Automotive Cybersecurity: It's More Than Just Cryptography

NXP Tech Day – Paris

November 21st, 2019

Fabrice Poulard – Automotive Security Expert Group

NXP | SECURE CONNECTIONS FOR A SMARTER WORLD

Autonomy

Electrification

Connectivity

Global Mobility

Enabled by Safe and Secure Systems

Cybersecurity: Cryptography & More

Threats?

Crypto-Agility?
Future Proof?

Incident Response?

Key Management?

Cryptography

Essential Cybersecurity Toolbox

Root-of-Trust?

System Integration?

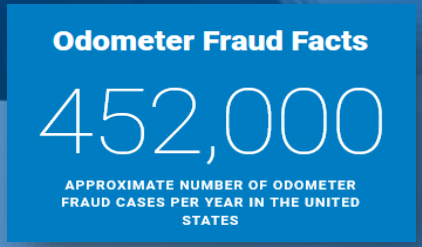
Platform Security?

Standards?
Compliance?

A Glimpse at Cybersecurity Threats in Automotive

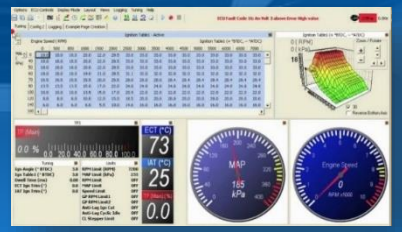
Local Attacks → Remote Attacks

Tampering the odometer



https://www.nhtsa.gov/equipment/odometer-fraud

Engine tuning



Workshop around the corner, or in your garage

Vehicle theft by relay attack

https://www.youtube.com/watch?v=8pffcngJJq0

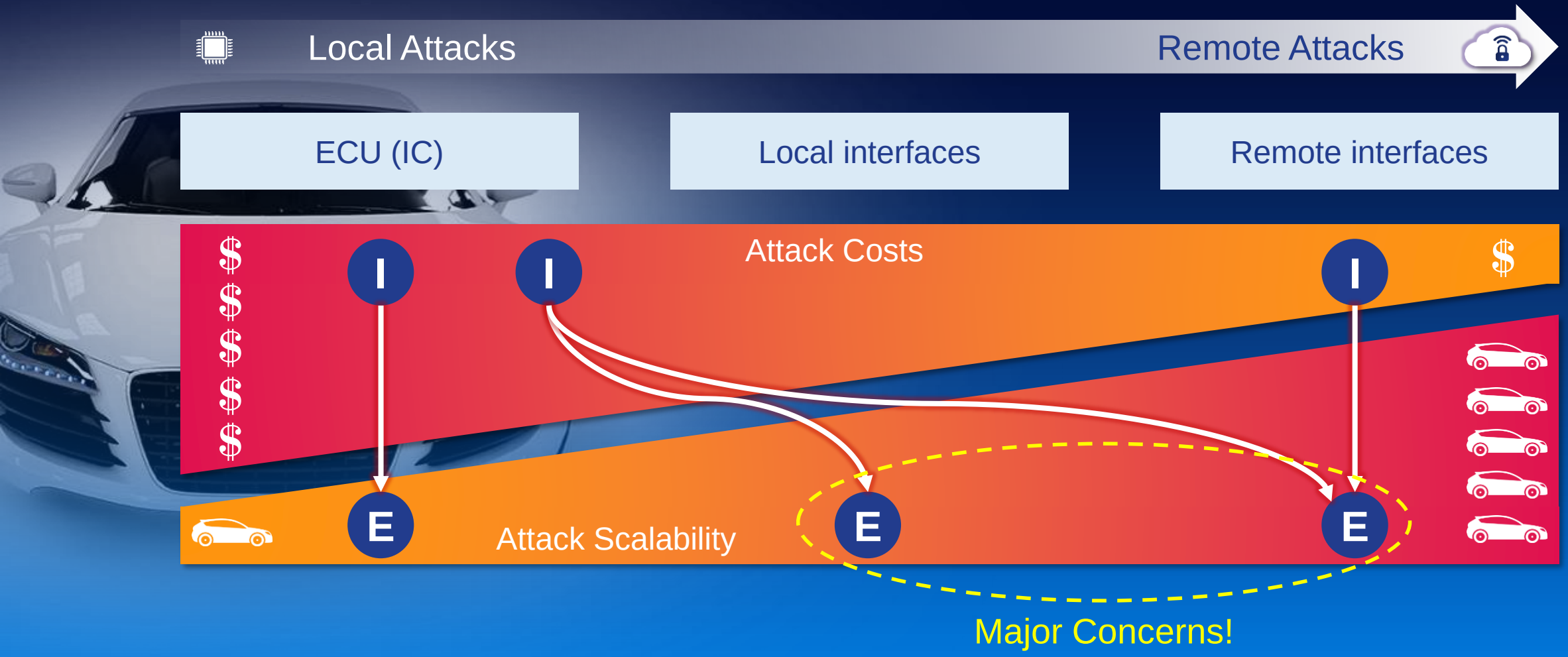
Ransom for a drive

VDI Conference on IT Security for Vehicles
(Berlin / July 2017)

Remote hack of an unaltered car (July 2015)

https://www.youtube.com/watch?v=MK0SrxBC1xs

Cyberattack Costs vs. Scalability



I Identify vulnerability

E Exploit vulnerability

Security Measures

Local Attacks → Remote Attacks

ECU (IC)	Local interfaces	Remote interfaces

Resistance to **Local Attacks**

Core Security Principles

- Secure **External Interfaces**
- Secure **Domain Isolation**
- Secure **Internal Communication**
- Secure **Software Execution**

Secure Foundations (HW + FW)

