THALES
Building a future we can all trust

Post-Quantum Cryptography

Impact for Automotive

CSVF

2025, May 22nd

www.thalesgroup.com

Agenda

- PQC introduction
- Automotive ecosystem
- PQC strategy at GlobalPlatform
- GlobalPlatform is not alone
- Conclusion

THALES
Building a future we can all trust

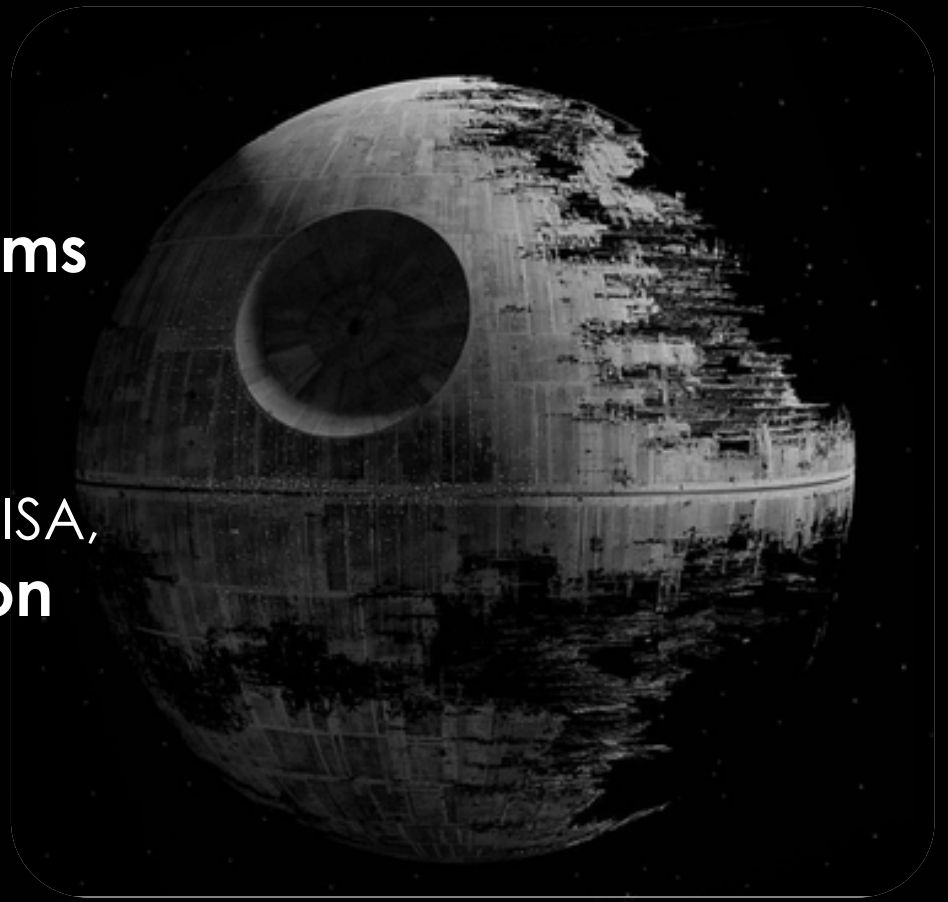
PQC Introduction

A threat? When? How to protect?

www.thalesgroup.com

A new threat in the IT galaxy

- **Quantum computing puts cryptographic algorithms at risk**
  - ➢Especially public-key/asymmetric cryptography
- **Beyond institutes and associations** (NIST, CACR, ENISA, NICT…), **governments are launching specific action plans (US, Korea, China…)**
- **Standard organizations are on a war footing**

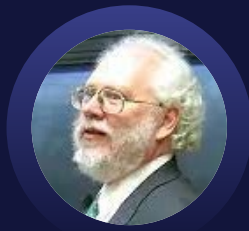


How a quantum computer impacts cryptography

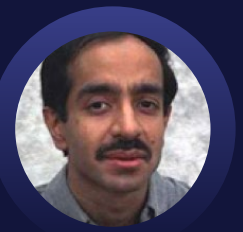
CRYPTOGRAPHIC ALGORITHM TARGETED	TYPE	PURPOSE	IMPACT FROM LARGE SCALE QC
RSA	Public key	Signatures, Key establishment	No longer secure
Digital Signature Algorithm		Signatures, Key exchange	
ECDSA (Elliptic Curve DSA)			

