ETSI/IQC Quantum Safe Cryptography Event

Firmware integrity in the quantum age – How to prepare against threats of quantum computing now

Dr. Martin Schläffer

15/02/2023

Security is essential

Security is a fundamental need of society with increasing importance

The connected world is further driving the demand for security

We believe in hardware-based security as an essential trust anchor

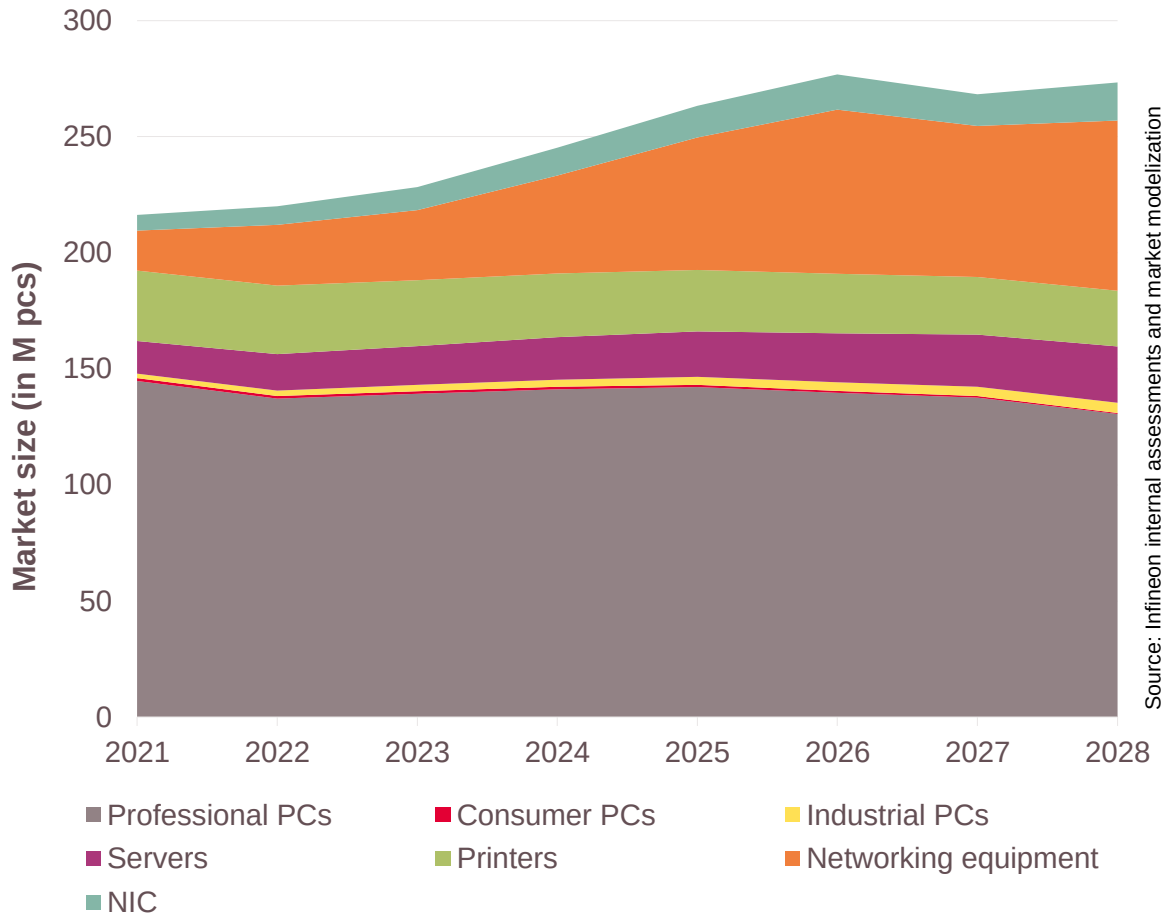
Discrete TPM, key root of trust for multiple applications

What a TPM does

- Offers a standardized solution
- Allows trusted and secured communication
- Protects exchanged valuable data
- Supports the latest security requirements
- Is updatable, particularly "in the field"

