PEACE OF MIND IN A DANGEROUS WORLD

Post-Quantum Secure Boot for Space Infrastructures

Petri Jehkonen

Director of Strategic Programs, Partner, Xiphera Ltd.

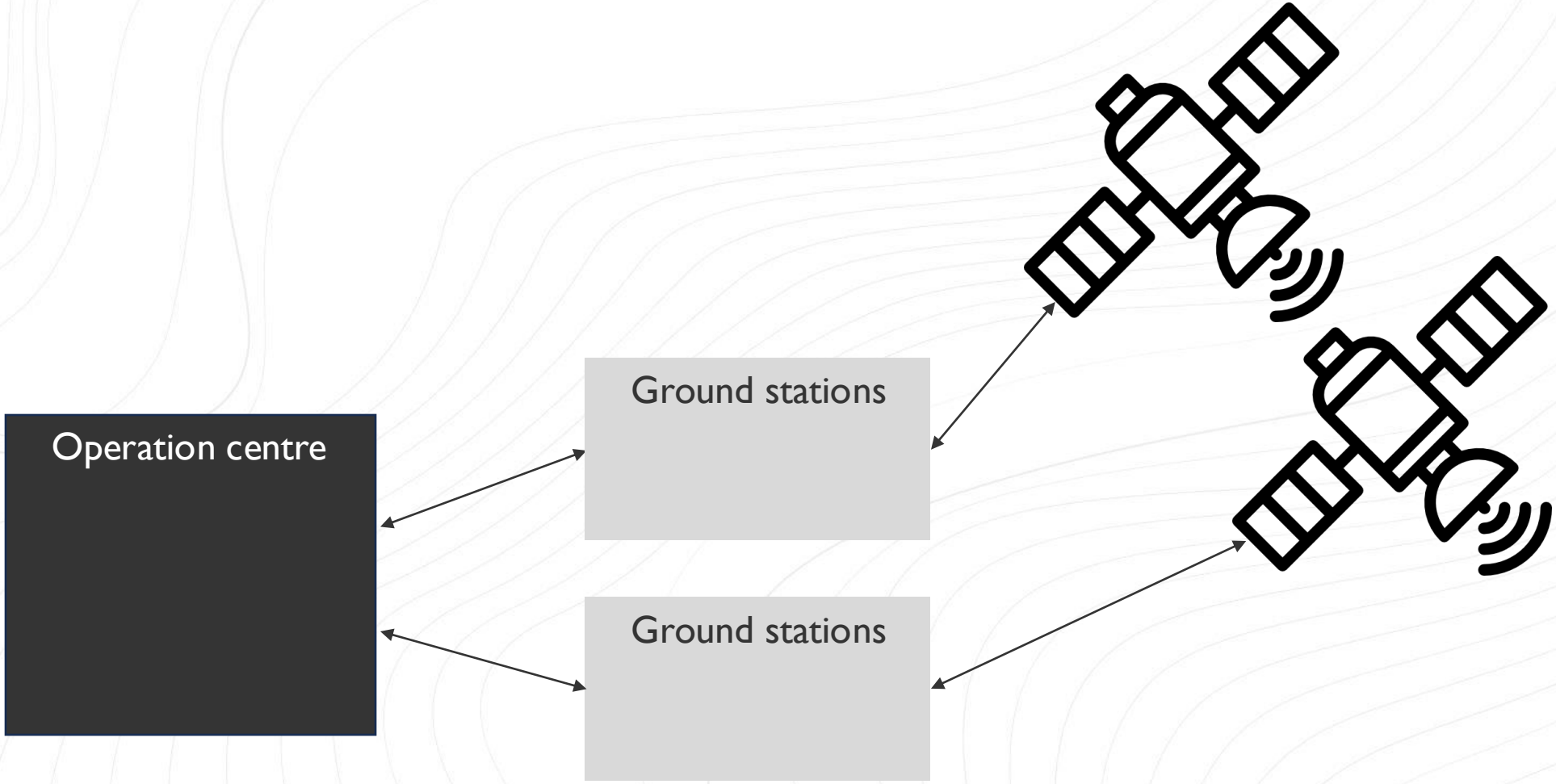
Agenda

1. Short Company Intro
2. Creating Trust in Computing Platforms
3. Platform Security Building Blocks
4. Introducing Secure Boot
5. Real-life Example: nQrux® Secure Boot
6. Hardware Root-of-Trust Elements

Xiphera Ltd.