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

Peter SHOR



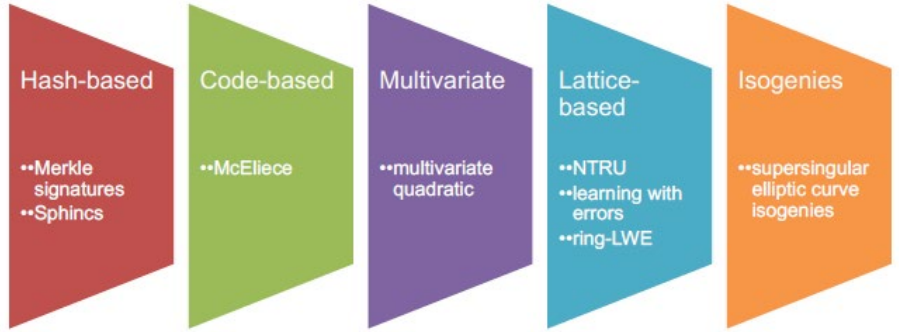
Lov GROVER



Fortunately, standards are here!

> NIST published standards (August 2024)

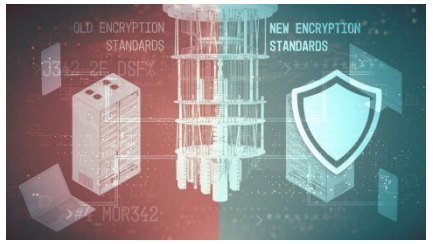
- **KEM**
  - **FIPS 203**: Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM)
  - Just announced **HQC** selection as an additional KEM
- **Signature**
  - **FIPS 204**: Module-Lattice-Based Digital Signature Standard (ML-DSA)
  - **FIPS 205**: Stateless Hash-Based Digital Signature Standard (SLH-DSA)
  - To come by end 2025 FIPS 206 FN-DSA (Falcon)
  - More to come, (possibly non-lattice-based) selection is ongoing



> NIST SP 800-208 (October 2020) LMS/XMSS

- Stateful Hash-Based Signature Schemes
  - Specific constraints of implementation
  - Niche use cases such as Firmware of Software signatures

Fortunately, standards are here!



> NIST published standards (August 2024)

- **KEM**
  - **FIPS 203**: Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM)
  - Just announced **HQC** selection as an additional
- **Signature**
  - **FIPS 204**: Module-Lattice-Based Digital Signature
  - **FIPS 205**: Stateless Hash-Based Digital Signature S
  - To come by end 2025 FL-DSA
  - More to come, (possibly non-lattice-based) selec

> **The question** of **"IF"** or **"WHEN"**
> there will be **quantum computers**
> is **no longer in the foreground.**
>
> **Post-quantum cryptography**
> will become **THE STANDARD** in the long term.

Bundesamt für Sicherheit in der Informationstechnik

> NIST SP 800-208 (October 2020) LMS/

- Stateful Hash-Based Signature Schemes
  - Specific constraints of implementation
  - Niche use cases such as Firmware of Software signatures

Migration path

> EU view: promote hybrid mode (phase?) for asymmetric crypto until PQC is mature (2030?)

- Recommend NIST PQC standards with category 3 or 5 (ANSSI/BSI/ENISA)

> ANSSI recommends to increase size/digest as a conservative approach for symmetric and hash

- i.e., migrate AES-128 to AES-256 and SHA-256 to SHA-384

> NSA, UK, Australia, Canada push directly to standalone PQC

> NSA recommends

- NIST PQC standards category 5
- Increase size/digest as a conservative approach for symmetric and hash
- Deprecate classic asymmetric crypto from 2035