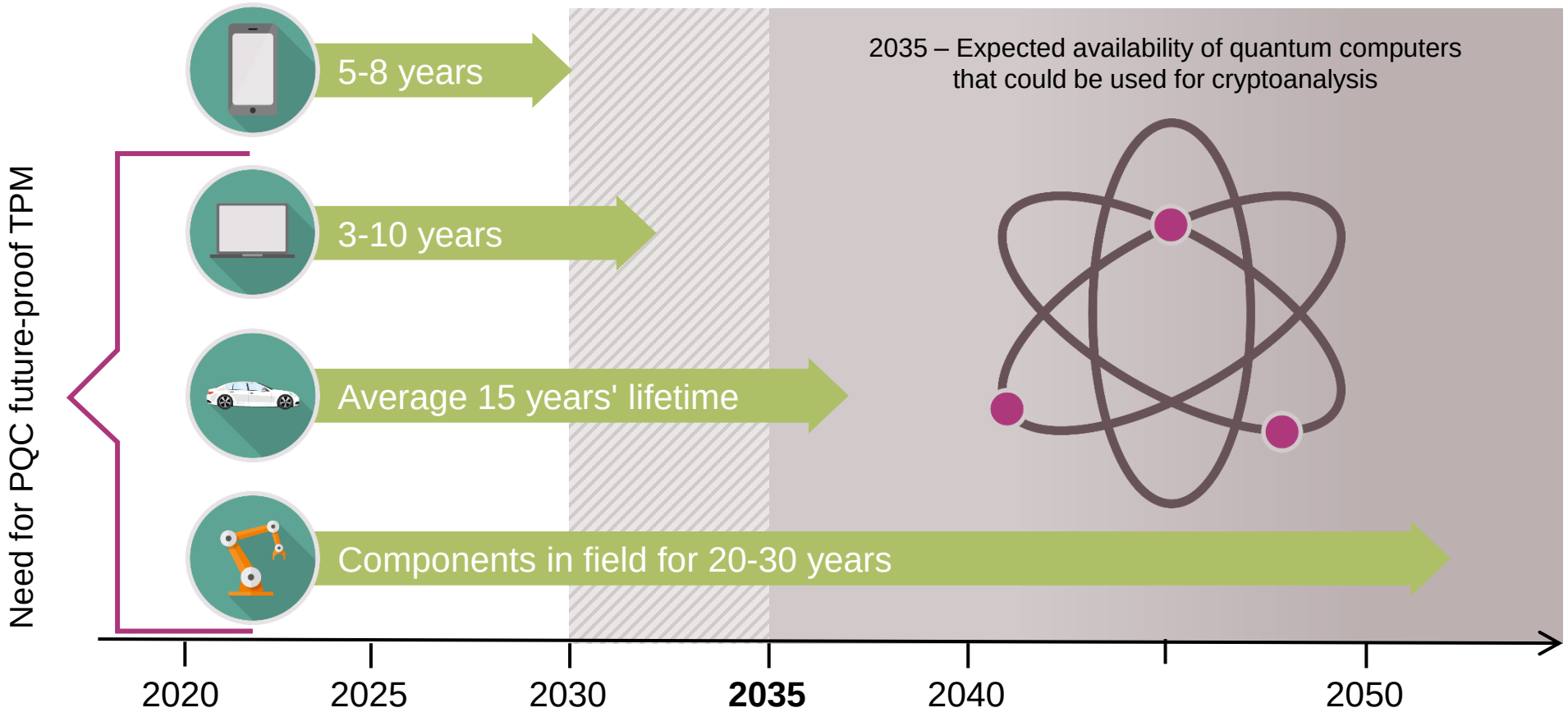
Forecasted markets for discrete TPM

A stable base market and significant growth in other segments



Considered timeline

Devices with over 10 years of lifecycle must be prepared for the quantum computing age now



