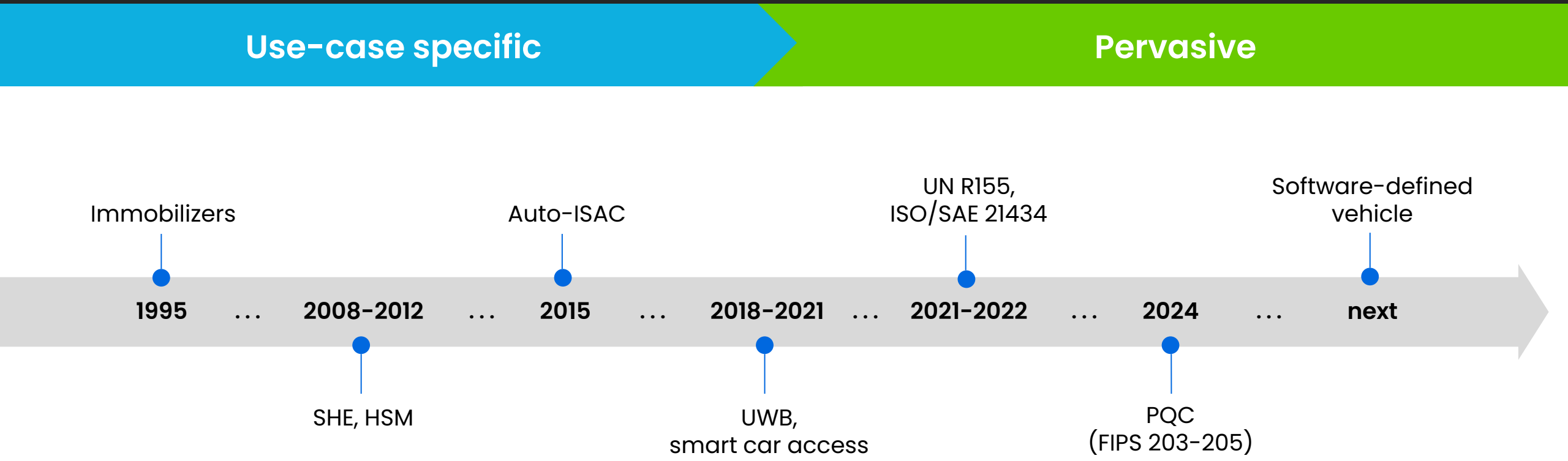
The past & future of automotive security

Timo van Roermund

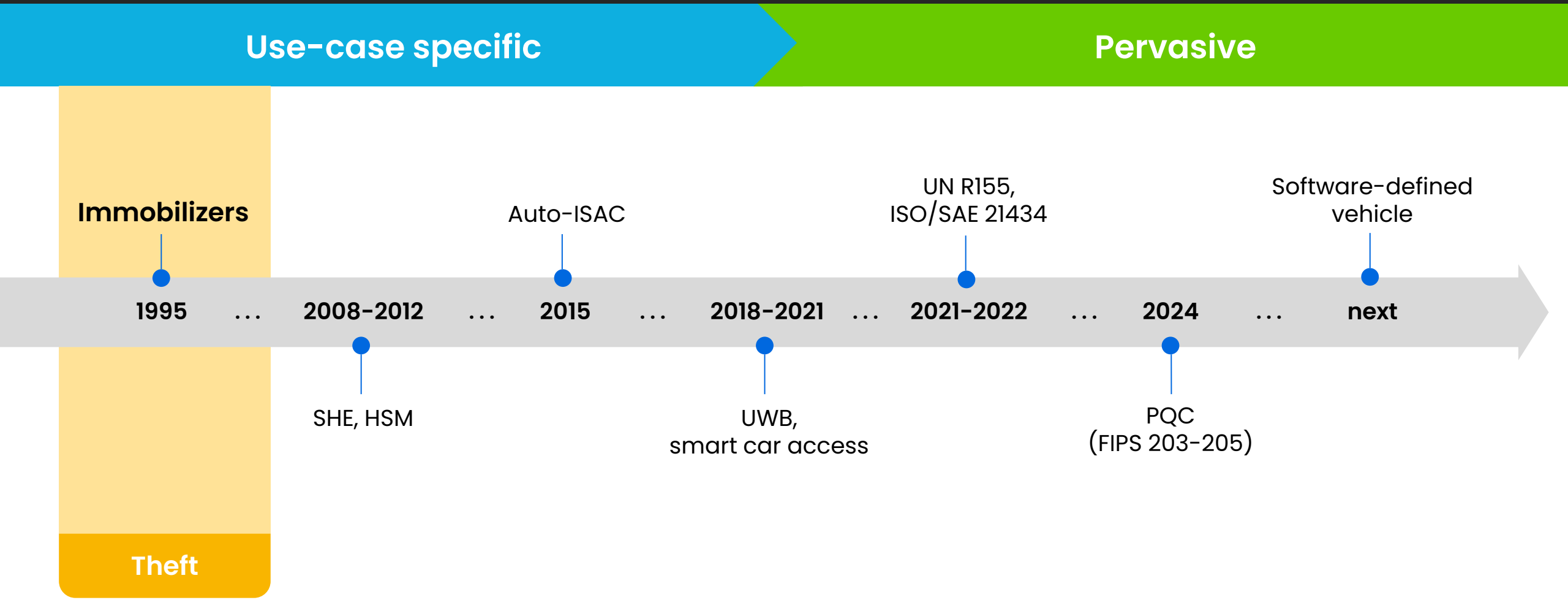
IFIP WG 10.4 workshop on Cybersecurity of Transportation Systems – June 26, ischia

Do you recognize this?

Looking back at 30 years of automotive security

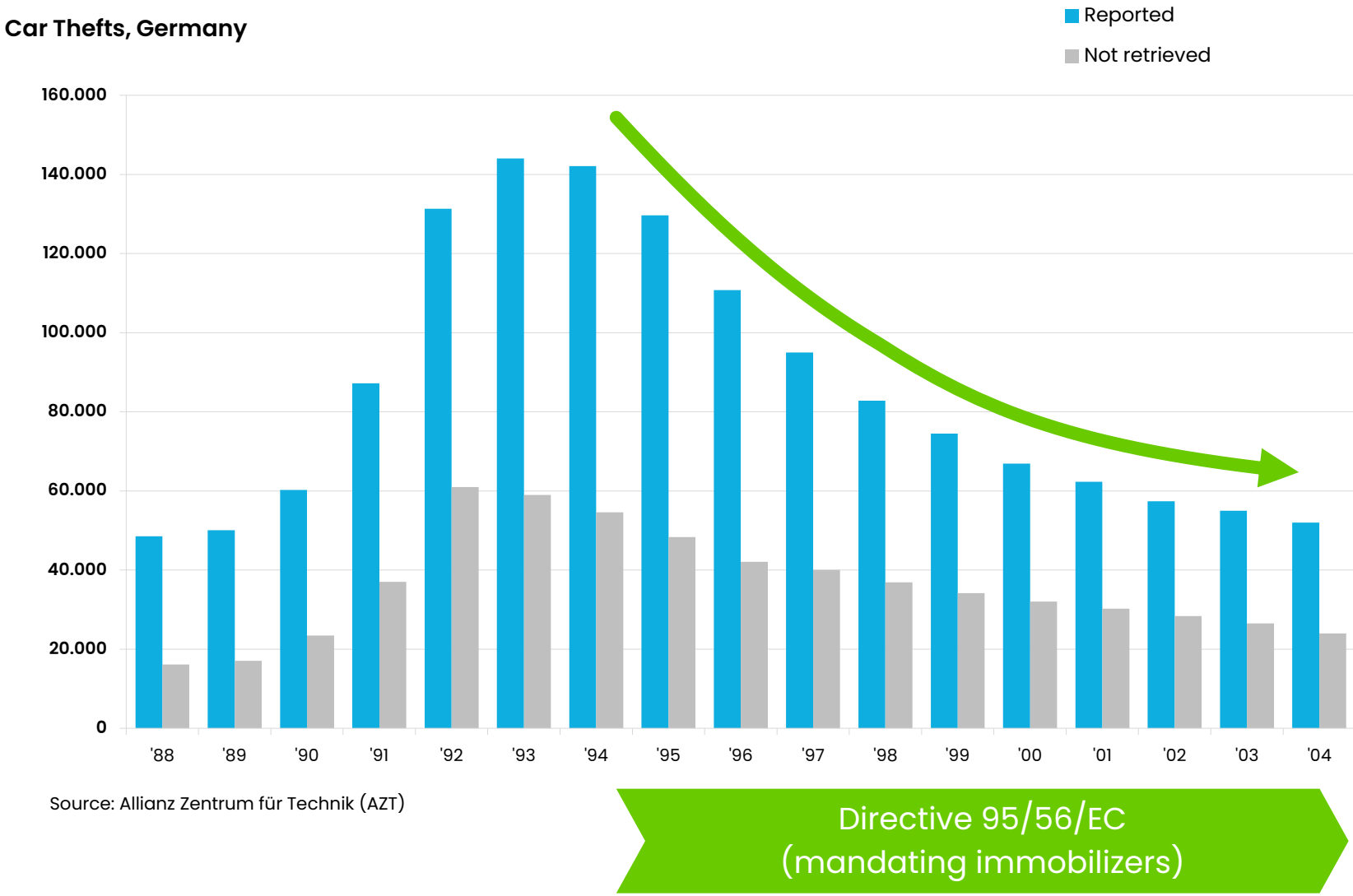


Looking back at 30 years of automotive security



Immobilizers

Vehicle theft became a real issue in the early 90s

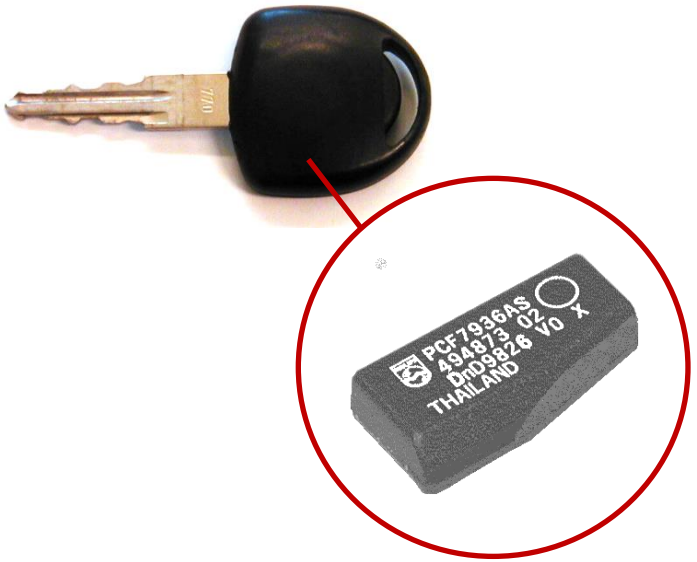


How was this achieved?