- Finnish company founded in 2017
- Hardware-based security solutions with standardised cryptographic algorithms
- Secure and efficient cryptographic IP cores for digital logic (FPGAs and ASICs)
- All products and solutions designed fully in-house
- Committed roadmap to future cryptographic standards

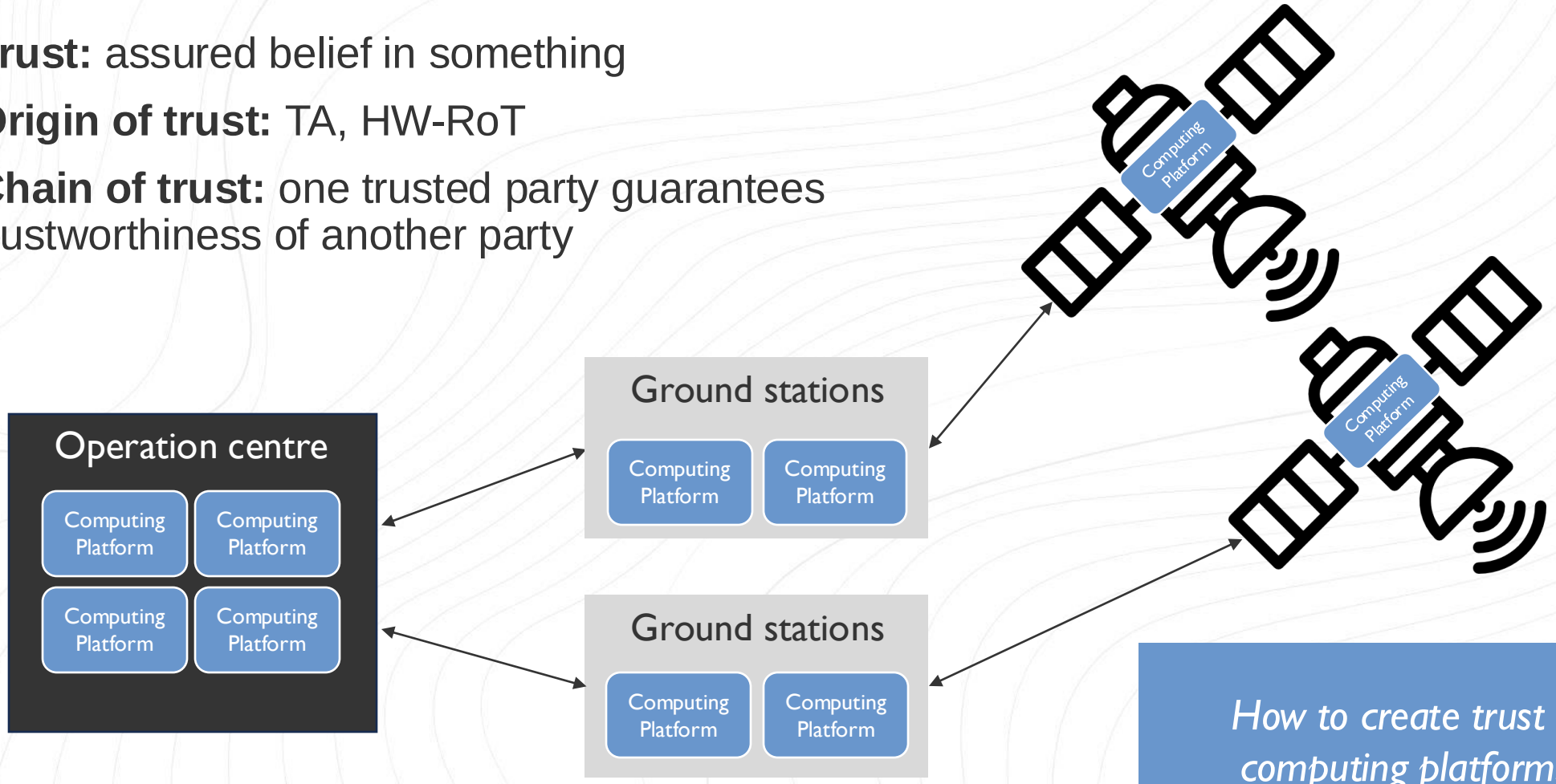
Why Do We Talk About Trust?



Icons from Freepik – Flaticon

Why Do We Talk About Trust?

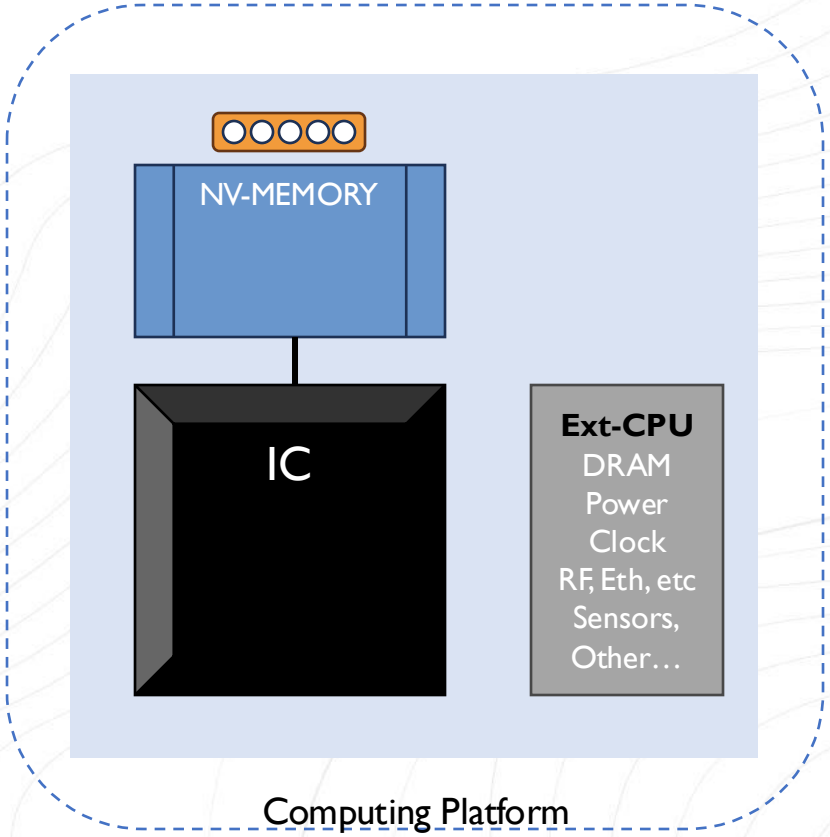
- **Trust:** assured belief in something
- **Origin of trust:** TA, HW-RoT
- **Chain of trust:** one trusted party guarantees trustworthiness of another party