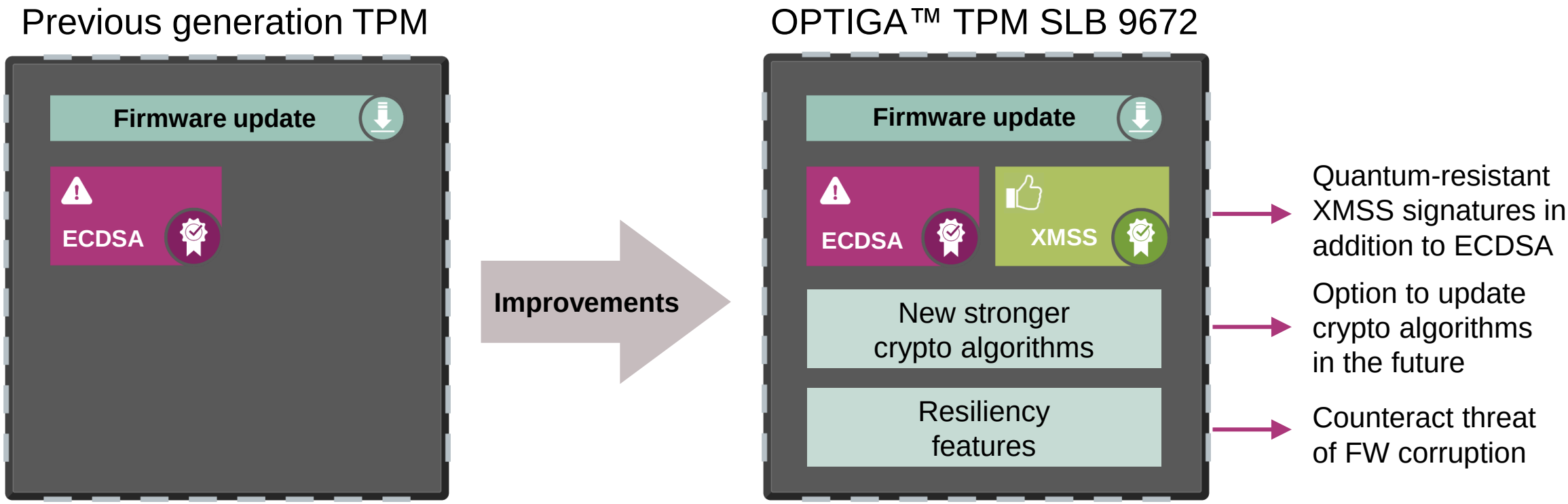
Infineon TPM: First steps into the world of quantum computing

OPTIGA™ TPM SLB 9672:

The first TPM on the market with a **PQC protected** firmware update mechanism.

OPTIGA™ TPM SLB 9672, a future-proof TPM

A PQC protected firmware update mechanism is essential
for the security over the entire operational lifetime of a TPM



Quantum computers, a threat to currently known crypto algorithms

Asymmetric cryptosystems (RSA/ECC):
Completely broken using **Shor's algorithm**

Currently	Quantum world
ECC-256 and RSA-3072 have **128-bit** security	Almost **no** security

Symmetric cryptography:
Security levels effected by **Grover's algorithm**

Currently	Quantum world
AES-128 has **128-bit** of security	AES-128 has about **128-ε-bit** of security*

Quantum world (in 10-20 years)

Heavily affected:
RSA, ECDSA, ECDH

Currently considered safe:
AES-128*, AES-256, SHA-256*, SHA-512, SHAKE256, SHA3-512, …

* Quantum-Resistant Cryptography by Ericsson Security Research: https://arxiv.org/ftp/arxiv/papers/2112/2112.00399.pdf
NIST Post-Quantum Cryptography FAQs: https://csrc.nist.gov/Projects/post-quantum-cryptography/faqs

Hash-based PQC algorithms are ready today

NIST SP 800-208: “Recommendation for Stateful Hash-Based Signature Schemes”

- Date published: October 2020
- Included algorithms: LMS, XMSS
- Hierarchical multi-level variants: HSS, XMSS^{MT}
- Hash functions: SHA-256 and SHAKE256
- Limited number of signatures: (2^{10} – 2^{60})
- Recommended for firmware updates
- **128-bit post-quantum security**

Advantages

- Well understood
- Fast verification
- “Small” key/signature size

Drawbacks

- (Very) slow key generation
- State **must not** be reused!
- Number of signatures limited