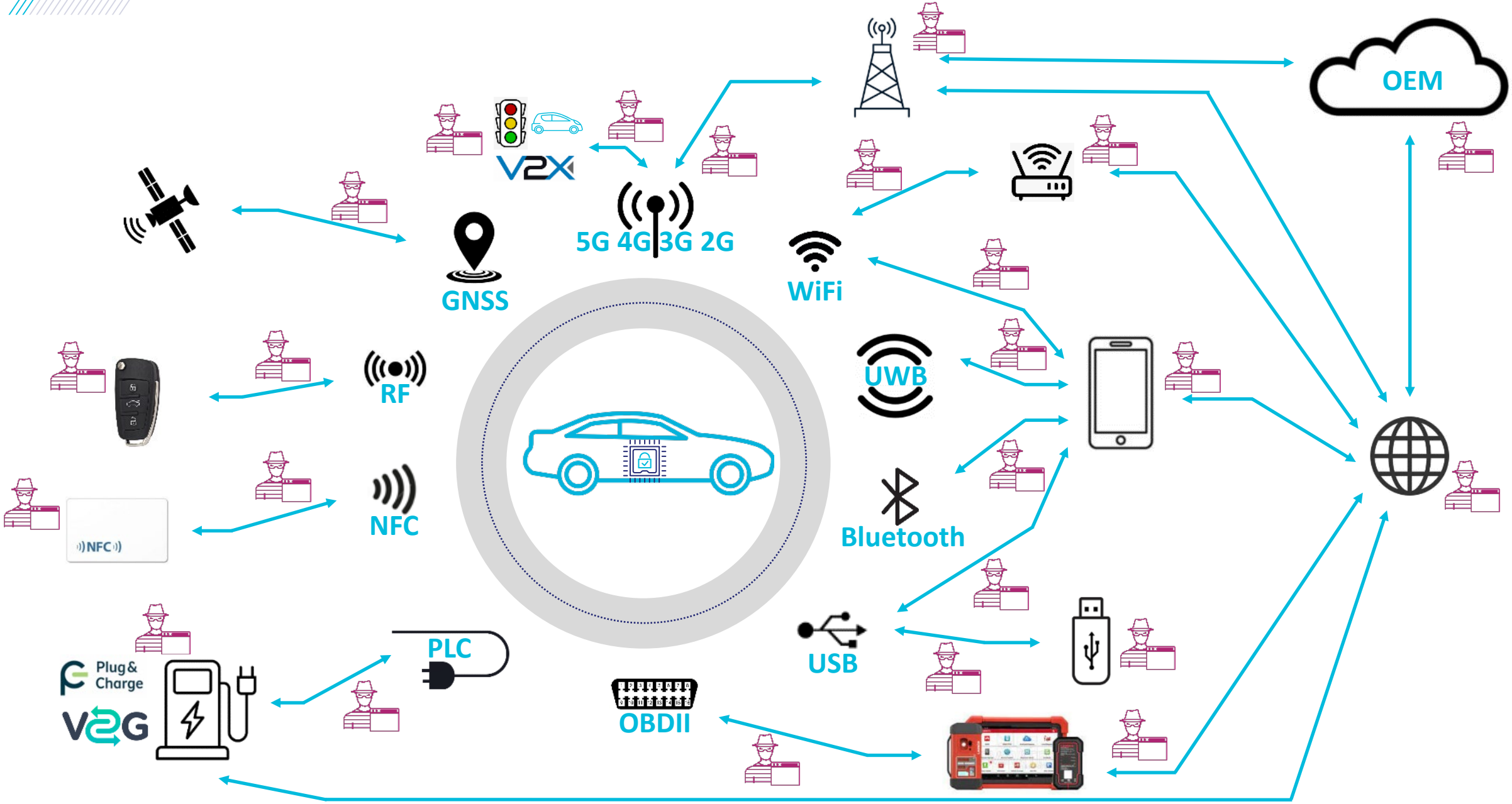
Security Category	Corresponding Attack Type	Example
1	Key search on block cipher with 128-bit key	AES-128
2	Collision search on 256-bit hash function	SHA3-256
3	Key search on block cipher with 192-bit key	AES-192
4	Collision search on 384-bit hash function	SHA3-384
5	Key search on block cipher with 256-bit key	AES-256