With semiconductors!

Technology borrowed from the “Schweinepille”

Initially, using ID verification only;
later using cryptography



Unlocking new use cases

Solving problems

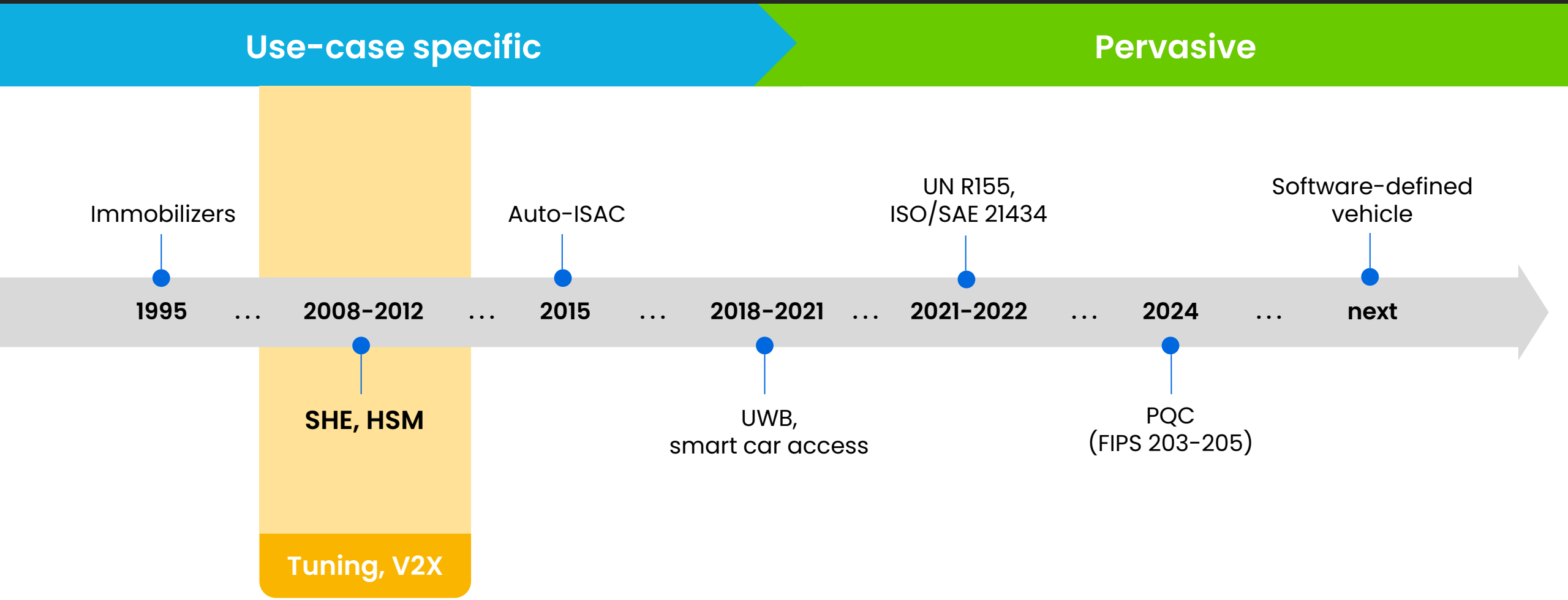
Anti-theft system
with transponders

Enhancing user experience

Remote key-entry systems

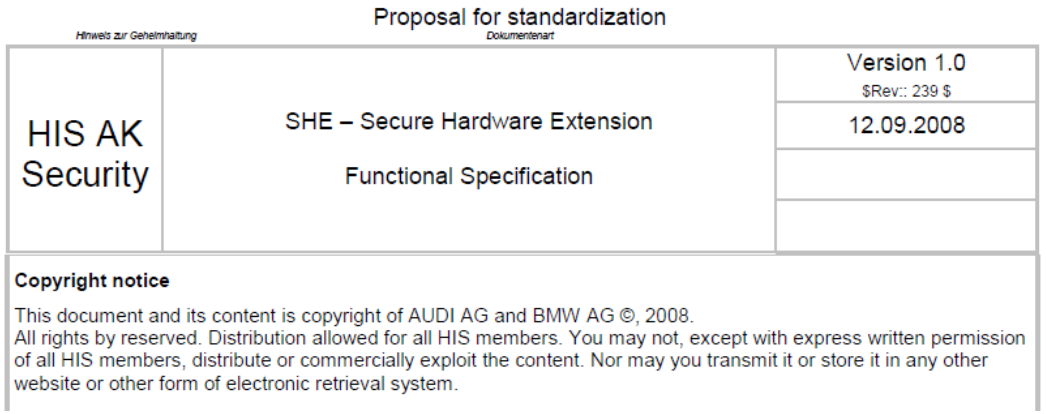
Keyless entry systems
Keyless engine start/stop

Looking back at 30 years of automotive security



SHE

EVITA HSM



Proposal for standardization

Hinweis zur Geheimhaltung | Dokumentenart

HIS AK Security	SHE – Secure Hardware Extension Functional Specification	Version 1.0 $Rev:: 239 $
		12.09.2008

First silicon implementations:

MPC56 with CSE (2011)

AUDO MAX SHE (2011)

RH850 with ICU (2012)

MPC57 with HSM (2012)

Evolution into modern secure enclaves

SHE

AES-128 (ECB, CBC, CMAC)
Miyaguchi-Preneel (hash, KDF)
PRNG (opt. TRNG)
10 key slots
Secure boot, debug

High-performance compute

Flashless MPUs
Distributed security architecture
Protocol offloading
On-chip resource control & isolation
Fast secure boot for multicore systems

Future proof

Upgradeability
Anti-rollback
Crypto-agility (in-field)
Post-quantum crypto
Long-term support

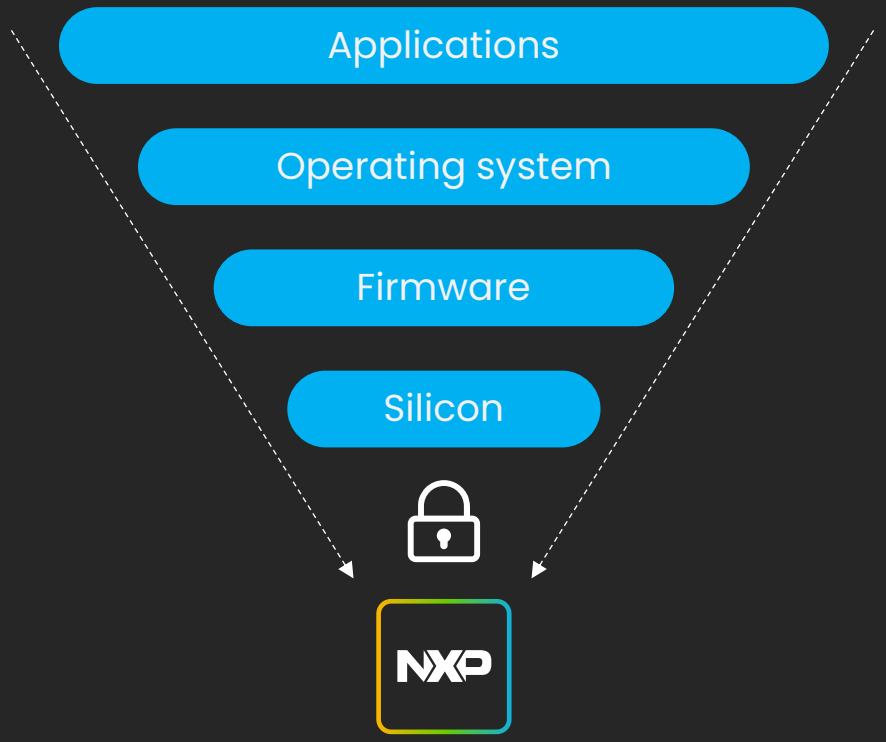
Increased features (“HSM”)

More cipher modes (CTR, GCM, CCM, …)
More algorithms (HMAC, SHA2/3, KDF2, DH, RSA, ECC, …)
Larger keys (~256b security strength)
More key slots (+ key import/export)
Strict secure boot

Increased resistance, assurance

Run-time integrity checks
Remote attestation
Hardening against FI & SCA
Third-party security evaluations (SESIP)
ISO/SAE 21434 compliance

