



Welcome to a new generation of future-proof TPMs: OPTIGA™ TPM SLB 9672

Guillaume Rimbault
Senior Manager TPM Product Marketing & Management
16 February 2022



Why 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 the essential trust anchor

Discrete TPM, key root of trust for multiple applications

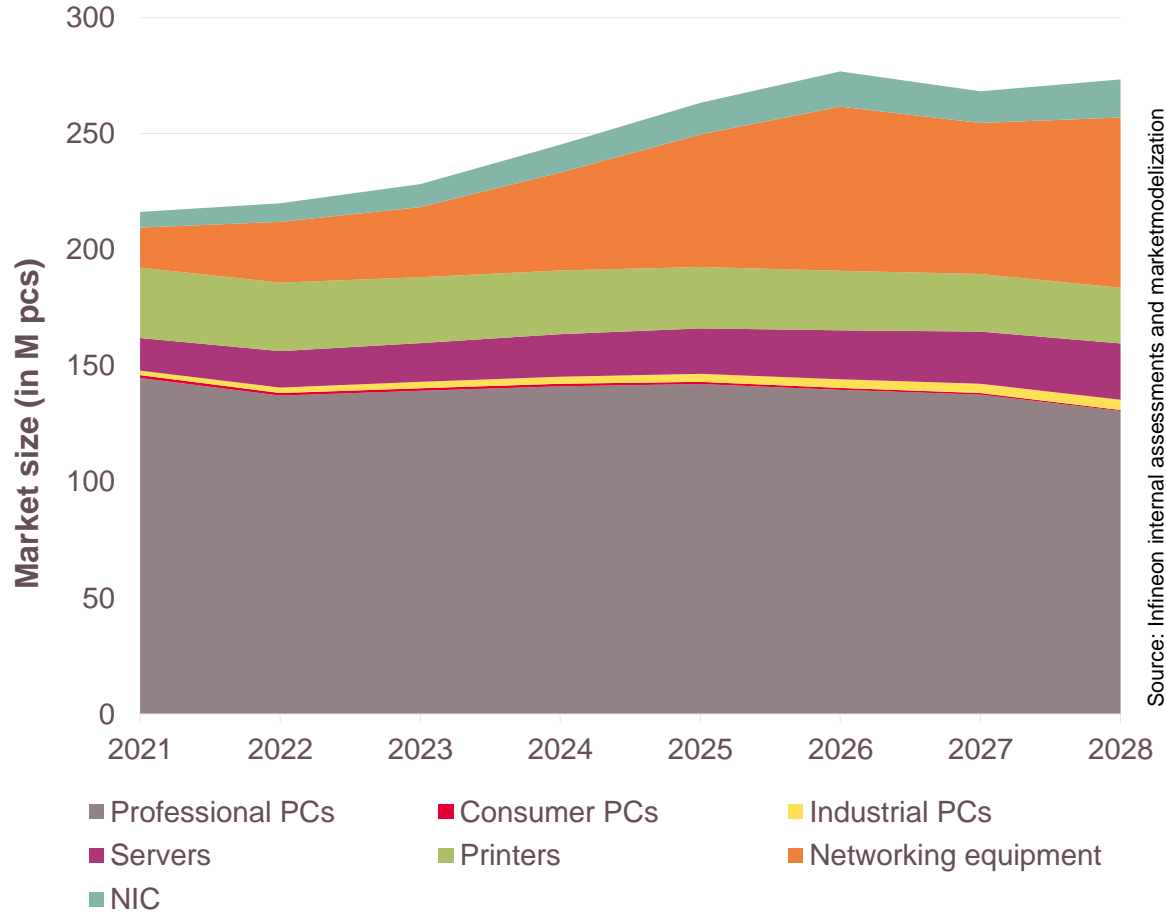
What a TPM does

- > 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



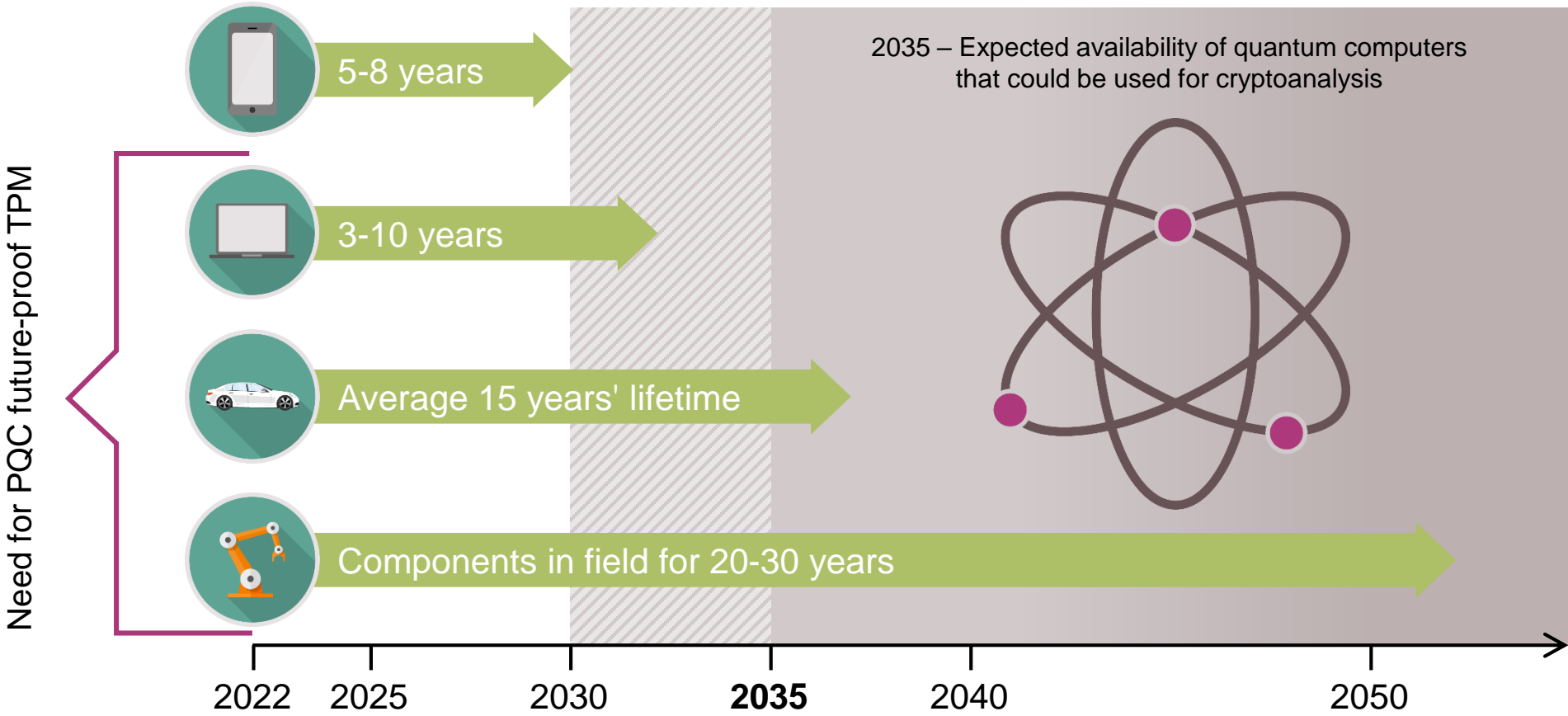
Future challenges for TPMs: The threat of quantum computers to cryptography

Within the next 10 to 20 years, quantum computer attacks on today's cryptography are expected to become reality.



Considered timeline

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



Quantum computers, a threat to currently known security algorithms

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

Currently

ECC-256 and RSA-3072 have **128-bit** security



Quantum world

Almost **no** security

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

Currently

AES-128 has **128-bit** security



Quantum world

64-bit security

Quantum world
(in 10-20 years)

Heavily affected:
RSA, ECDSA, ECDH

Affected:
AES-128, 3DES

Currently considered safe:
AES-256, SHA-256*, SH-A512,
SHAKE-256, SHA3-512, ...