THALES
Building a future we can all trust

Automotive ecosystem

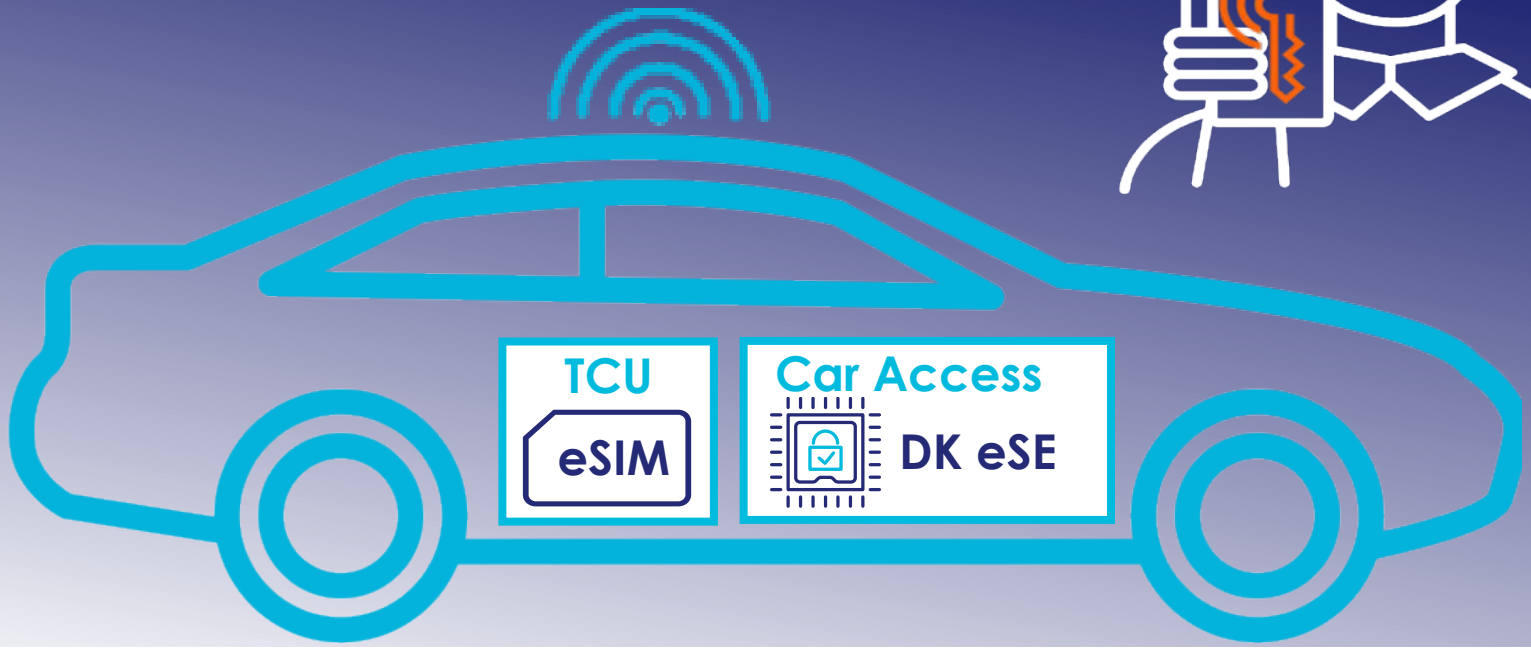
Secure Element focus

www.thalesgroup.com



Deployed in all connected vehicles