Anchoring trust in secure enclaves



Secure Enclave as foundation

High performance, security

Rich security services

End-to-end chain of trust

Platform security (and keys) rooted in the Secure Enclave

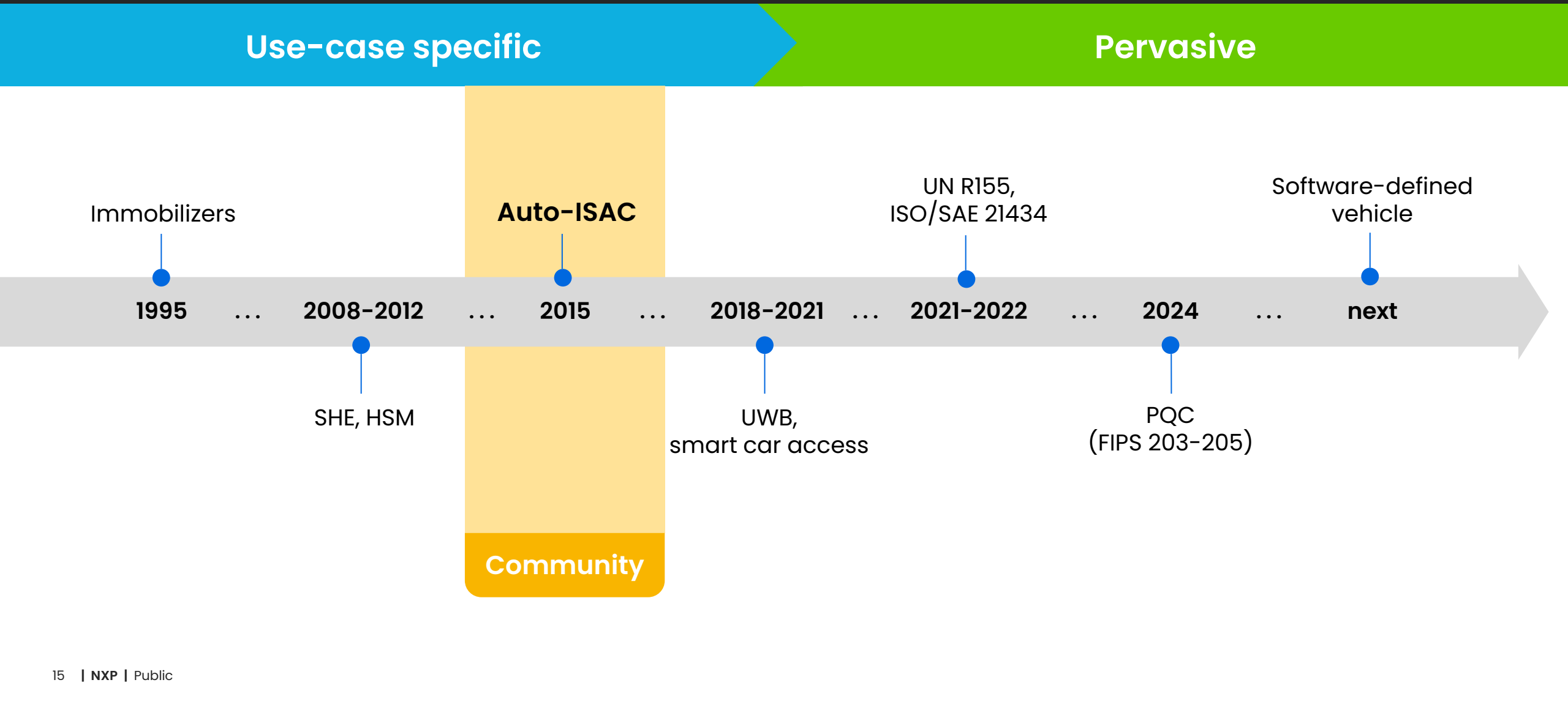
Chain of trust extends into the OS and applications

Trust enforced at the manufacturing floor

NXP provides the manufacturing root-of-trust (MRoT)

And as a service to protect customer keys using MRoT

Looking back at 30 years of automotive security



Establishing a global cybersecurity community

"In 2015, 14 light-duty vehicle OEMs decided to come together to charter the formation of Auto-ISAC. Our prospectus acknowledged the international nature of the automotive industry and included participation of global international Members. **Auto-ISAC was incorporated in August 2015 and became fully operational in January 2016.**"

Source: https://automotiveisac.com/faq

AUTO-ISAC
Automotive Information Sharing and Analysis Center

European manufacturers and suppliers join with Auto-ISAC

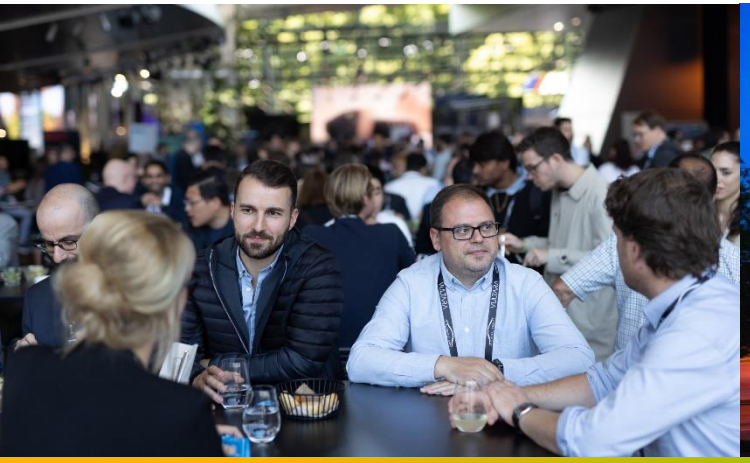
12 October 2022

The Automotive Information Sharing and Analysis Center (Auto-ISAC) announces a formal collaboration with the European Automobile Manufacturers' Association (ACEA) and the European Association of Automotive Suppliers (CLEPA) to create a central European hub for information sharing on motor vehicle cybersecurity.

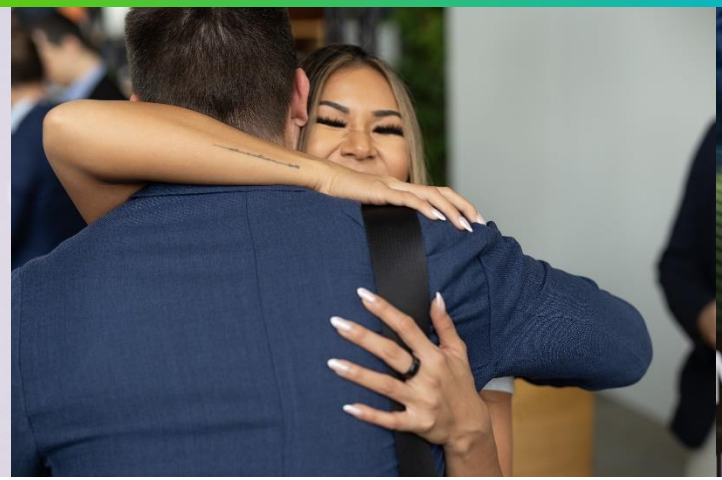
Source https://www.acea.auto/news/european-manufacturers-suppliers-join-with-auto-isac/

Since 2022 also in Europe

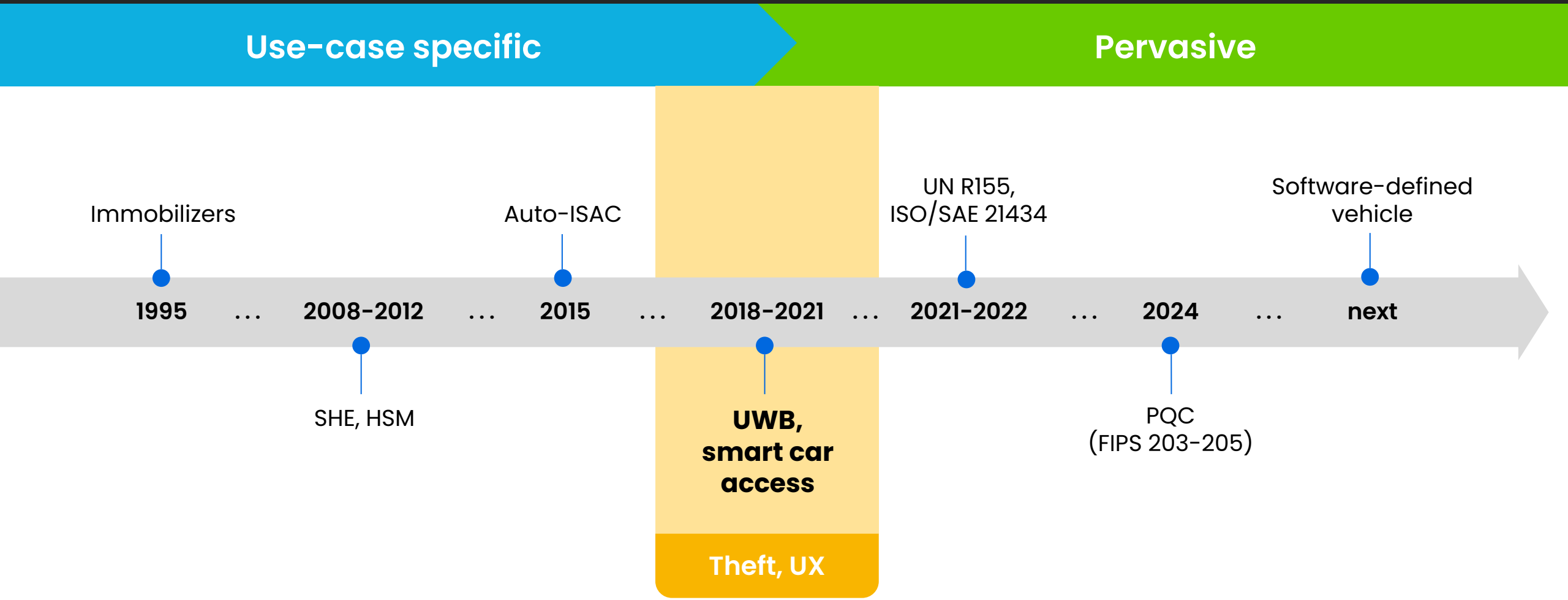
AUTO-ISAC EUROPE
Automotive Information Sharing and Analysis Center



Bringing 300+ automotive security professionals together!