Secure **Solutions & Services**

Holistic Approach – Solutions

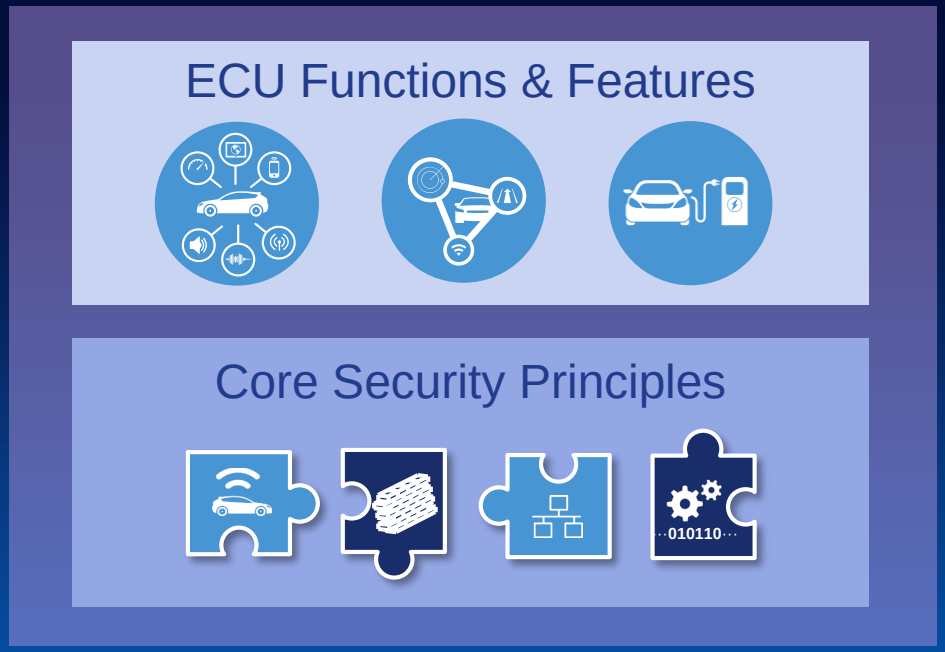
	PREVENT access	DETECT attacks	REDUCE impact	FIX vulnerabilities
Secure Interfaces	M2M Authentication & Firewalling	Intrusion Detection Systems (IDS)		Secure Updates
Secure Domain Isolation	Firewalling (context-aware message filtering)		Separated Functional Domains	
Secure Networks	Secure Messaging		Message Filtering & Rate Limitation	
Secure Processing	Code / Data Authentication (@ start-up)	Code / Data Authentication (@ run-time)	Resource Control (virtualization)	

Holistic Approach – Solutions and Organization

	PREVENT access	DETECT attacks	REDUCE impact	FIX vulnerabilities
Secure Interfaces	M2M Authentication & Firewalling	Intrusion Detection Systems (IDS)		Secure Updates
Secure Domain Isolation	Firewalling (context-aware message filtering)		Separated Functional Domains	
Secure Networks	Secure Messaging		Message Filtering & Rate Limitation	
Secure Processing	Code / Data Authentication (@ start-up)	Code / Data Authentication (@ run-time)	Resource Control (virtualization)	
Secure Engineering	SDLC incl. Security Reviews & Testing, …	Threat Monitoring, Intelligence Sharing, …	Incident Management / Response	
	Security-Aware Organization, Policies, Governance			

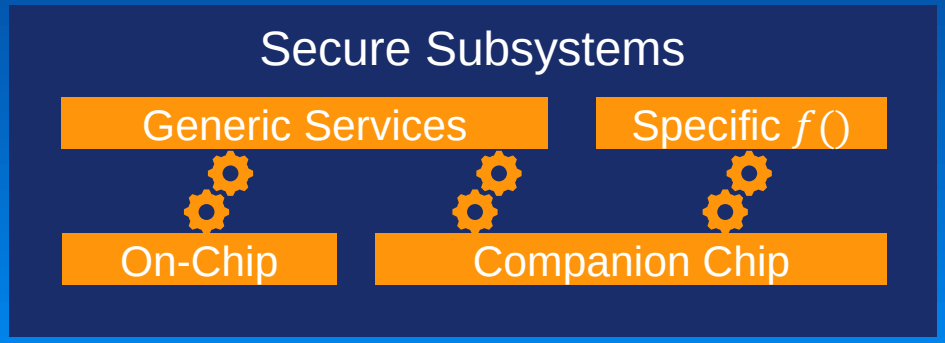
Anatomy of a Secure Automotive ECU

Application Domain
Complex Subsystems
Multiple Processing Elements
Multiple Interfaces