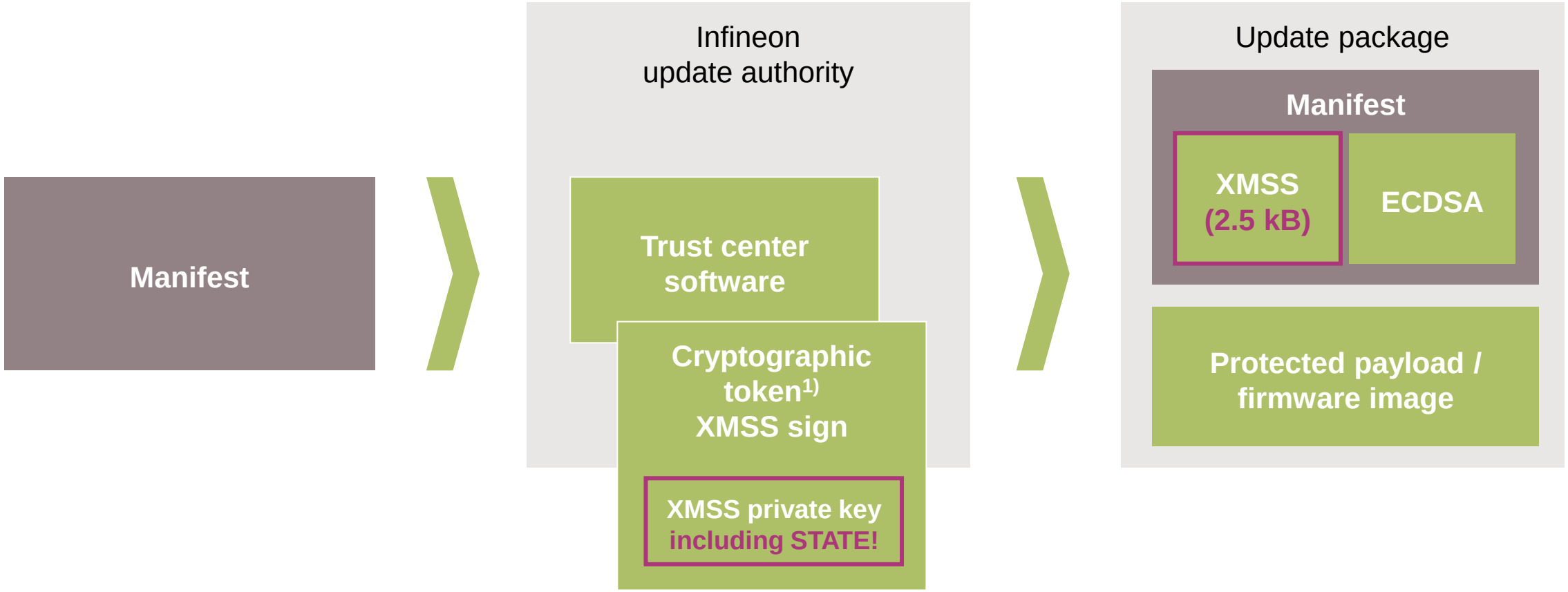
XMSS time/area trade-offs (example)

		[Bytes]			[hash calls]			[seconds]		
#signatures	variant	public key	secret key	signature	KeyGen	Sign	Verify	KeyGen	Sign	Verify
2^10	XMSS-SHA2_10_256	64	1.373	2.500	1.238.016	5.725	1.149	149	0,69	0,14
2^16	XMSS-SHA2_16_256	64	2.093	2.692	79.000.000	9.163	1.155	9.480	1,10	0,14
2^20	XMSS-SHA2_20_256	64	2.573	2.820	1.268.000.000	11.455	1.159	152.160	1,37	0,14
	XMSSMT-SHA2_20/2_256	64	5.998	4.963	2.476.032	7.227	2.298	297	0,87	0,28
	XMSSMT-SHA2_20/4_256	64	10.938	9.251	154.752	4.170	4.576	19	0,50	0,55
2^40	XMSSMT-SHA2_40/2_256	64	9.600	5.605	2.535.000.000	13.417	2.318	304.200	1,61	0,28
	XMSSMT-SHA2_40/4_256	64	15.252	9.893	4.952.064	7.227	4.596	594	0,87	0,55
	XMSSMT-SHA2_40/8_256	64	24.516	18.469	309.504	4.170	9.152	37	0,50	1,10
2^60	XMSSMT-SHA2_60/3_256	64	16.629	8.392	3.803.000.000	13.417	3.477	456.360	1,61	0,42
	XMSSMT-SHA2_60/6_256	64	24.507	14.824	7.428.096	7.227	6.894	891	0,87	0,83
	XMSSMT-SHA2_60/12_256	64	38.095	27.688	464.256	4.170	13.728	56	0,50	1,65