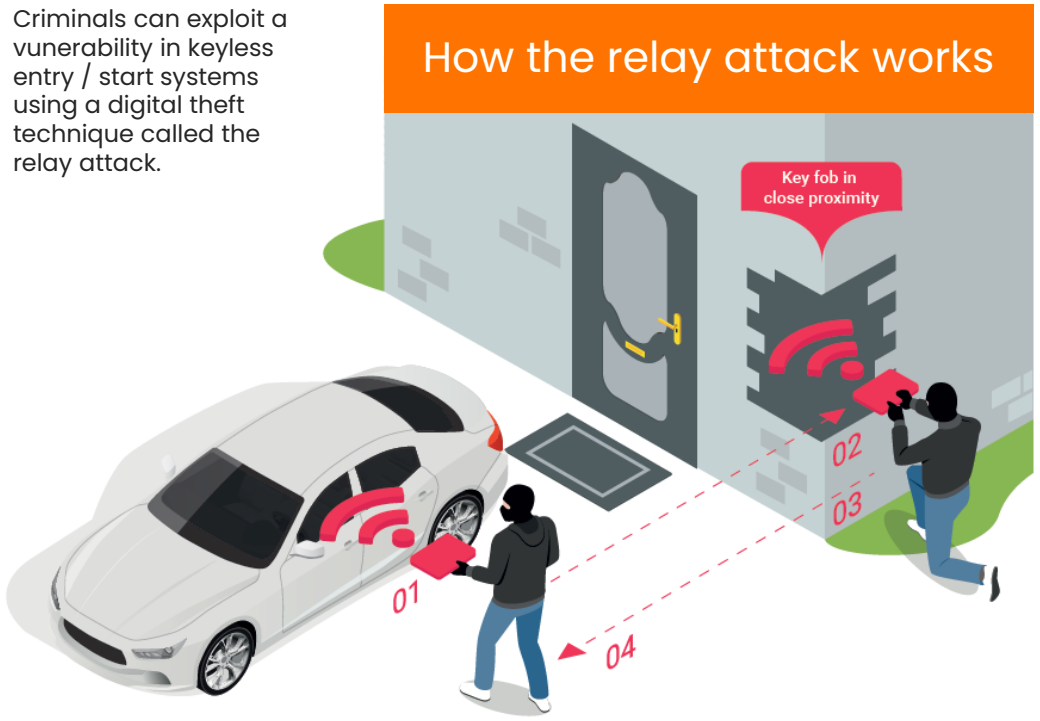



Looking back at 30 years of automotive security



UWB to prevent modern vehicle theft

Criminals can exploit a vunerability in keyless entry / start systems using a digital theft technique called the relay attack.



Source: Thatcham Research - What is keyless entry / start?

“Digitale Funktechnik schützt besser

Mit digitaler Funktechnik können Hersteller ihre Keyless-Modelle sicherer machen. Diese Technik verwendet Computerchips mit Ultra-Wide-Band-Technik (UWB) im Schließsystem, mit deren Hilfe aus der Laufzeit der Funksignale präzise die Entfernung des Schlüssels zum Auto ermittelt werden kann. Bei Verwendung der vom ADAC benutzten Funkverlängerung reagiert das Auto dann nicht mehr.

Erfreulicherweise hat Jaguar Land Rover als erster Autohersteller seit 2018 diese Technik in neuen Modellen verbaut.“

Source ADAC - Keyless-Diebstahl: Auch neue Autos sind noch leicht zu knacken

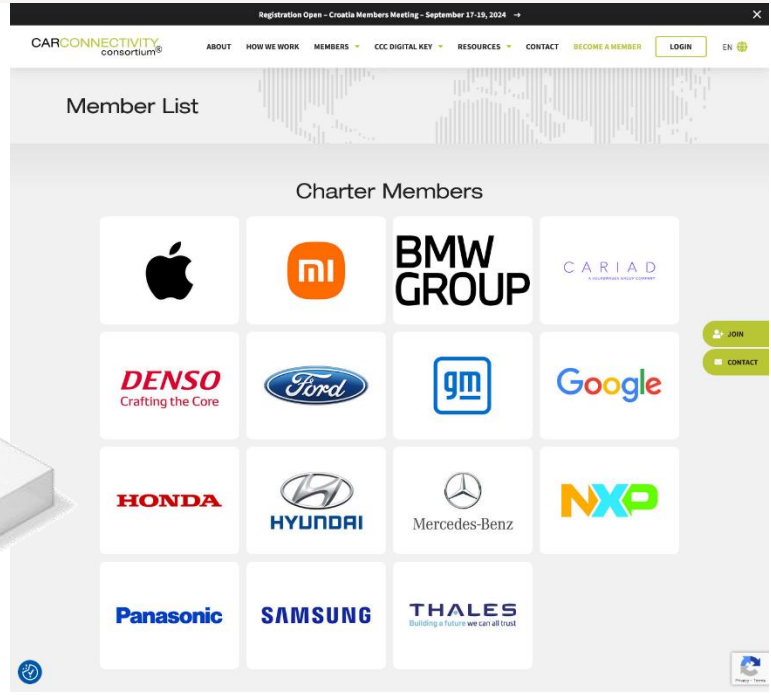
Unlocking new use cases

Solving problems

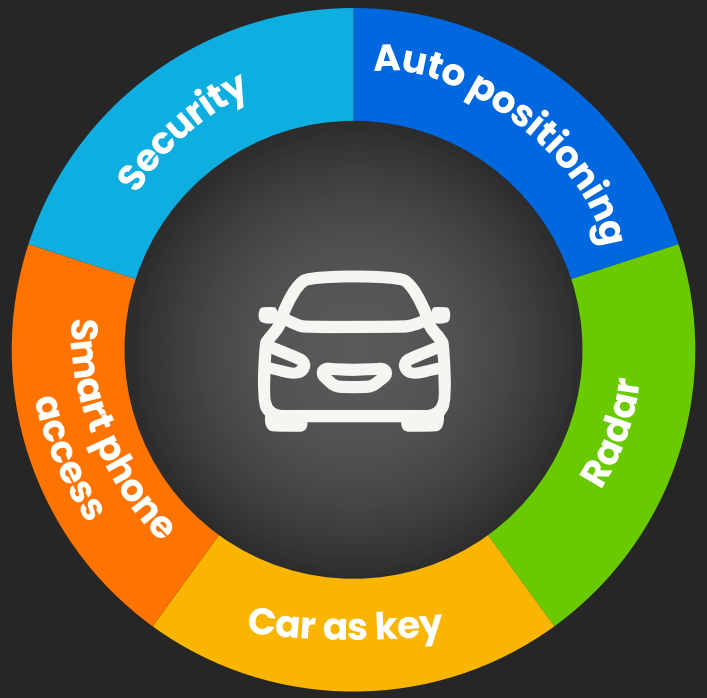
Relay station attacks

Enhancing user experience

Smart car access using CCC Digital Key™



Further use cases for UWB



Security
Protection against relay station attack

Auto positioning
Automated parking (AVP)
EV charging (W/C-EVC)

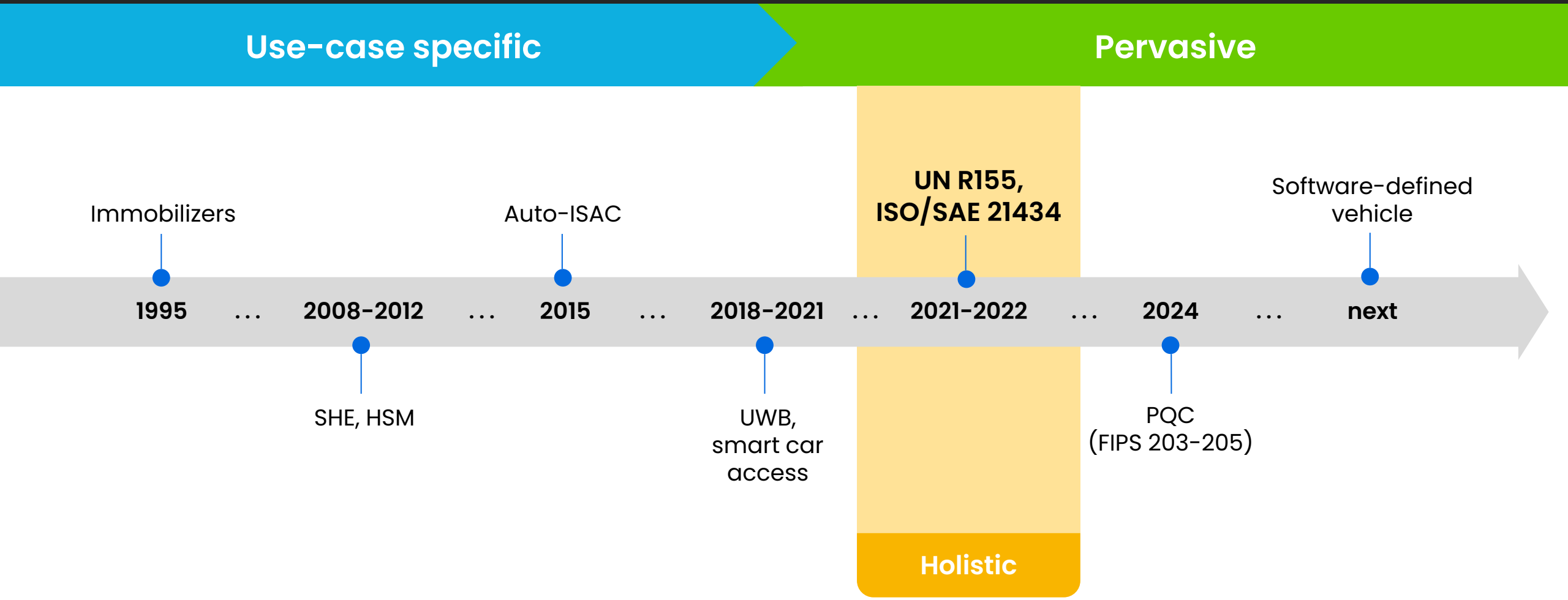
Smart phone access
Truly handsfree access
RSD for phone & fobs