* Preimage resistance

The key benefits with Infineon's newest TPM family member – OPTIGA™ TPM SLB 9672



Future-proof

- › PQC-protected firmware update mechanism
- › Extended memory space
- › Stronger cryptographic algorithms

Robust security

- › Improved computational performance
- › Resiliency features
- › Fully compliant with the TCG requirements and certified accordingly

Easy integration

- › Standardized root of trust
- › Tools to support design activities
- › Supports the latest versions of Windows and Linux

The new TPM 2.0 with SPI interface for computing

Trusted Platform Module: Secure your software and data

- › Compliant with TCG 2.0 rev.1.59 specification

Certified and standardized security

- › Official TPM product listed by Trusted Computing Group (TCG)
- › Independently security-evaluated and -certified:
 - According to the international Common Criteria standard
 - FIPS 140-2 certification pending
- › Meets already known Windows requirements effective April 2023 (23/H1)
- › Compliant with new NIST SP 800-90B

Meets demanding requirements

- › Operating temperature range -40 to +85°C
- › Extended lifetime of 10 years
- › Supports 192-bit key length with preparation for 256-bit key length by FW updates
- › Support for various cryptographic algorithms:
 - up to RSA-4096
 - AES-256
 - ECC NIST P256, ECC BN256, ECC NIST P384
 - SHA2-256, SHA2-384
- › Firmware upgrade capability with PQC-protected firmware update mechanism
- › Increased space for key or data storage in NV index data (~51 KB)
- › 3 GPIO



Applications

- › Servers and PCs
- › Computing and data storage
- › Network infrastructure devices and equipment such as
 - Gateways
 - Routers
 - Wireless access points
 - Network interface cards
 - Switches
- › Intel x86, ARM platforms and others

Product details (SLB 9672 FW15.21)

Set-up	Turnkey	Interface	SPI
Data store	51 kB	Cryptography	AES*, ECC, RSA, SHA
Availability status	Mass production in November 2021	Package	UQFN-32, 5x5 mm ²

More Info

<http://www.infineon.com/OPTIGA-TPM-SLB9672>

OPTIGA™ TPM SLB 9672:

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

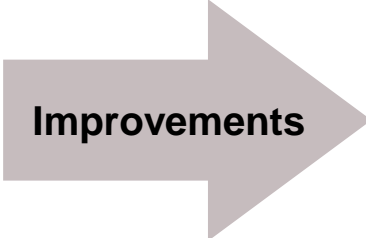


OPTIGA™ TPM SLB 9672, a future-proof TPM

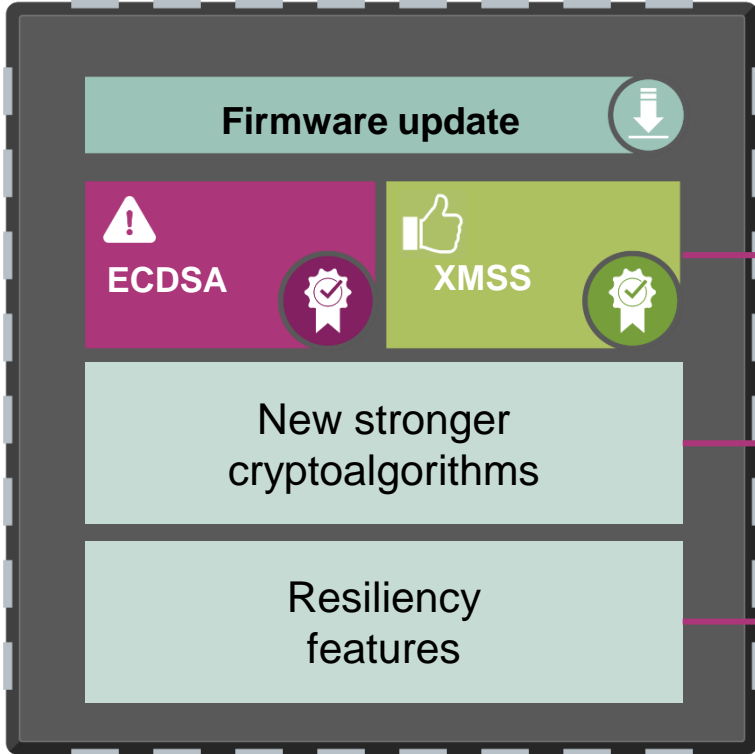
Previous-generation TPM



TCG-certified version 2
As per revision 1.38



OPTIGA™ TPM SLB 9672



- Quantum-resistant
- RSA 3k and 4k
SHA-384, ECC 384
- counteracts the threat of FW corruption

TCG-certified version 2
As per revision 1.59

PQC-ready with PQC-protected FW update mechanism essential for secured upgrades in the long term

The **FW update mechanism is essential for the security** of systems featuring a TPM over their entire operational lifetime:

From a security perspective, the trustworthiness of the TPM application cannot be higher than the FW package authentication strength.