Car Connectivity Consortium **Digital Key**



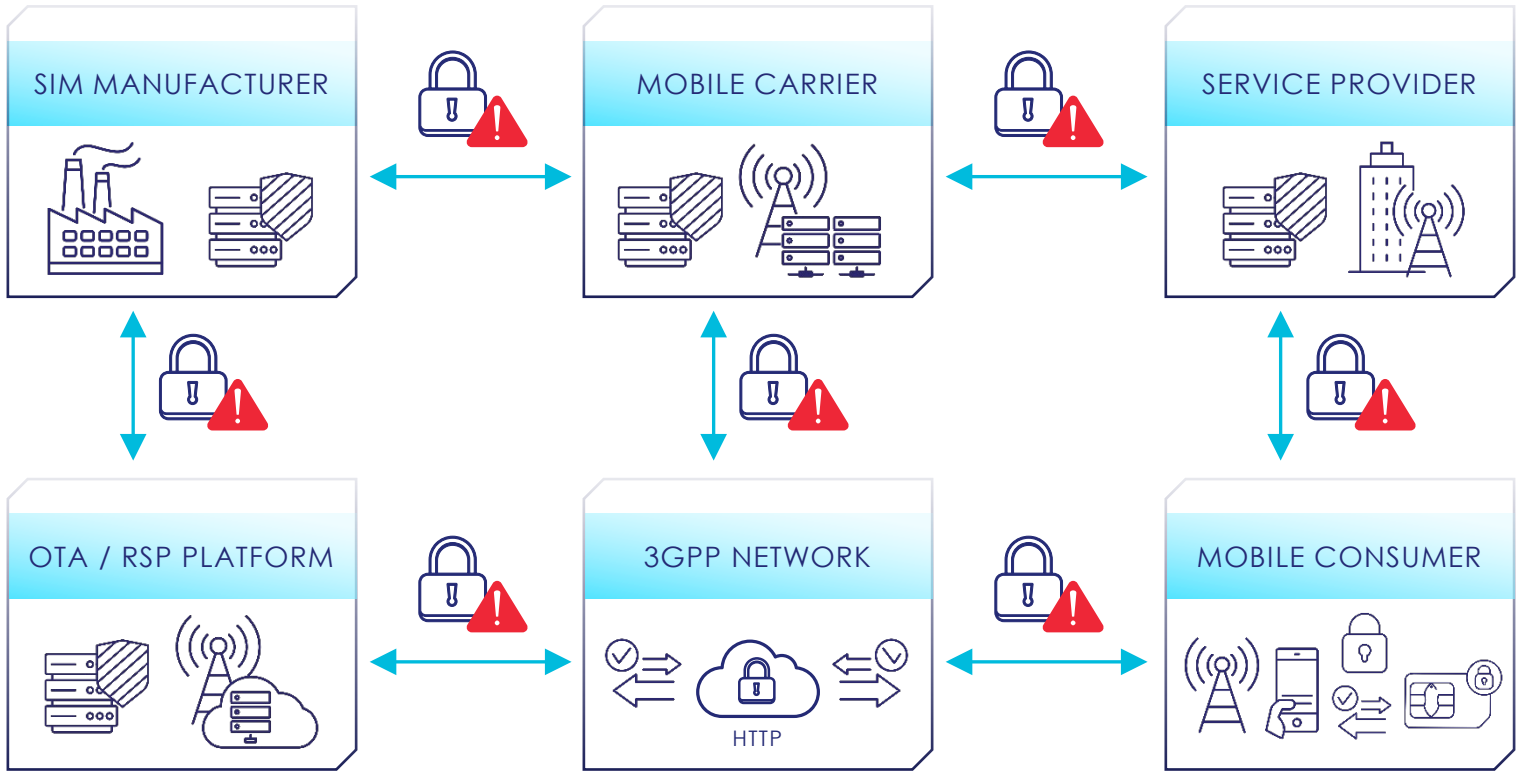
Quantum computing puts cryptographic algorithms at risk, including those used in communication protocols in the Mobile Connectivity ecosystem

