and what is the rational of the change ?
Ex: Generate localy (in the Telematic Control unit)
2 applicative keys derived from a master keys received from the OEM server
Ex: Crypto or MAC flexibility might not be compatible with frozen functions available in EVITA

life.augmented

Field typical request

HSM or secure enclave

+

eSE or TEE

Ex: EVITA_full (CSM Autosar APIs) available with conservative approach
***but** new crypto algo could miss*
*or **new request** to automatize some functions*
*or **reinforce** security robustness*

Ex1: to extend EVITA FULL with new specific crypto algo

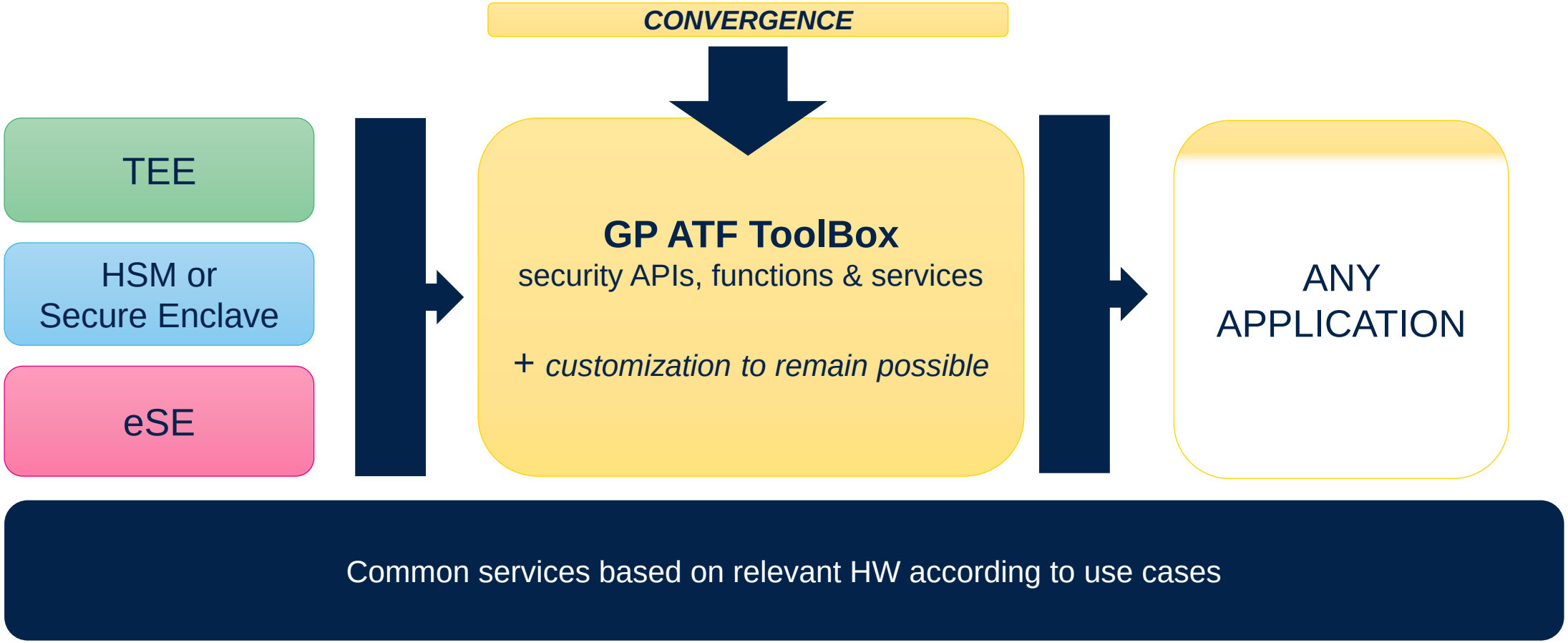
Ex2: Key Derivation Function automatized (HKDF)

Ex3: Create a robust RoT to validate paltform integrity at Boot

Mainstream OEMs/Tiers1 request is to add services/functions/APIs on top of existing solution HSM based to improve flexibility and/or security robustness

But many OEMs/Tiers1 do not know how to start ?

GP ATF Toolbox to help security convergence



GP could help to define a set of APIs, functions and services
as a **Automotive ToolBox superset**

GP ATF Toolbox in 3 steps

To identify and list mainstream APIs, functions and services :
- RoT
- Key Derivation and Key Management
- Data Personalization (with Security Domain)
- Mainstream Crypto, MAC, Hash functions
- Remote services (to leverage on top of SCP and SPI/I²C GP T=1)
- Etc ….

To formalize a GP specification (thanks to GP ATF)
and setup draft JVC Applet (on top of default JVC 3.0.5)
with incremental approach based on regular field feedbacks
to improve to solution set

To implement such GP ATF ToolBox Applet POC
- provide performance improvment metrics
- provide easy guide to ease porting and adoption
=> mainly focused on HSM, used as a proxy, to extend solution « GP ATF ToolBox » based