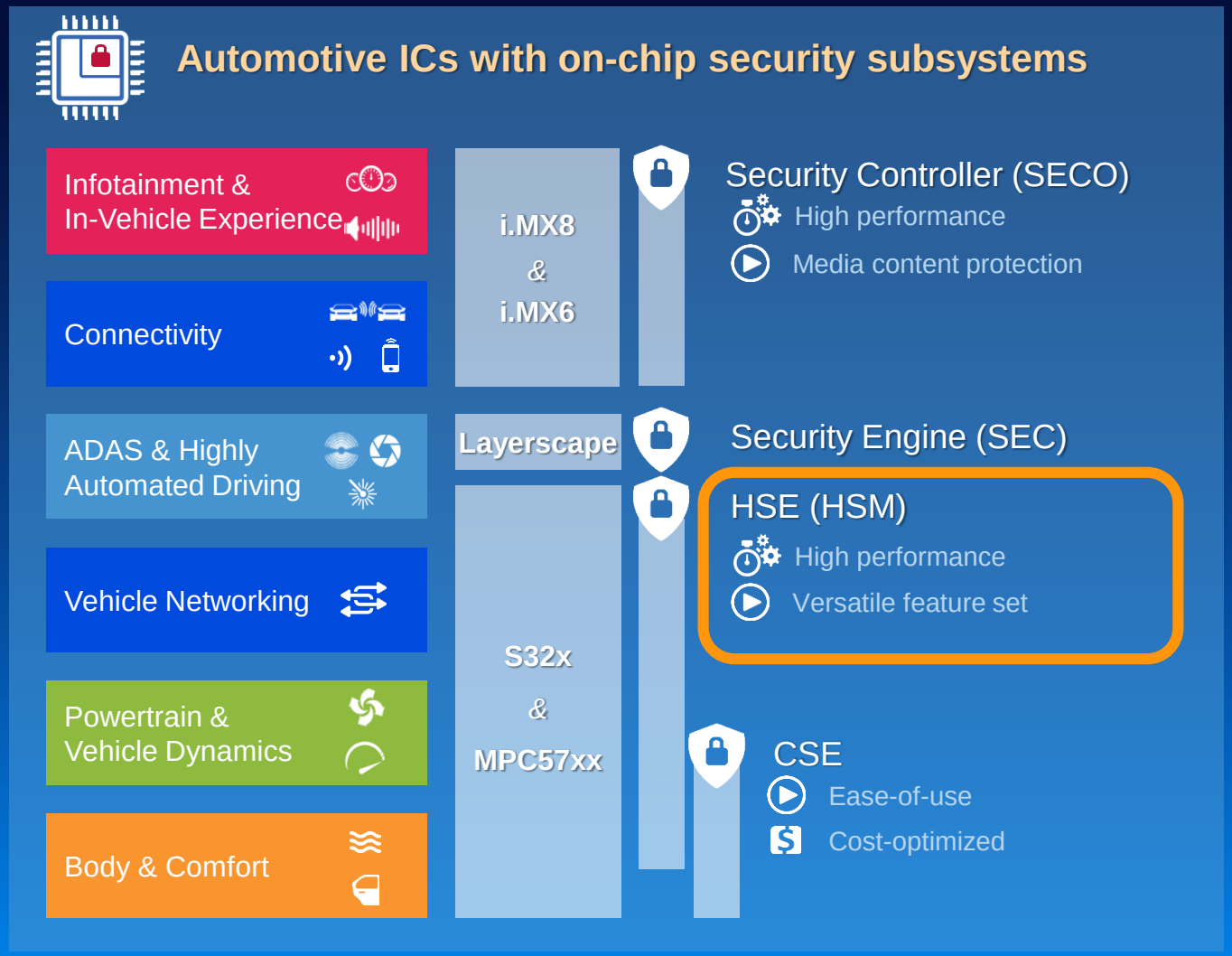


Hardware Enforced Isolation

Secure Domain
Resistance to Local Attacks
Root of Trust
Acceleration of Security Primitives



NXP's Automotive Security Solutions



On-chip Secure Subsystems

Generic Set of Services

High Performance

Platform Control

S32's On-Chip Secure Subsystem: HSE

Accelerates

Cryptographic Operations

Conceals

All Secret Keys

Establishes Trust

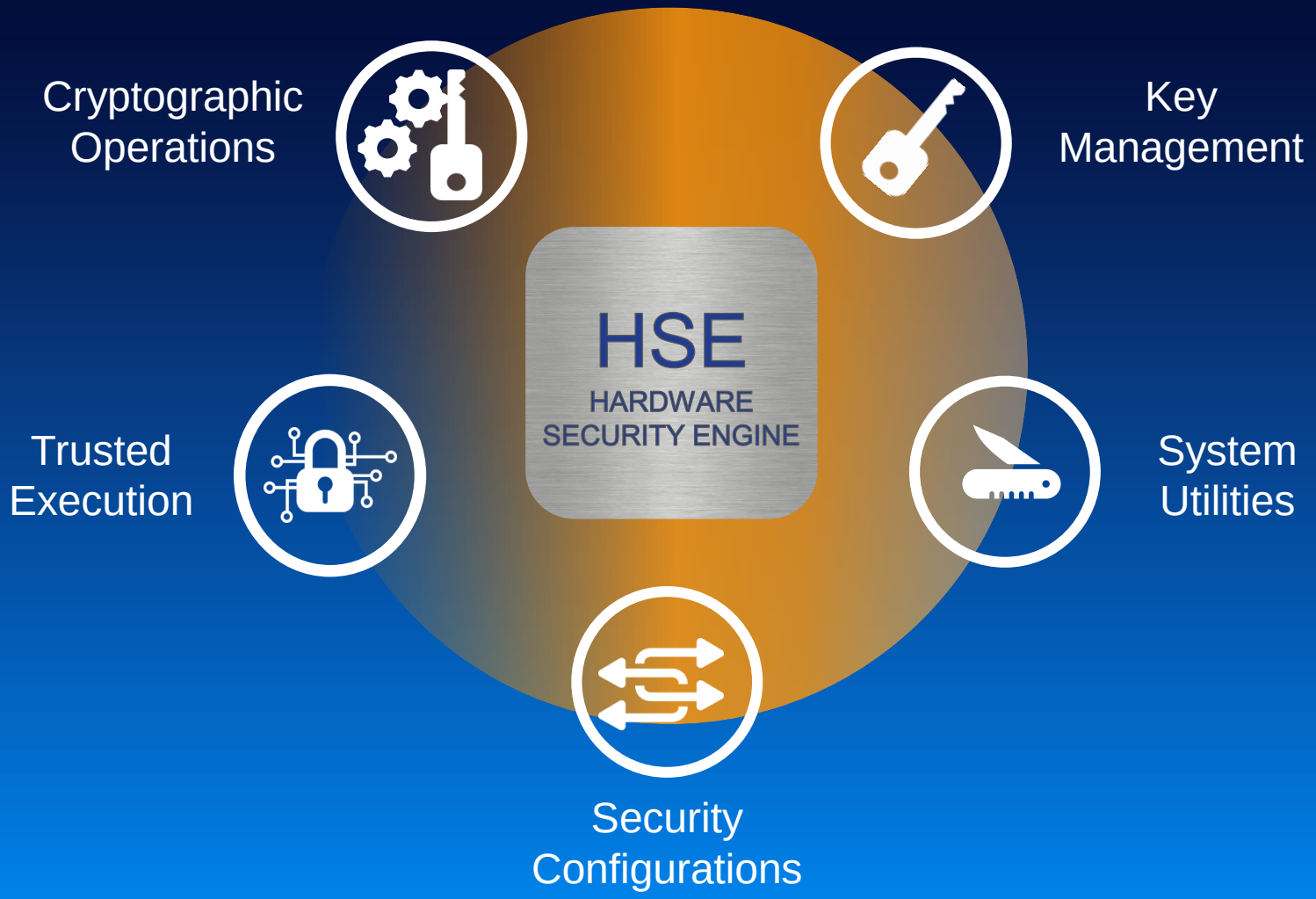
Secure Boot + Root of Trust

Easily Integrates

In Your Design

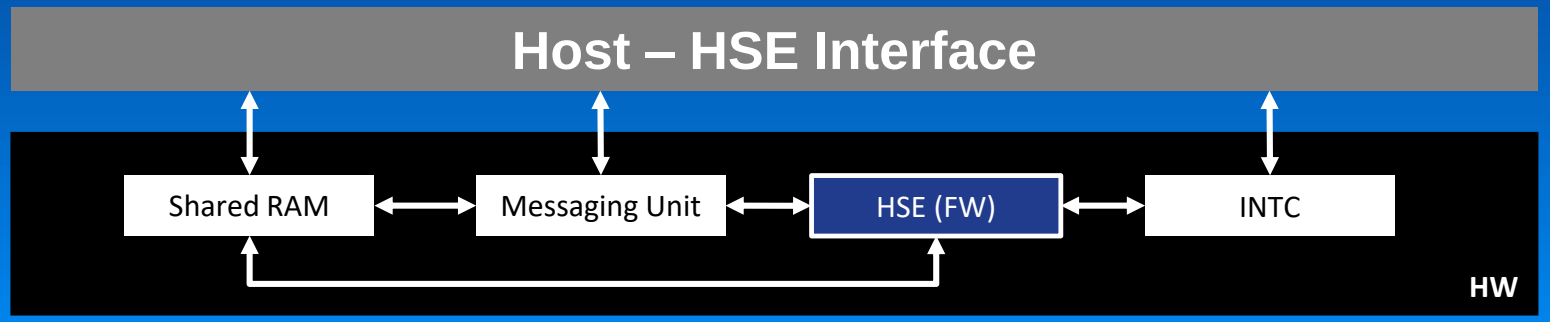
Adapts

Through Secure Updates



Integrating NXP's HSE in Standard Security Stacks

- Rich Service API
- Multi-Thread Ready
- Buffer-free Interface
- Domain Separations