Need to secure exchanges between

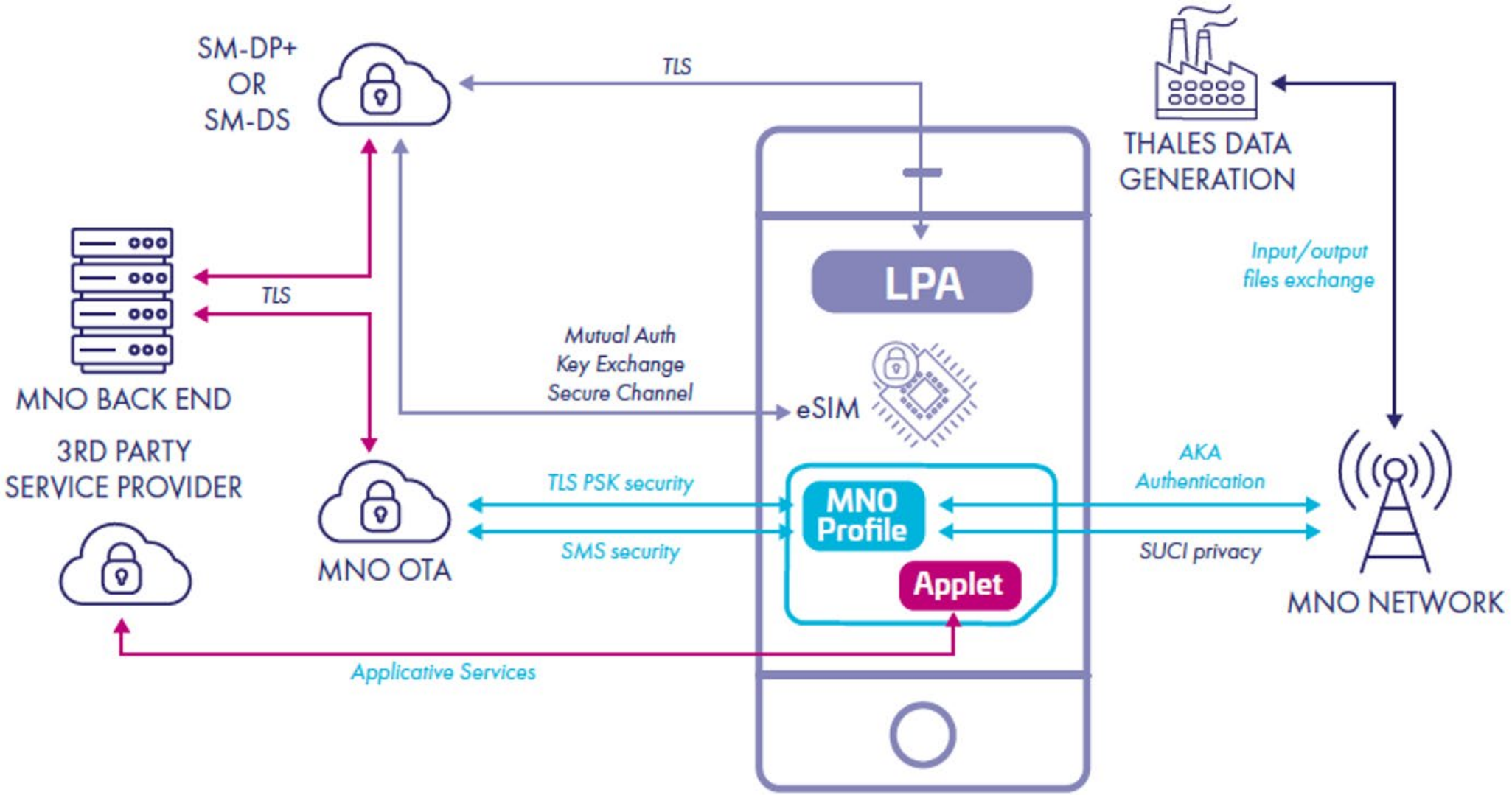
- (e)SIM
- (e)SIM management platforms
- 5G core network
- SIM manufacturer
- All IT based communications (VPN,…)

Beyond algorithms, the overall ecosystem is impacted

- Communication protocols
- Certificates
- Key management protocols



Mobile Connectivity ecosystem (e.g. SGP.22)



THALES
Building a future we can all trust

PQC strategy at GlobalPlatform

STF, SE

www.thalesgroup.com

Crypto Sub-Task Force

> Monitoring regional activity (China, Korea, Russia)

> Monitoring national recommendations (ANSSI, BSI, ENISA, NIST, NSA, NCCS,…)

- Trying to align as much as possible on timelines, algorithms and key sizes

> Publishing « Cryptographic Algorithms Recommendations », see GP_TEN_053

- The latest version 3.0 (April 2025) includes PQC algorithms and hybrid constructions

Crypto Sub-Task Force

Deprecated	Legacy use until 2030	Recommended (at least)	Hybrid PQC	PQC era (at least)
DES, 3DES SHA-1, SHA-224 RSA-1024 ECDSA-160, ECDSA-224 TLS 1.0 & TLS 1.1	RSA-2048	AES-128 SHA-256 RSA-3072 EdDSA ECDSA-256 TLS 1.2 & TLS 1.3	Combine PQC with classic	AES-128 SHA-256 LMS/XMSS ML-DSA* ML-KEM* * NIST Category 3 or 5

SE Committee activity

> High level decisions

- Crypto agility
- Focus on ML-DSA and ML-KEM as cryptographic primitives
- All new asymmetric schemes will support Hybrid as well as a PQC standalone mode (and potentially also classic mode)
- Follow IETF wording and hybrid mechanisms for signature and KEM combinations from ETSI and IETF

> New crypto agile SCP04 (symmetric secure channel protocol)

- SCP04 is composed of a set of Protocol Functions:
  - Data Derivation, MAC Calculation, Rekeying, Cipher, Sensitive Data Encryption/Decryption and Random Number Generation.
- These building blocks are configurable to allow for cryptographic agility of the protocol specification.
  - This is a Protocol Configuration

Protocol Identifier	Key Derivation	MAC	Cipher	Sensitive Data Encryption	Random
'01'	CMAC	GP Core Spec MAC	AES-CBC	GPCS AES-CBC	'60' (True Random) or '61' (Pseudo-Random) according to 'i' parameter
'02'	CMAC	SM4 MAC	SM4	SM4-CBC	
'03'	CMAC	'42'	AES-GCM	GPCS AES-CBC	