› @100 MHz, 12000 cycles for 3 SHA-256 blocks (openssl, 32-bit ARM), secret key/sign using BDS algorithm

Quantum-resistant update package generation @ update authority

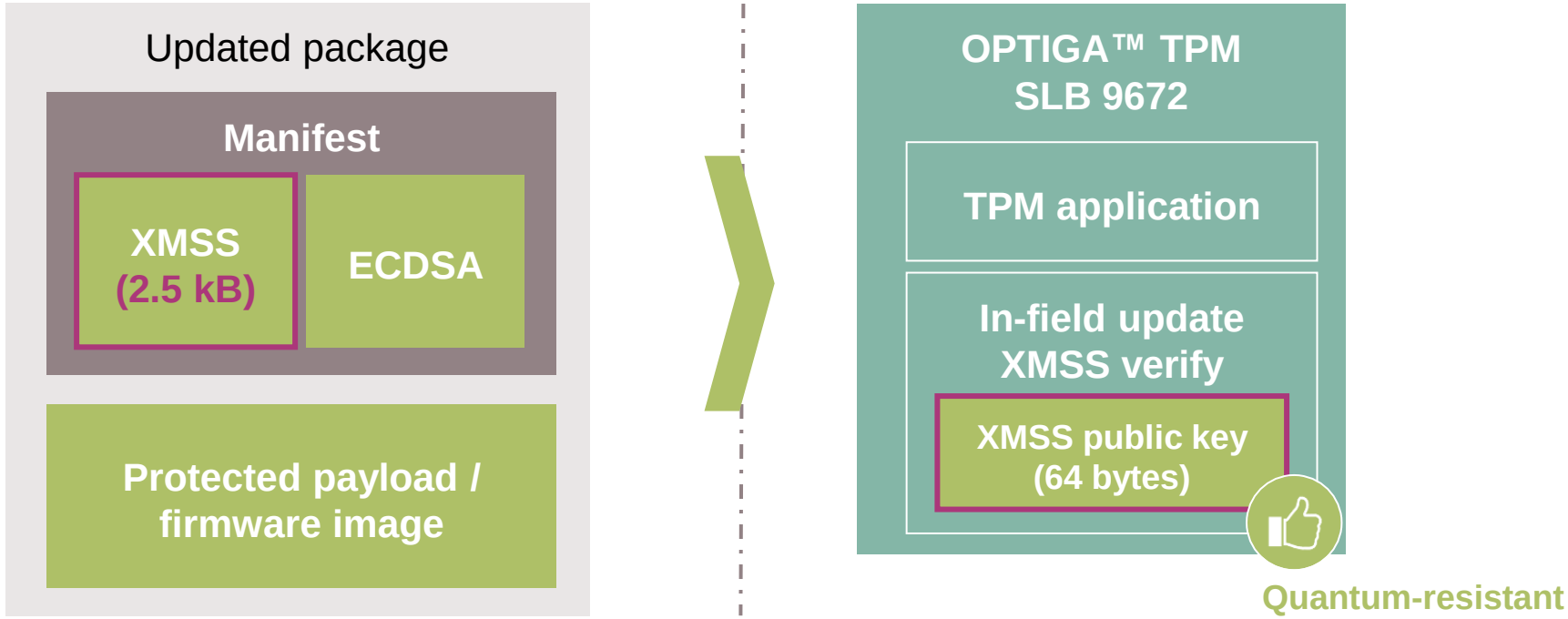
Update authorities manage the valid XMSS keys, including the state (counter) and backups.
Then it provides secured operations and allows clear business continuity.



1) Infineon Java Card

Quantum-resistant update package processing @ OPTIGA™ TPM

In the field, the OPTIGA™ TPM SLB 9672 checks the PQC protected XMSS signature and consequently validates (or not) the transferred payload.



Crypto agility

Challenge: migration and agility

- RSA and ECC are used almost everywhere (big investment)
- Integration of new crypto into old protocols
- Need for flexible replacement of crypto
- Ship today and update cryptography later
- The hardware needs to support PQC
- Hybrid requirements lead to cost increase
- **The firmware update mechanism is essential to enable long-term security**

Part of your life. Part of tomorrow.