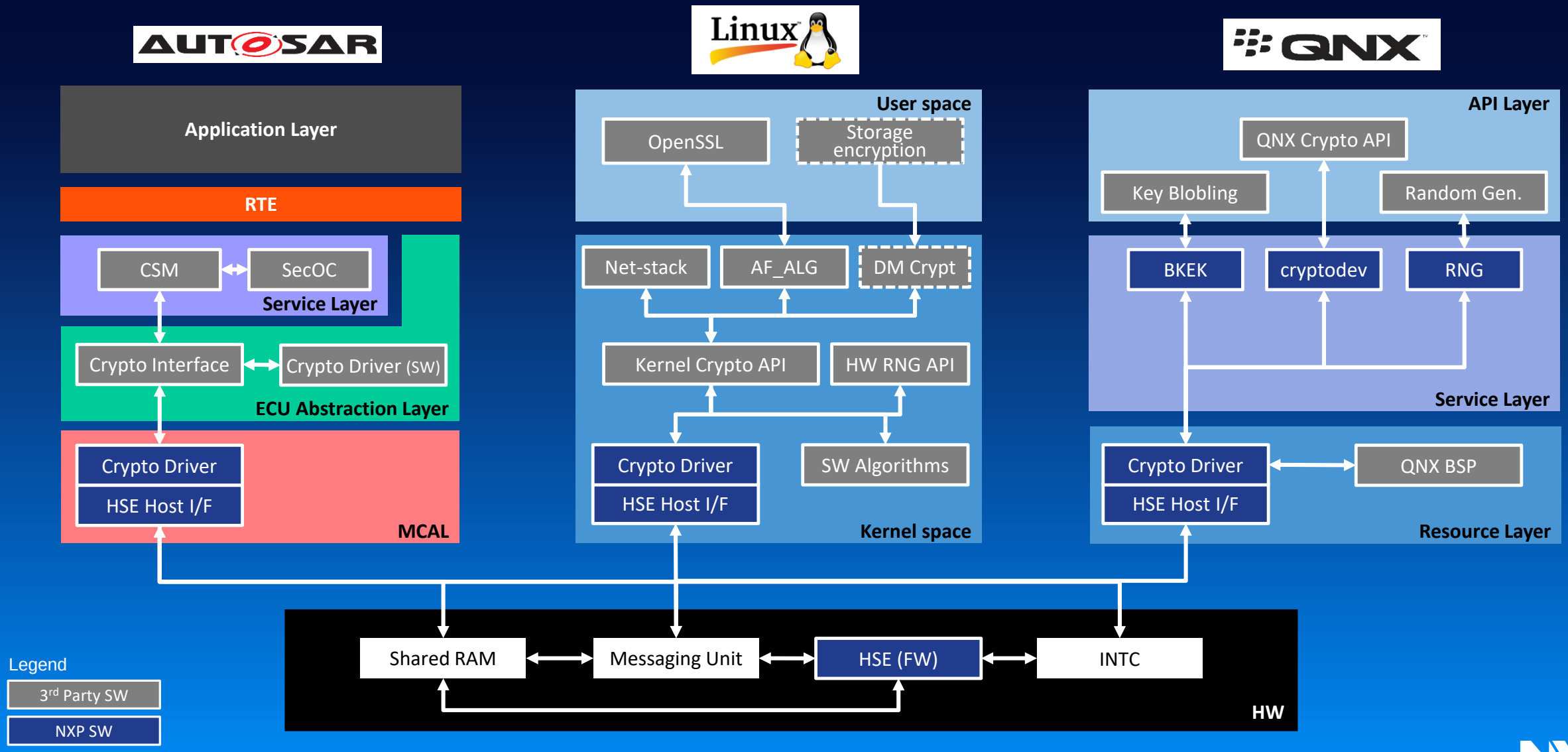


Legend

3rd Party SW

NXP SW

Integrating NXP's HSE in Standard Security Stacks



HSE: Three Main Service Classes

Key Management

- Key file management
- Key import
- Key export
- Key generation
- Key derivation
- Key exchange

AES key up to 256 bits
RSA key up to 4096 bits

Cryptographic Operations

- AES
  Encryption & decryption
- CMAC / HMAC
  Generation & verification
- Hashing (SHA2 & SHA3)
- RSA / ECC signature
  Generation & verification
- RSA OAEP / ECIES
  Encryption & decryption
- Random generation

All operations
HW accelerated

Secure Boot Secure Use

- Strict secure boot
  Verify then start
- Parallel secure boot
  Start then verify
- On-demand verification
  Secure boot control in app.
- Configurable sanctions
  E.g. key usage restrictions

Secure boot
optimized for speed

Your Key Benefits With NXP's HSE Solution

One-Stop-Shop
NXP responsible for the complete solution

Off-the-shelf Enablement

Optimum Performances

Optimum Security Assurance Level

Faster Time-to-Market
Firmware availability aligned with customer samples

Custom Extensions If Required

NXP's Automotive Security Solutions

Automotive ICs with on-chip security subsystems

- Infotainment & In-Vehicle Experience
- Connectivity
- ADAS & Highly Automated Driving
- Vehicle Networking
- Powertrain & Vehicle Dynamics
- Body & Comfort

i.MX8 & i.MX6

Security Controller (SECO)
- High performance
- Media content protection

Layerscape

Security Engine (SEC)

S32x & MPC57xx

HSE (HSM)
- High performance
- Versatile feature set

CSE
- Ease-of-use
- Cost-optimized

Security companions

Secure Element (SE)

Tamper-resistant secure system ideal for M2M authentication (e.g. V2X)