Car as key
Garage / parking-lot access
Drive through payment

Radar
Passenger detection
Easy trunk access
Intruder alert

And safety!

Looking back at 30 years of automotive security



Security is no longer an option

UNECE SUSTAINABLE DEVELOPMENT GOALS

UNECE PRESS RELEASES

More options

Three landmark UN vehicle regulations enter into force

SDGs ▷ Intelligent Transport Systems ▷ Vehicle Regulations ▷ Sustainable Development ▷ Transport ▷

05 February 2021

EDN

ISO/SAE 21434 auto cybersecurity standard: Dawn of a new era?

Technical requirements for vehicle information security

Technical requirements for vehicle cybersecurity

National Standards | Mandatory | Coming Soon

GB 44495-2024 – Implementation: Jan. 1, 2026

Road Vehicle Information Security Engineering

Road vehicles—Cybersecurity engineering

National Standards Program | Formulate | Recommended

20230389-T-339 – equivalent to ISO/SAE 21434:2021

NXP

NXP Announces Compliance With ISO/SAE 21434, the New Standard for Automotive Cybersecurity

September 9, 2021 12:00 PM by NXP Semiconductors News Brief

NXP cybersecurity engineering processes are now certified as compliant with the new automotive cybersecurity standard ISO/SAE 21434.

Compliance with ISO/SAE 21434 aligns with the existing NXP principle of security-by-design in automotive applications.

Scope of ISO/SAE 21434

[introductory chapters 1-4 omitted]

5. **Overall cybersecurity management** — Organizational aspects & general requirements

6. **Project dependent cybersecurity management**

7. **Distributed cybersecurity activities** — Joint developments

8. **Continual cybersecurity activities** — Monitoring, incident response, vulnerability management

9. **Concept**

10. **Product development**

11. **Cybersecurity validation**

Product creation

12. **Production**

13. **Operations & maintenance**

14. **End of c.s. Support & Decommissioning** — (Post-)development

15. **Threat analysis & risk assessment methods [TARA]**

Describes the **WHAT**, but not the **HOW**

- Engineering requirements
- No technical requirements

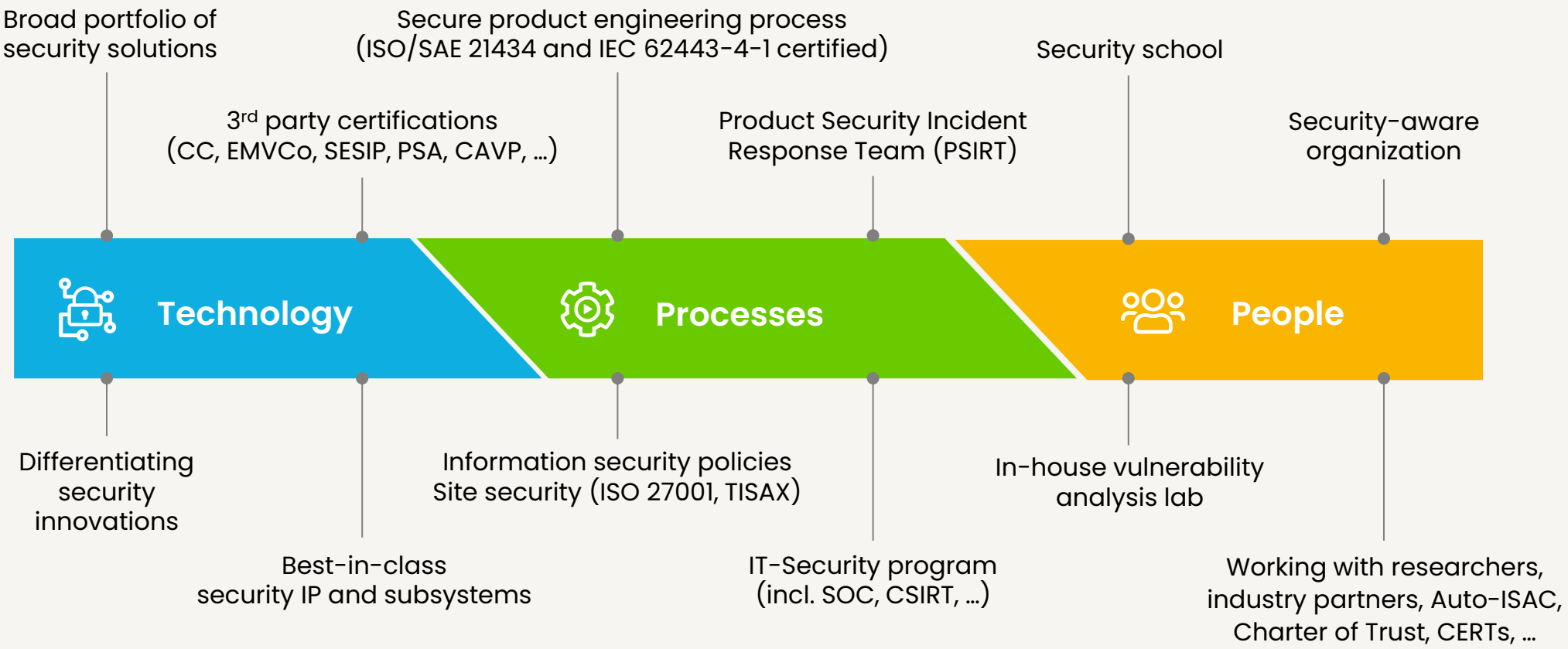
Covers entire lifecycle, with emphasis on product creation

The TARA is created in product creation & maintained afterwards (CS support period)

A holistic approach is required

NXP's approach to product security, aligned with industry standards & best-practices:

20+ years inthe security industry



High assurance requires verifiable claims

ZERTIFIKAT ◆ CERTIFICATE ◆ 認證證書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

TÜV SÜD Product Service

CERTIFICATE

No. Q4B 109577 0002 Rev. 01

Holder of Certificate: **NXP Semiconductors Netherlands B.V.**
Chief Technology Office
High Tech Campus 60
5656 AG Eindhoven
THE NETHERLANDS

Factory(ies): **NXP Semiconductors Netherlands B.V.**
Chief Technology Office
High Tech Campus 60, 5656 AG Eindhoven,
THE NETHERLANDS

Certification Mark:

TÜV SÜD ISO/SAE 21434

Scope of Certificate: **Business Creation and Management (BCaM) Process and Product Security Incident Response Process (PSIRP)**

Cybersecurity engineering processes according to ISO/SAE 21434. This process framework applies to all of NXP's R&D projects. For more details about the scope refer to the report listed below

Applied Standard(s): ISO/SAE 21434:2021

The Certification Body of TÜV SÜD Product Service GmbH certifies that the company mentioned above has established and is maintaining a management system which meets the requirements of the listed standards. The results are documented in a report. For details see: www.tuvsud.com/ps-cert

Report No.: NH97136T
Valid from: 2024-09-02
Valid until: 2027-09-01

Date, 2024-09-02

(Christian Dirmeier)

Page 1 of 1
TÜV SÜD Product Service GmbH • Certification Body • Ridlerstraße 65 • 80339 Munich • Germany

TÜV®

ISO/SAE 21434

Road vehicles – Cybersecurity engineering

TRUSTCB
TRUST AND VERIFY

SESIP™

Certificate ID	SESIP-2100009-01
	TrustCB B.V. declares that
Product	S32G2 Version 2.0
	of
Sponsor (and Developer)	NXP USA, Inc. *in* Austin, USA
	complies to the requirements described in Standard and ST Reference
Standard	GlobalPlatform Technology, Security Evaluation Standard for IoT Platforms (SESIP), GP_FST_070, Public Release v1.1, June 2021 **Based on** Common Criteria for Information Technology Security Evaluation (CC) Parts 1-3, Version 3.1 Revision 5 (ISO/IEC 15408-1, ISO/IEC 15408-2, ISO/IEC 15408-3)
ST Reference	S32G2 SESIP Security Target, version 1.3
	Summarised:
Assurance Package	SESIP2 *with* Limited Physical Attacker Resistance *and* Software Attacker Resistance: Isolation of Platform
SESIP Profile	SESIP Profile for Secure MCUs and MPUs – Public Release v1.0
	As evaluated by:
Evaluation Facility	Riscure B.V. located in Delft, The Netherlands
	Under scheme:
Scheme	SESIP *As described in* TrustCB Scheme Procedures v2.1
Validity	Date of issue: 2022-03-07 Date of expiry: 2024-03-02
Certification Mark	SESIP™2
Signatory	Wouter Slegers, CEO