The FW update mechanism and FW package signing key/algorithm should be as strong as possible. With quantum computing in development, a quantum-resistant algorithm in addition is recommended by BSI.

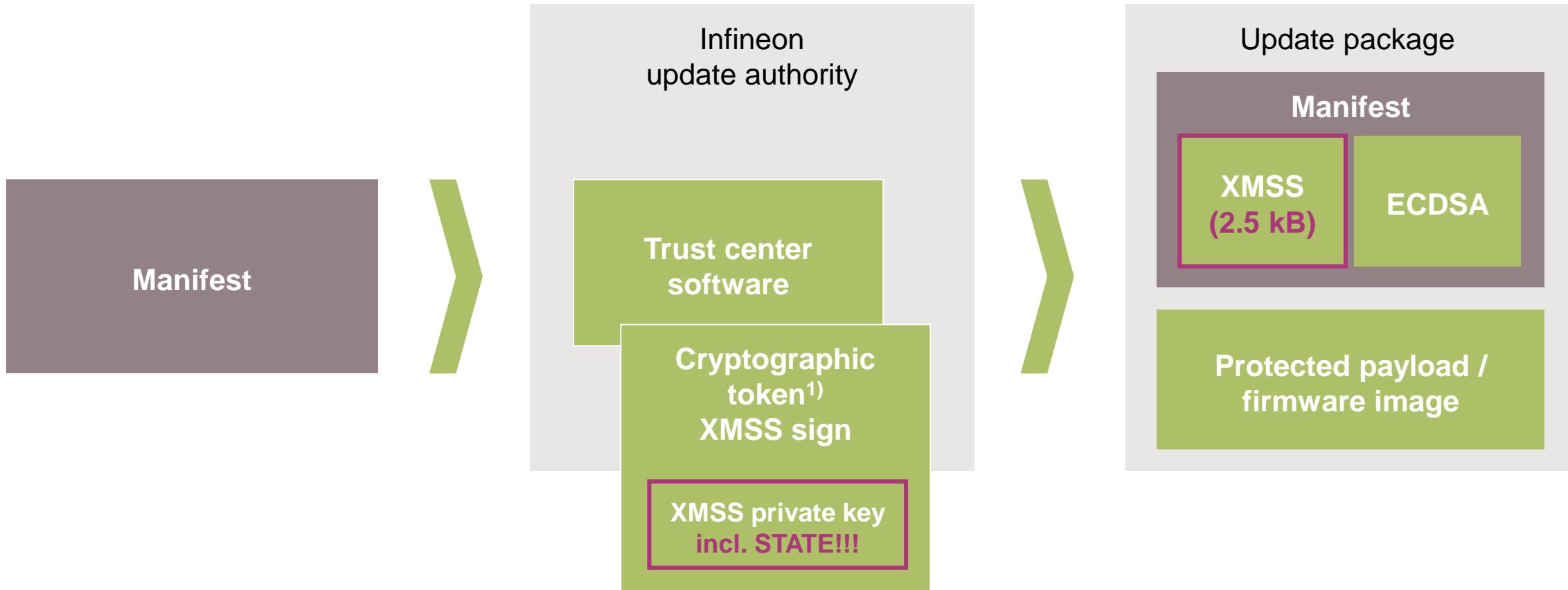
OPTIGA™ TPM SLB 9672 is equipped with a FW update mechanism using a 256 bit key length with an additive check, based on post-quantum cryptography (PQC).