Stand-alone Secure Subsystems

Generic Set of Services

High-resistance Against Local Attacks

NXP’s Automotive Secure Element Certified against CC

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Schéma français d’évaluation et de certification de la sécurité des technologies de l’information

CERTIFICAT ANSSI-CC-2018/60

Ce certificat est associé au rapport de certification ANSSI-CC-2018/60

Produit NCJ38A0 B0.207

Développeur : NXP Semiconductors

Critères Communs version 3.1 révision 4

EAL5 Augmenté

(ADV_IMP.2, ADV_INT.3, ADV_TDS.5, ALC_CMC.5, ALC_DVS.2, ALC_FLR.1, ALC_TAT.3, ATE_COV.3, ATE_FUN.2, AVA_VAN.5, ASE_TSS.2)

conforme au profil de protection
Security IC Platform Protection Profile with Augmentation Packages, version 1.0,
certifié BSI-CC-PP-0084-2014

Commanditaire : NXP Semiconductors
Centre d’évaluation : Serma Safety & Security

Paris, le 9 janvier 2019

Le directeur général de l’agence nationale de la sécurité des systèmes d’information
Guillaume POUPARD
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

Dans le cadre du CCRA, le produit est reconnu au niveau EAL2.

Ce certificat est émis conformément au décret 2002-535 du 18 avril 2002 modifié relatif à l’évaluation et à la certification de la sécurité offerte par les produits et systèmes des technologies de l’information.

Secrétariat général de la défense et de la sécurité nationale, Agence nationale de la sécurité des systèmes d’information 51, boulevard de La Tour-Maubourg, 75700 PARIS 07 SP

NXP's Automotive Security Solutions

Automotive ICs with on-chip security subsystems

- Infotainment & In-Vehicle Experience
- Connectivity
- ADAS & Highly Automated Driving
- Vehicle Networking
- Powertrain & Vehicle Dynamics
- Body & Comfort

i.MX8 & i.M

Security Controller (SECO)
- High performance
- Media content protection

Layer

S32x & MPC57xx

- High performance
- Versatile feature set

CSE
- Ease-of-use
- Cost-optimized

Stand-alone IC

Specific Set of Services

Optimized for the Target Function

Security companions

Secure Element (SE)
- Tamper-resistant secure system ideal for M2M authentication (e.g. V2X)

Function-specific secure ICs

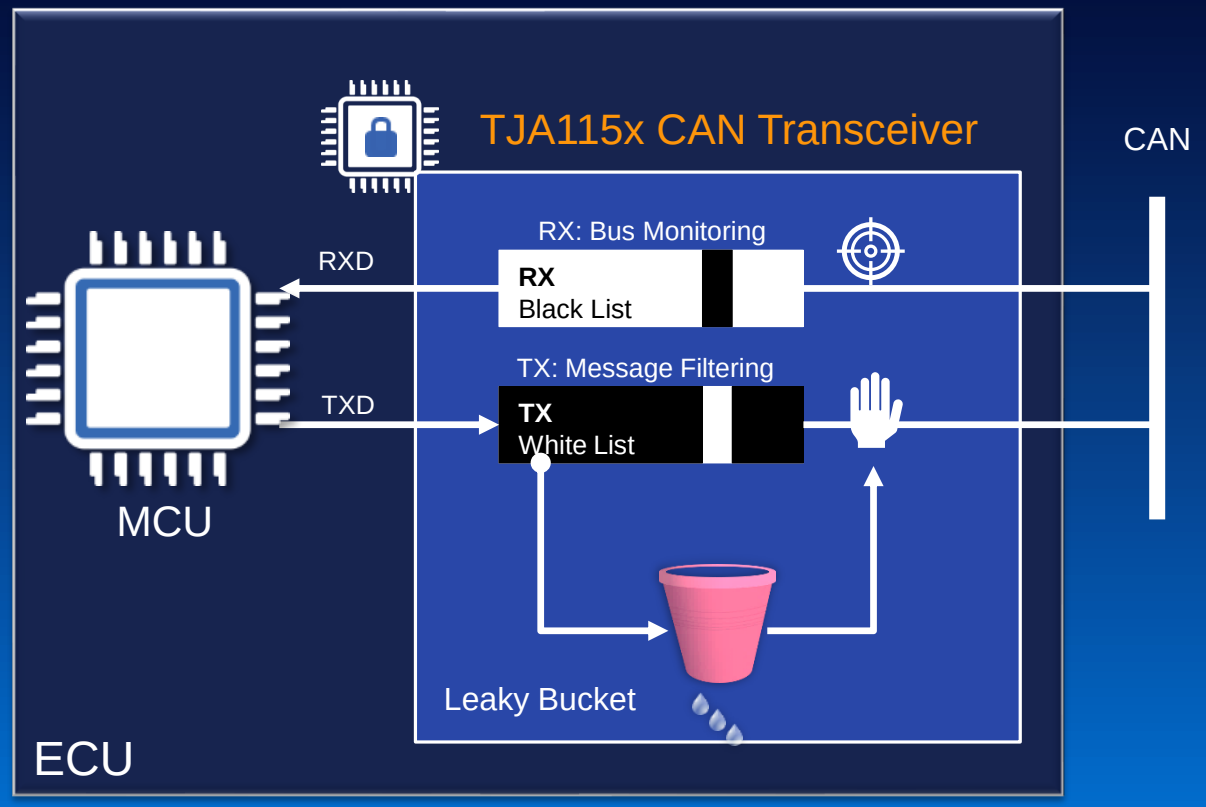
Secure CAN Transceiver (TJA115x)
- For enhanced IDS & IPS

Secure Ethernet Switch
- Network frame analysis (L2/L3/L4)

Secure Car Access ICs
- For advanced RKE / PKE solutions

V2X DSRC Baseband (SAF5x00)
- Ultra-fast ECDSA verifications

Function-specific Secure IC: Secure CAN Transceiver



Simple CAN transceiver replacement

Pure hardware based solution (no software)