SESIP (EN 17927)

Security Evaluation Standard for IoT Platforms

For further information, see: NXP security certifications, GlobalPlatform SESIP, SESIP Certificates

Achieving verifiable claims using SESIP

NXP supplies

- Threat Modelling
- Threat Mitigation (Security Mechanisms)
- NXP Security Claims
- Security Guidance
- ISO/SAE 21434 Compliance claims
- Source Code
- ISO/SAE 21434 Process & Evidence

Security Lab evaluates and verifies

- Security Testing
- Compliance Claim proof (Crypto, RNG)
- Code Review
- Development Process proof

Reflection

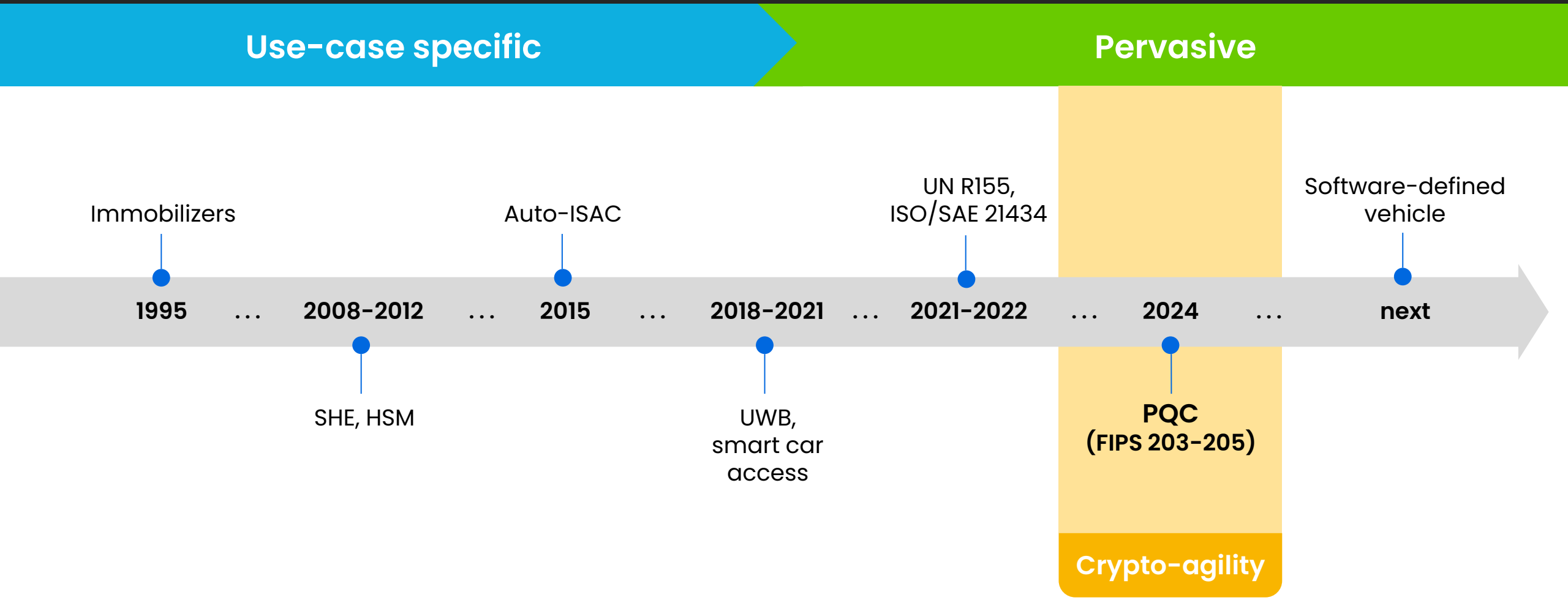
A significant step forward:

- Security is present in every project
- Increasing alignment within the industry
- Networks established

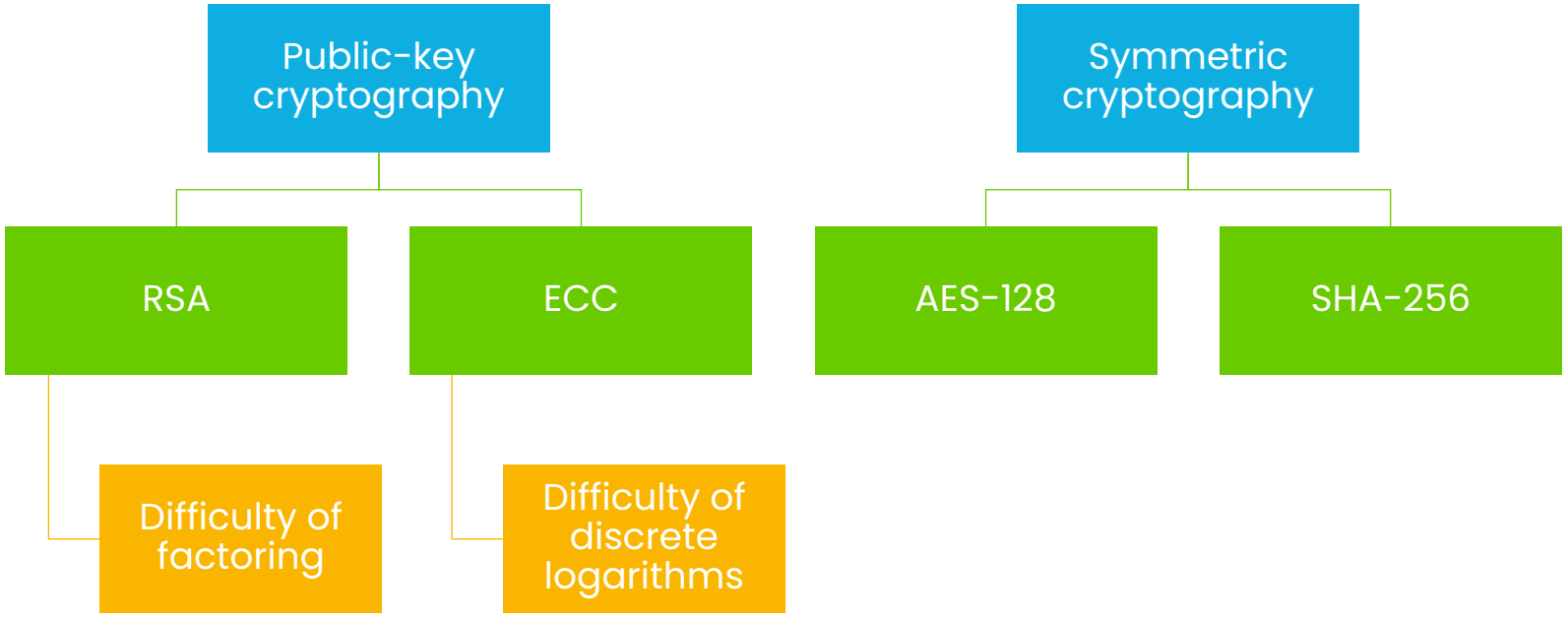
Attention points:

- Establish common baselines & thresholds (threats, attack resistance, assurance)
- Align TARAs
- Avoid wild growth of standards
- Avoid unnecessary ‘paperwork’
- Long-term cybersecurity support

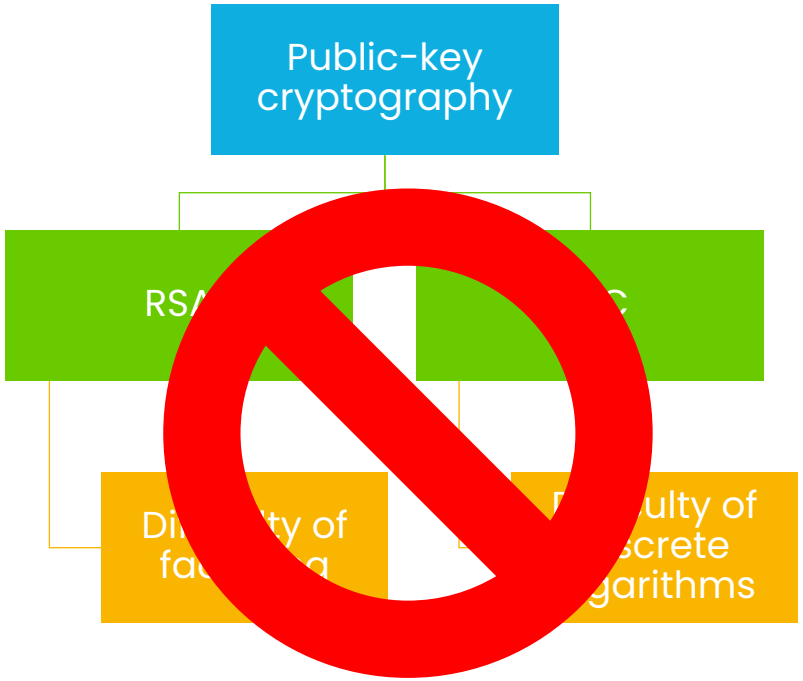
Looking back at 30 years of automotive security



Contemporary cryptography

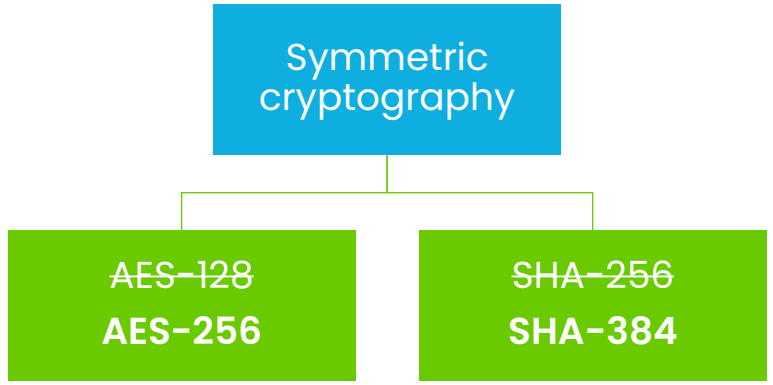


The potential impact of quantum computers



Broken!