> Under definition: new SCP12 (asymmetric secure channel protocol)

- For Hybrid KEM operation, the combiner function will be based on
  - ETSI TS 103 744 v. 1.2.1 (March 2025), "*Quantum-safe Hybrid Key Establishment*": CatKDF and CasKDF
  - NIST draft SP 800-227 (January 2025), "*Recommendation for Key-Encapsulation Mechanisms*"
- Discussion on certificate for hybrid mode (based on work of IETF Lamps WG, e.g., https://draft-ietf-lamps-pq-composite-sigs-04)

THALES
Building a future we can all trust

GlobalPlatform is not alone

Other standards in the SE ecosystem

www.thalesgroup.com

Several standard organizations may be listed

> Java Card Forum

- ML-KEM
  - New Java Card Crypto API
  - New Java Card Key API
- ML-DSA
  - New Java Card Signature API
  - New Java Card Key API

> GSMA PQTN (GSMA, IBM and Vodafone)

- Practical guidelines and support to manage quantum risk
- Collaborative work with other consortiums and groups
- PQ Telco Network Impact Assessment, Guidelines for quantum risk management for Telco, PQC in IoT ecosystem
- To come: Guidelines for NTN use cases migration

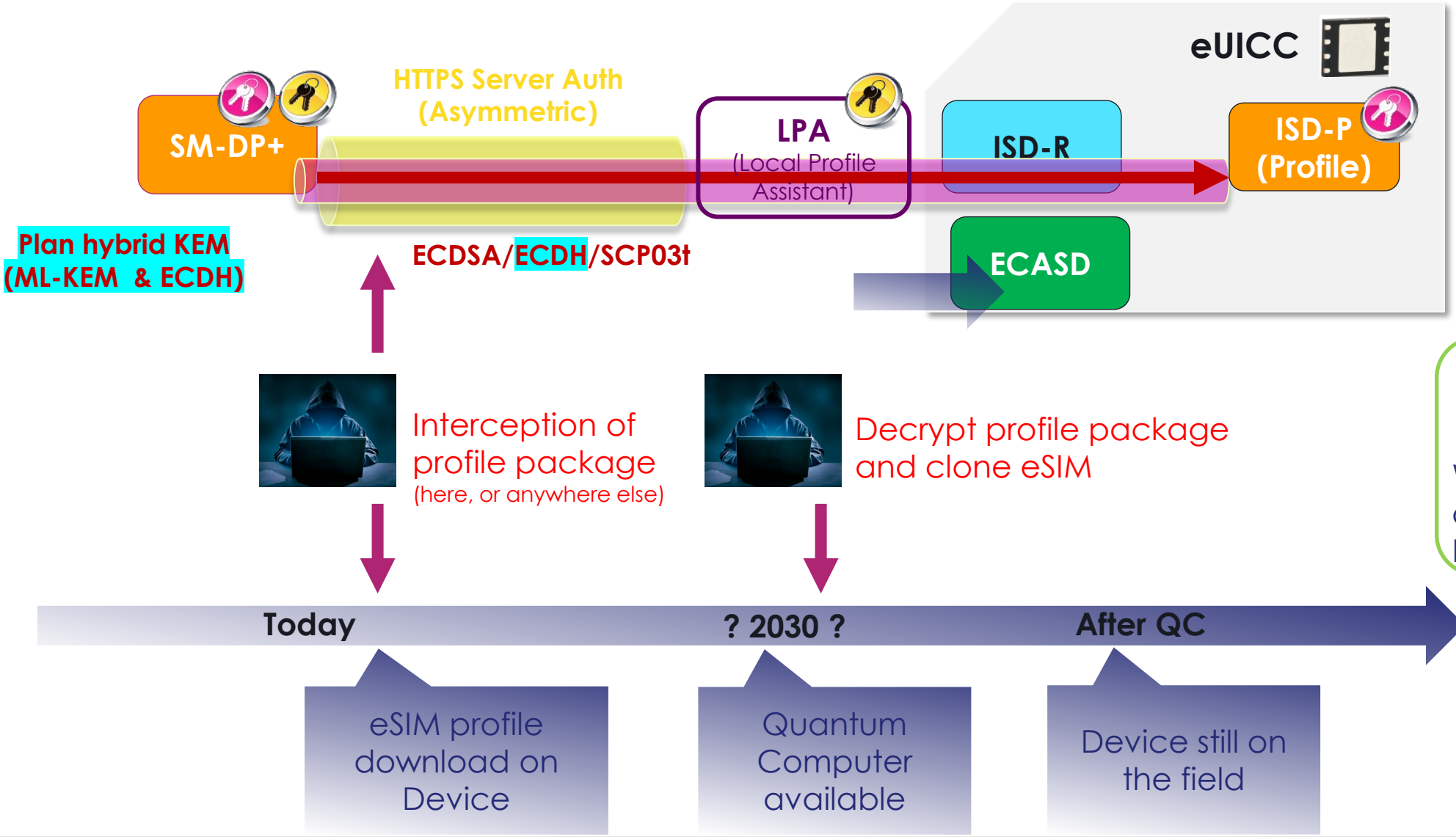
> 3GPP SA3

- Symmetric algorithms
  - AES-128, SNOW 5G, ZUC, MILENAGE-128, TUAK-128 (256 version), SHA-256…
  - Confident in 128-bit security used in 4G and 5G for quantum era
  - MILENAGE-256 recently published is based on Rijndael 256-256
- Asymmetric algorithms
  - A new Study is under discussion to transition to PQC (for 6G?)
    - › SUCI (**SU**bscription **C**oncealed **I**dentifier)

> ETSI SET

- Draft TR 104 005: "*Impacts of the post-quantum cryptography on ETSI TC SET specifications*"
  - Main impact is on TS 102 226 "*Remote APDU structure for UICC based applications*"
    - › Update on key size and algo, waiting for new GlobalPlatform secure channel specifications

“Harvest now, Decrypt Later” – SGP.22 Remote SIM Provisioning example



With SGP.02, usage of PSK-TLS mitigates PQC threat.

GSMA eSIM Working Group: Remote SIM Provisioning (RSP)

> Full PQC transformation show a huge impact on performances