On-the-fly CAN ID whitelisting & blacklisting

Flooding prevention by leaky bucket principle

Immediate intrusion containment

Secure in-field reconfiguration possible

Function-specific Secure ICs: Secure Car Access Solutions

Immobilizer Authentication for Engine Start	Transponde TP	1. LF Challenge 2. LF Response	Base station BS	
Remote Keyless Entry On-demand Authentication	RF Tx µC TP*	RF signal (rolling code) (on Button press) *Immobilizer function included	RF Rx BS*	
Passive Keyless Entry Hand-free, with Distance Bounding	LF Rx µC TP* RF Tx*	1. LF Wake-Up/Challenge 2. RF Response *Immo/RKE function included	LF Tx BS* RF Rx*	
Smart Car Management 2-way RF & Distance Bonding	RF Tx/Rx µC	RF Data Exchange	RF Tx/Rx µC	
Smart Access (mobile devices) access via NFC/BLE-enabled devices	BLE NFC eSE	Secure Data Exchange (e.g. CCC Digital Key)	BLE NFC eSE	

Introducing Ultra-Wideband (UWB) in Automotive

- **Protection against car theft**
  Security: ultimate countermeasure against relay attacks
- **Door lock user recognition**
  Convenience: individual movement pattern granting access
- **Child seat positioning**
  Safety: accurate guided positioning of the child seat
- **Trailer recognition**
  Convenience: approach-triggered trailer hitch
- **Easy trunk opening**
  Convenience: approach-triggered trunk opening

Going further https://www.youtube.com/watch?v=6Y8rgUD7DL4

NXP's Holistic Approach to Product Security

Secure product engineering process
Internal / external security evaluation (VA)

Broad portfolio of security solutions
(HW & SW / FW)

Product Security IR Team (PSIRT)
Security-aware organization
Threat intelligence feed

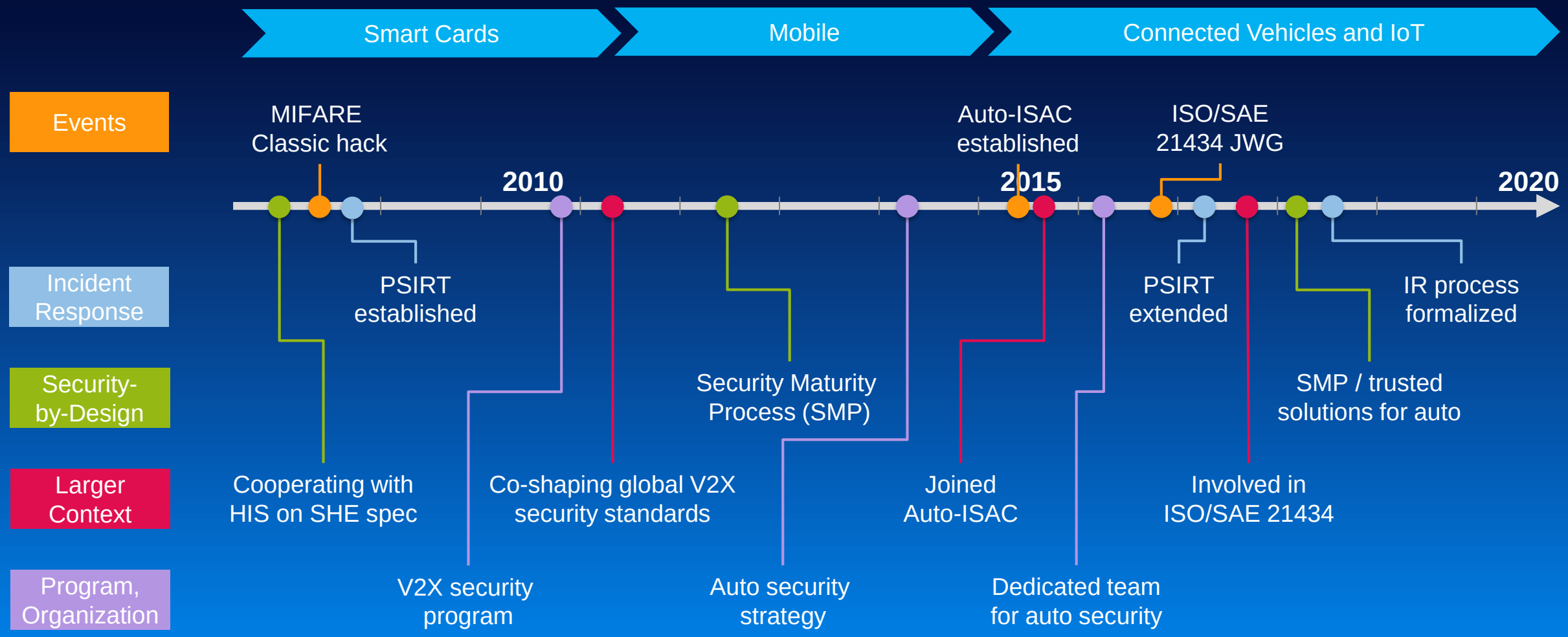
Information security policies
Site security (ISO 27001)

Researchers, industry partners,
Auto-ISAC, CERTs, …

Computer Security IR Team (CSIRT)
Security Operations Center (SOC)

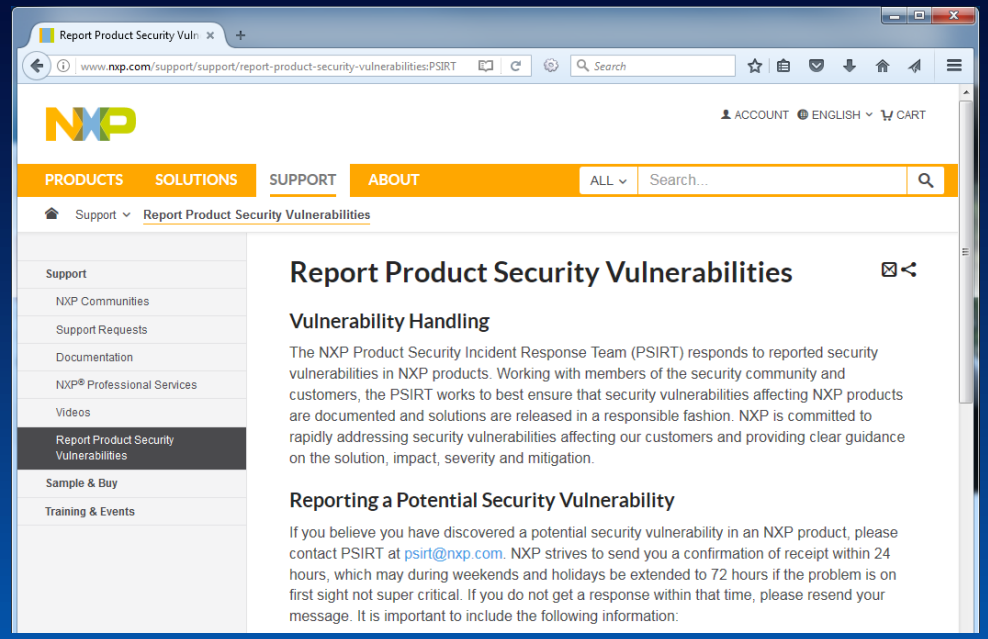
Security Culture and Organization – Matured Over Time