Shor's algorithm (1994)



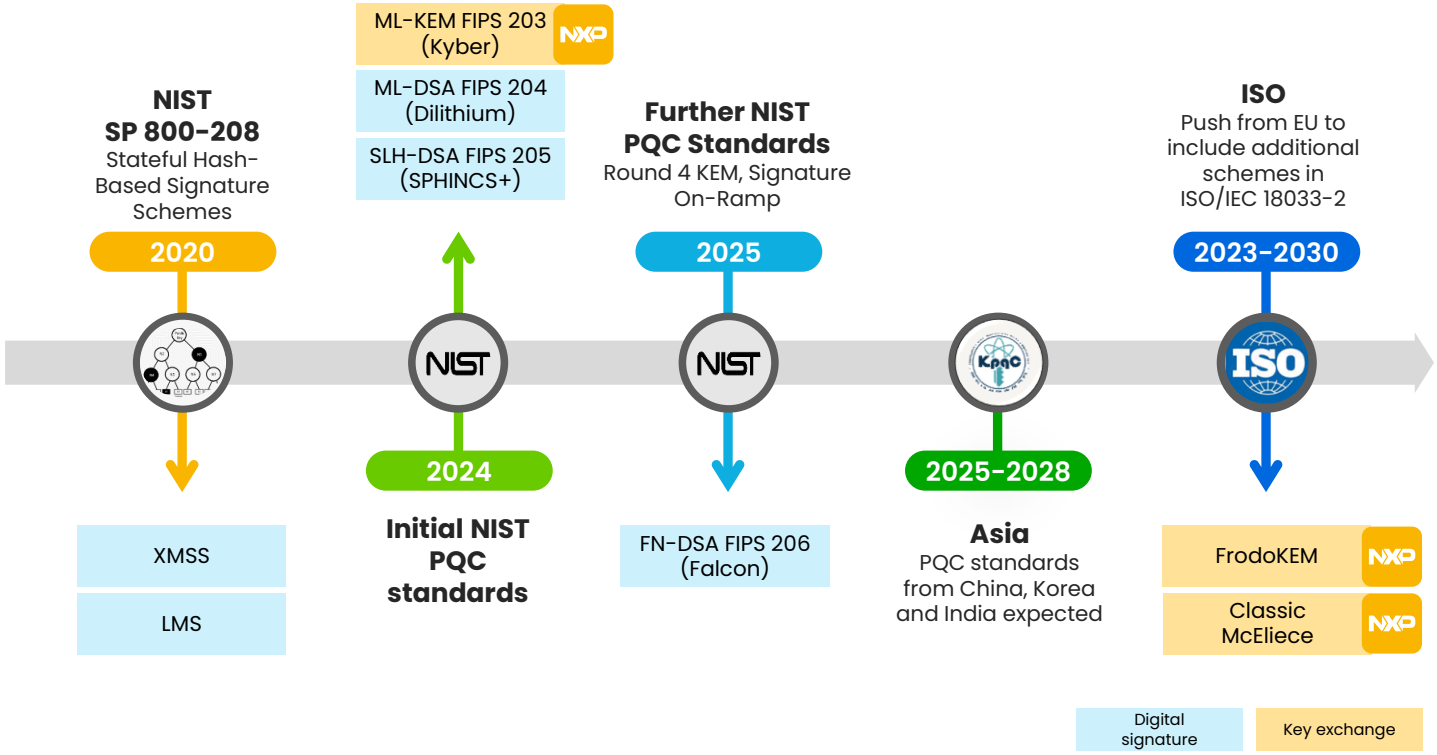
(Solution: "double" the key sizes)

"Weakened"

Grover's algorithm (1996)

Post-quantum crypto

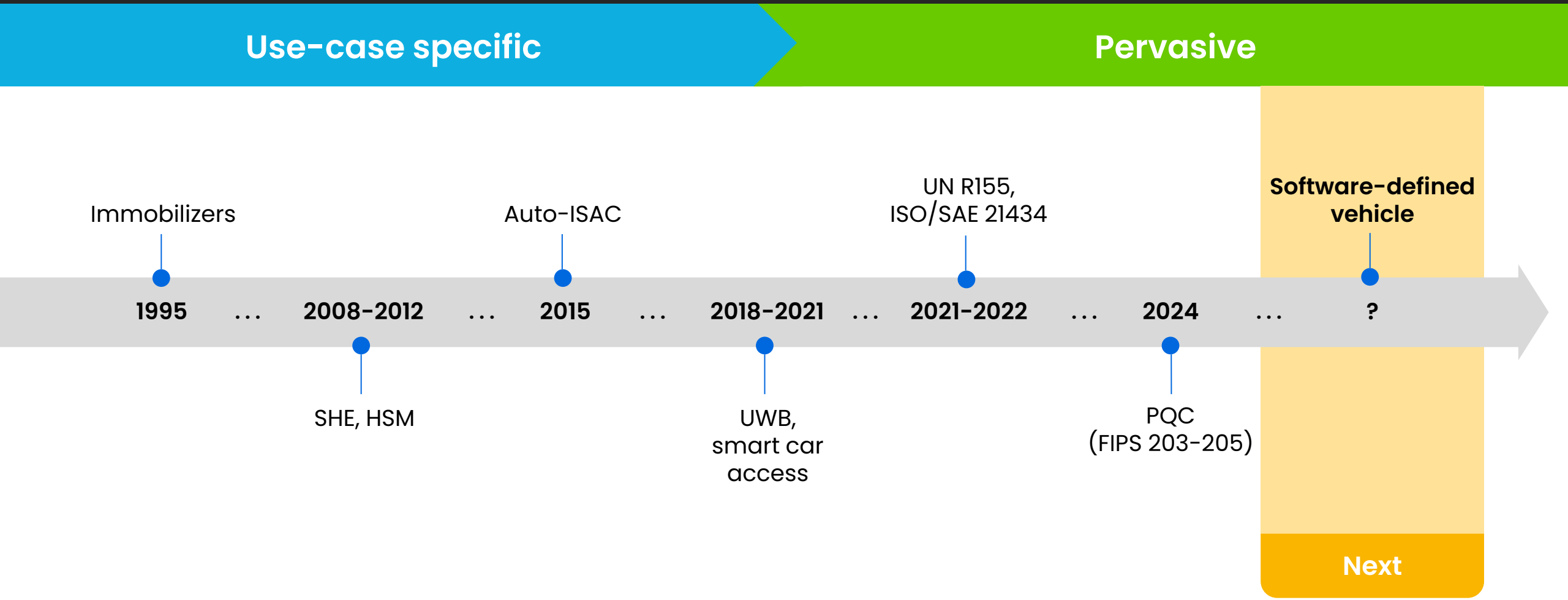
- NXP security experts co-authored six KEM proposals, including Kyber (FIPS 203), Classic McEliece and FrodoKEM (ISO/IEC 18033-2 Amd. 2).
- We work with industry partners, paving the way towards deployment (integration into protocols, systems & infrastructure).



Presentations at escar Europe, 2022 & 2023
Related papers: https://ia.cr/2023/965, https://ia.cr/2022/635

See https://www.brighttalk.com/webcast/19444/611650

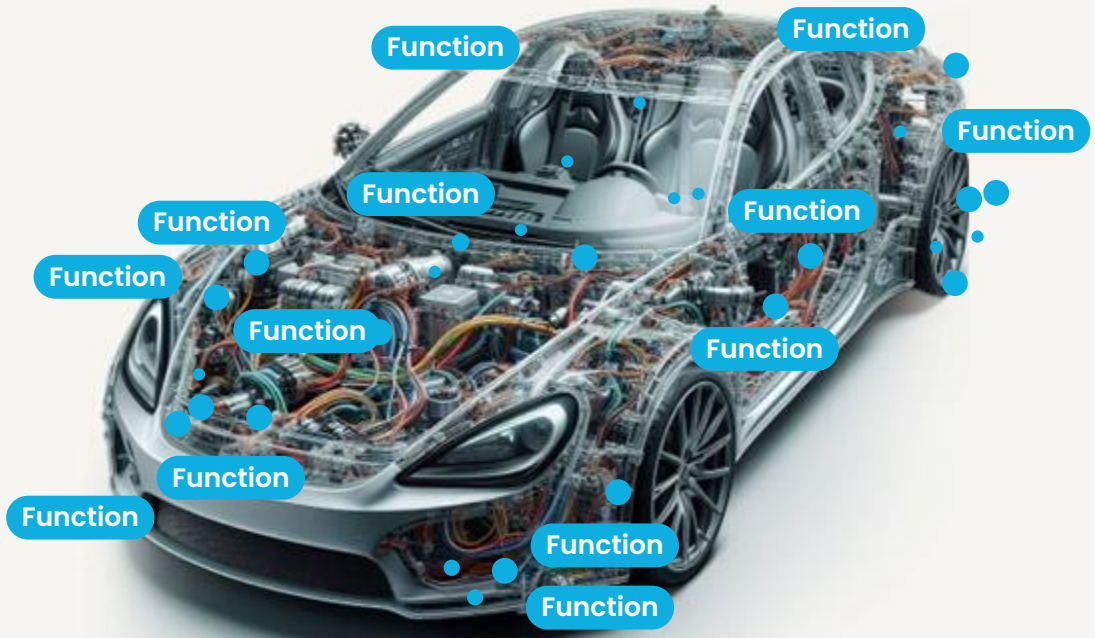
Looking back at 30 years of automotive security