The illustrated algorithm is recommended by NIST and BSI to protect firmware updates

Quantum-resistant update package generation @ update authority

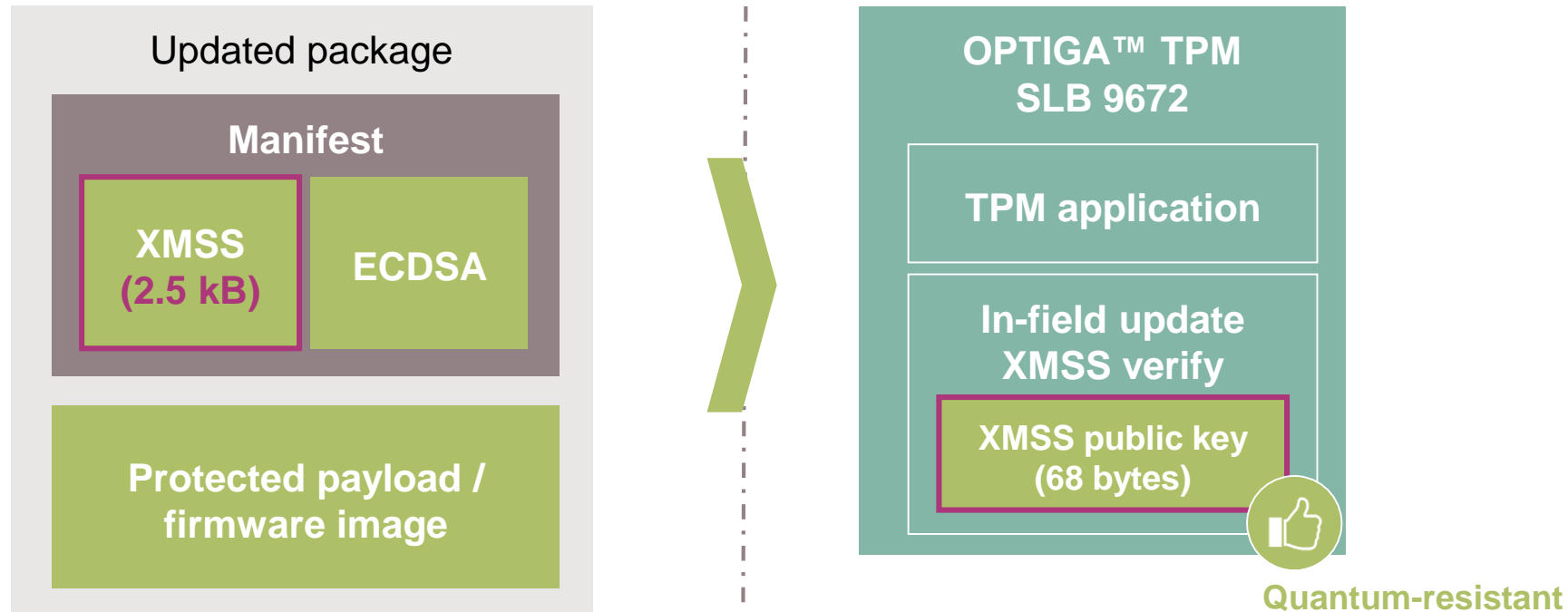
Update authorities manage the valid XMSS keys.
Then it provides secured operations and allows clear business continuity.



1) Java Card

Quantum-resistant update package processing @ OPTIGA™ TPM


In the field, the OPTIGA™ TPM SLB 9672 is able to transparently check the XMSS key thanks to its PQC algorithm and consequently to validate (or not) the transferred payload.




The OPTIGA™ TPM family offers rich functionality and flexibility



OPTIGA™ TPM SLM 9670
Industrial



OPTIGA™ TPM SLB 9670
OPTIGA™ TPM SLB 9672
Consumer/loT



OPTIGA™ TPM SLI 9670
In car

OPTIGA™
TPM

Key take-aways



Security is essential, and standardized HW-based security provides benefits beyond strong security including time-to-market, logistics, and scalability



New requirements will be emerging in the near future because of quantum computers and the threat to existing cryptographic algorithms



OPTIGA™ TPM SLB 9672 is the right choice if you want to meet the challenges of today and tomorrow



Part of your life. Part of tomorrow.



Information and tools for OPTIGA™ TPM
are available on Infineon's website

www.infineon.com/tpm

and our GitHub repository

<https://github.com/Infineon/optiga-TPM>