Some of the key milestones



Product Security Incident Response Team (PSIRT)

- Manages Product Security Incidents
  - Global across products / markets / regions
  - Established in 2008 after the MIFARE Classic hack
- Committed to Responsible Disclosure
  - In alignment with the security community
  - With our customers, partners, Auto-ISAC, CERTs
- Continuous Improvement
  - Evaluate and benchmark against Auto-ISAC's best practice guide for incident response management

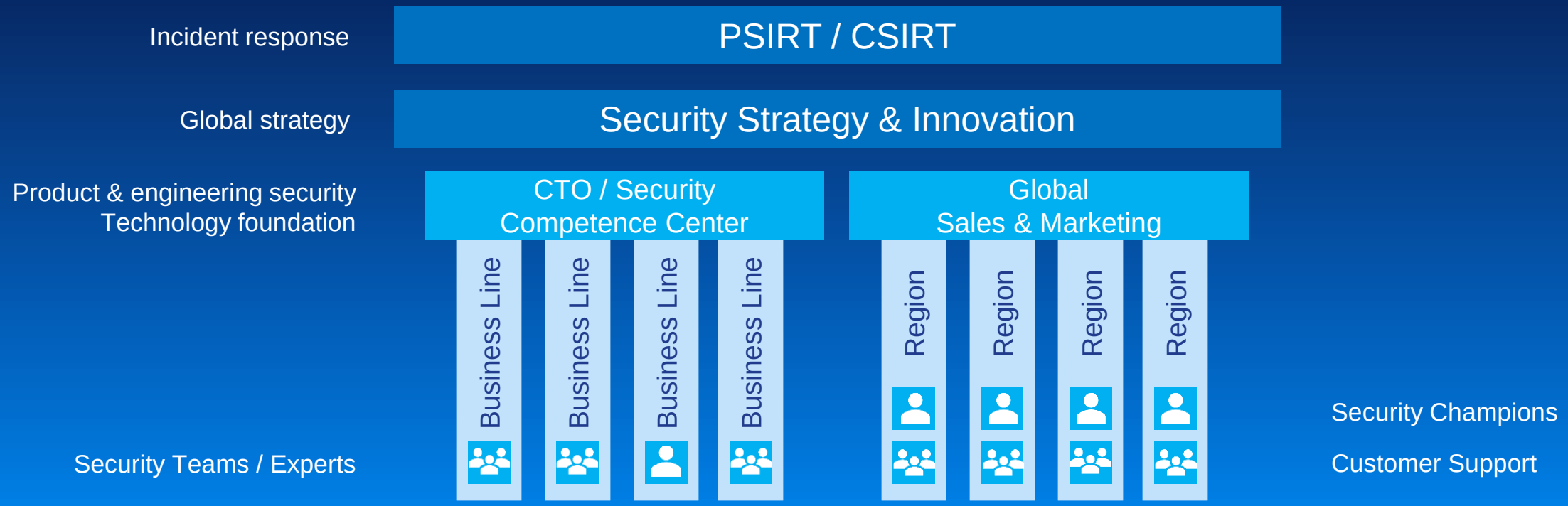


Web site: www.nxp.com/psirt Contact: psirt@nxp.com

1. Receive report
2. Evaluate vulnerability
3. Define solution
4. Communicate
5. Evaluate process
6. Closure

NXP’s Security Organization

- Dedicated expert teams – security as core competence
- Collaboration across organizations / teams / backgrounds / competences / markets
- Have expertise close to our customers



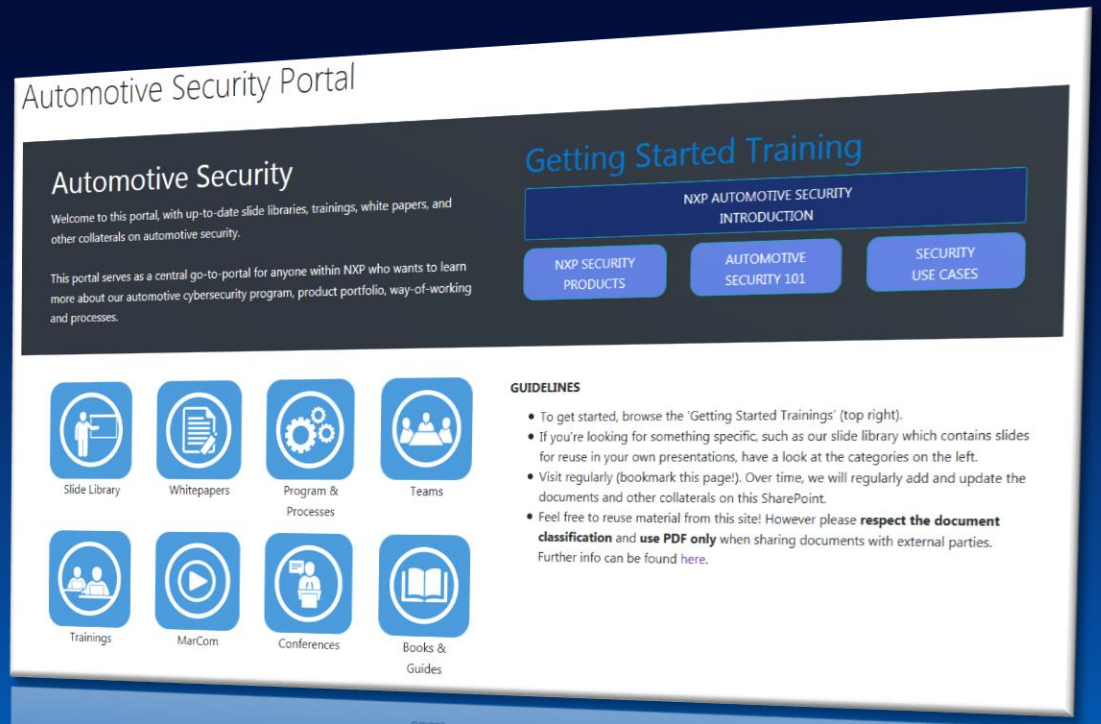
Training and Awareness – What do we do?