- Signature and authentication forging require real time attack capability while key agreement attack can be used in a "store now decrypt later" type of attack to get the Profile content.
  - Replace only the key agreement algorithm with hybridization of ML-KEM and ECDH
  - No change (for the moment) in
    - the authentication and signature using ECDSA
    - **the SCP**

> Impact on customer/IoT specifications

- PQC Key Exchange (ML-KEM) will be tackled from **next version**, expected to be finalized by December 2025.
- Main open items are:
  - Define hybridization mechanism (not started)
  - Decision if PQC will be optional or mandatory
  - PQC signature (ML-DSA)as an option
  - Add PQC to TLS flow

THALES
Building a future we can all trust

Conclusion

www.thalesgroup.com

Roadmap to make Mobile Connectivity Solutions quantum resistant

> Crypto agility (asap)

- Making the OS upgradable Over the Air post-issuance so that it can be updated with new algorithms when a product is already in use on the field.

> Hybrid cryptography (now)

- Integrating PQC algorithms in existing cryptographic security mechanisms including hybrid cryptography to comply with latest recommendations from Security Agencies.

> New HW/SW (mid/long term)

- Designing new hardware and software layers to onboard new high demanding PQC algorithms by increasing the processing power needed for the cryptographic operations.

Read More

GlobalPlatform Blogs

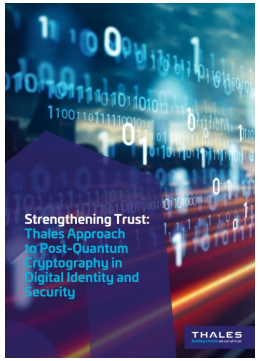
[GlobalPlatform Crypto agility: The (cryptographic) key to data security in a digital world – GlobalPlatform]

[GlobalPlatform Hybrid Crypto: Anticipating the Break of Asymmetric Crypto – GlobalPlatform]

[GlobalPlatform Quantum Computing and the Impact on Cryptography: What Do Organizations Need to Know? - GlobalPlatform]

Thales Approach to Post-Quantum Cryptography in Digital Identity and Security

- https://cpl.thalesgroup.com/sites/default/files/content/white-paper/post-quantum-cryptography-solutions-wp.pdf



THALES
Building a future we can all trust

Thank you

beatrice.peirani@thalesgroup.com
yves-emmanuel.le-bobinnec@thalesgroup.com

www.thalesgroup.com