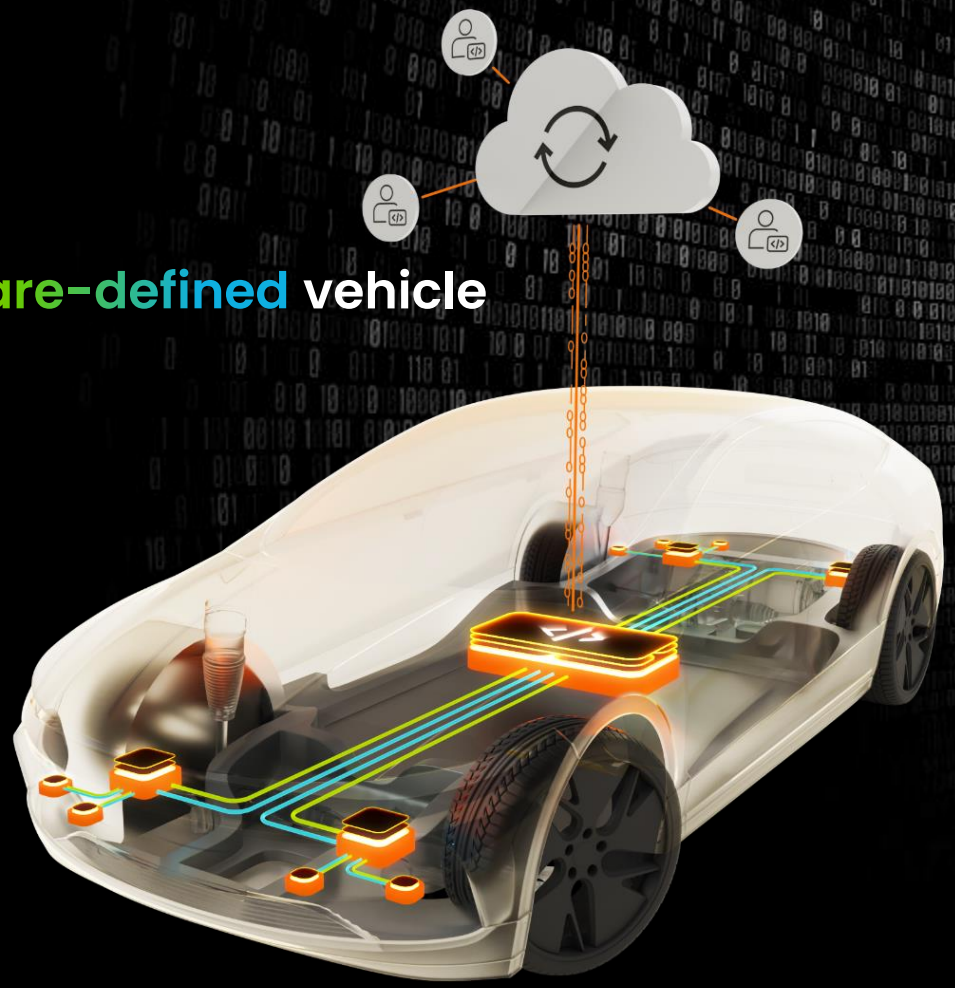


Moving into the software-defined future

Vehicle transformation underway

From hardware-oriented vehicle to software-defined vehicle





- Static
- Best performance when new
- Loses value over time

- Dynamic, updatable
- Performance increases over time
- Value increases over time

Do we need to reinvent security?

SDV needs at SoC level

On-chip isolation

Software-defined, hardware-enforced

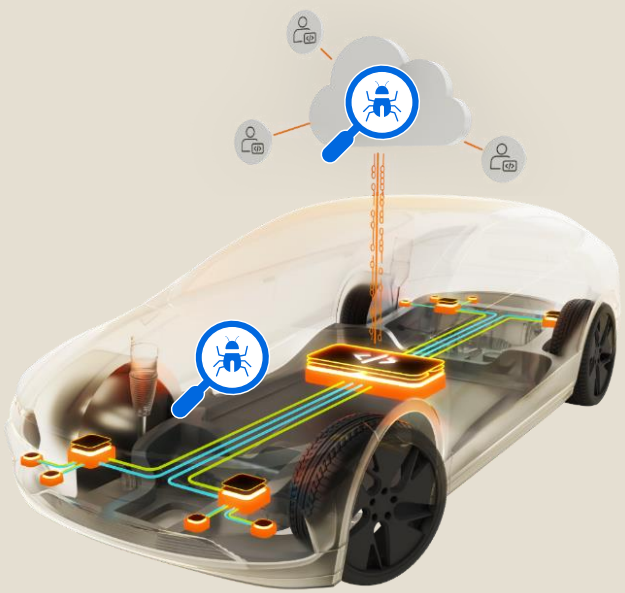
Enabling function consolidation within an SoC

Without compromising safety, security, or (supplier) IP

Remote attestation

Fleet-to-cloud monitoring (VSOC)

ECU-to-ECU monitoring



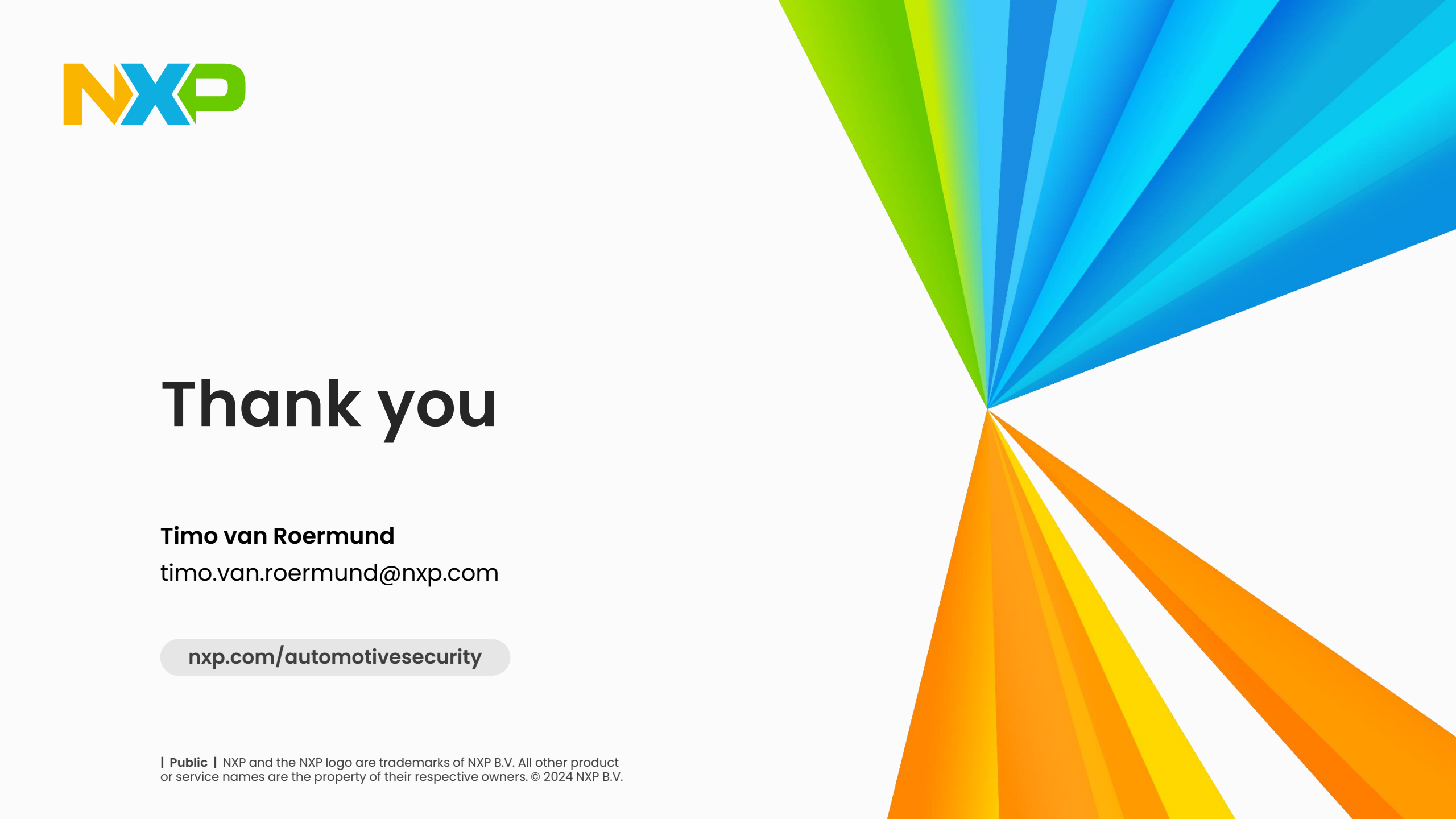
Conclusions

The automotive ecosystem has come a long way in addressing (cyber)security

Success factors:

- Collaboration within and across ecosystems
- Innovative semiconductor solutions

Both will be essential for future resilience as well



Thank you

Timo van Roermund
timo.van.roermund@nxp.com

nxp.com/automotivesecurity

nxp.com