Training and Knowledge Transfer

- Regular basic security training
- Expert training on dedicated topics – internally and through external partners

Awareness

- Regular bulletins and campaigns to increase awareness
- Internal and external information sharing, through:
  - Regular internal meetings and online portal
  - Workshops with partners
  - Bi-directional sharing with Auto-ISAC, CERTs, …



Collaboration, Information Sharing

We collaborate with various third parties

Researchers, industry partners, CERTs, …

We are an active member of the Auto-ISAC

A key forum and network for automotive cybersecurity

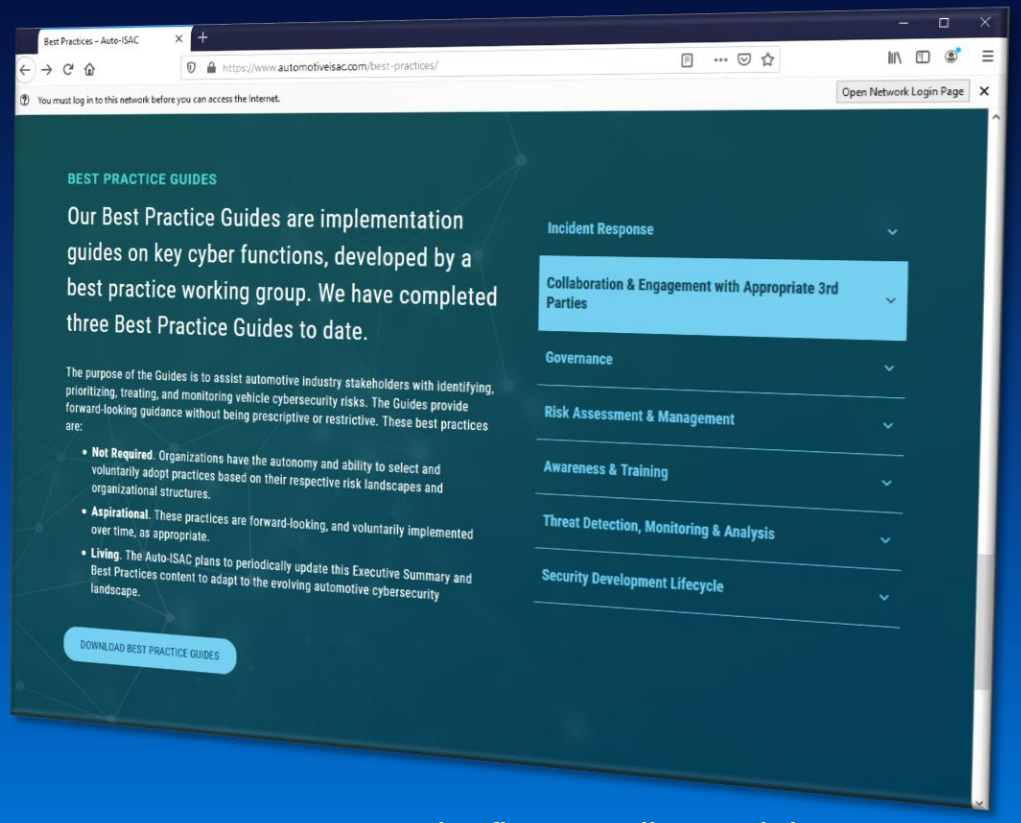
- Enables leveraging industry know-how & best practices, and sharing intelligence on threats & vulnerabilities
- Go-to-contacts for peer support and advise

Core values: collaboration, trust, confidentiality

Published 7 best practice guides

- Valuable benchmark for any cybersecurity program

AUTO-ISAC
Automotive Information Sharing and Analysis Center



NXP was amongst the first suppliers to join the Auto-ISAC (Aug. 2016)

Standards & Best Practices

NXP participates in the development of various Automotive security standards

ISO/SAE 21434

SAE TEVEES18 (J3061, J3101, …)

AUTOSAR WP-X-SEC

IEEE 1609 WAVE, ETSI TC ITS

Car Connectivity Consortium (CCC)

Digital Key Specification

Vehicle Safety & Cybersecurity Standards

Trend: Improve safety

+ Improve user experience

Through: Mechanics + Electronics + Connectivity + Autonomy

Mechanics	Electronics	Connectivity	Autonomy
• Seatbelts • Headrests • Crumple zones • Laminated glass	• Airbags • Anti-lock Braking System • Electronic Stability Control • Traction control	• V2X / DSRC • Remote diagnostics • User device connectivity • OTA (map, software) updates	• ADAS • Self-Driving • Sensors • AI & ML

Driving force for:	Functional Safety (ISO 26262)	Cybersecurity (ISO/SAE 21434)	SOTIF (ISO 21448)
To address:	Unintentional hazards	Intentional threats	Unanticipated hazards
In:	Known scenarios		
		+Unknown scenarios	

SOTIF = Safety Of The Intended Functionality

Product Development – Security Maturity Process

Threat intelligence, BPWG, …

Lessons learned (e.g. from IR)

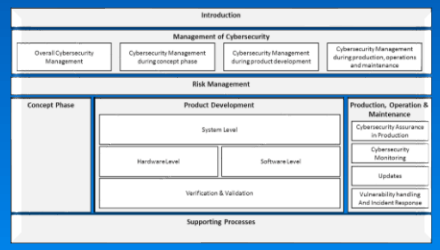
PROJECT LIFECYCLE

CONCEPT | DEFINITION | PLANNING | EXECUTION | CLOSURE

Security Milestones

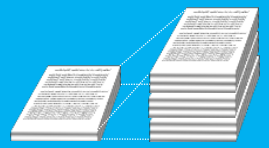
Training and awareness

Standards (ISO 21434, SAE J3061, …)



Monitoring security implementation at each gate

Independent and un-biased reviews – “4 eyes” principle



Process implementation can be adjusted per project

Your Key Takeaways!

20+ years in the smart card industry

HSE
HARDWARE SECURITY ENGINE

UWB

Security gates within our standard Automotive processes

www.nxp.com/psirt
psirt@nxp.com

SOLUTIONS & TECHNOLOGIES

PROCESSES

PEOPLE

Organization matured over time!

Automotive SE CC EAL5+

Secure CAN Transceiver

ISO/SAE 21434

AUTO-ISAC
Automotive Information Sharing and Analysis Center

Going further www.nxp.com/automotivesecurity blog.nxp.com/category/automotive

SECURE CONNECTIONS
FOR A SMARTER WORLD

www.nxp.com/automotivesecurity