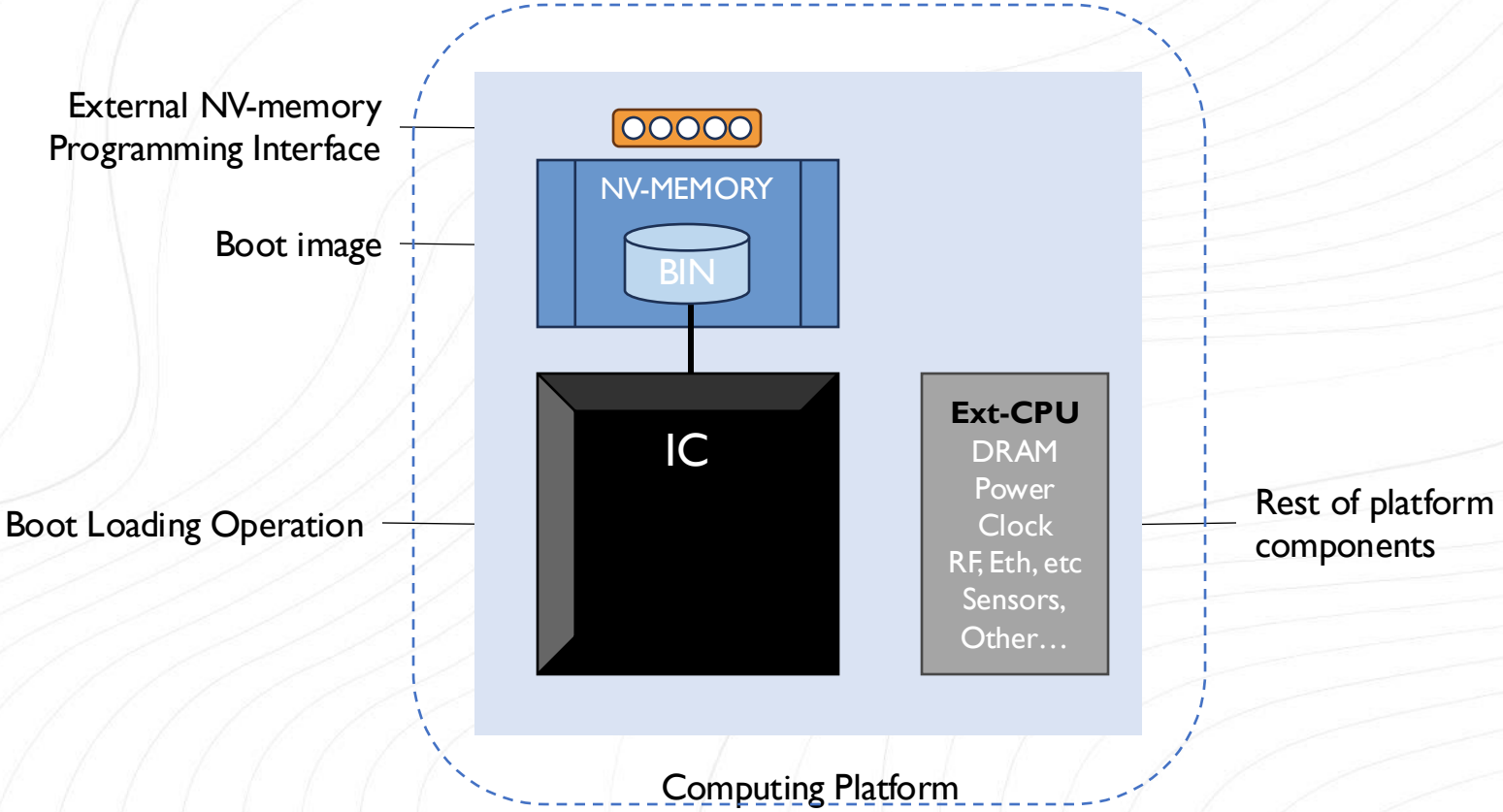
How to create trust on computing platforms?

Icons from Freepik – Flaticon

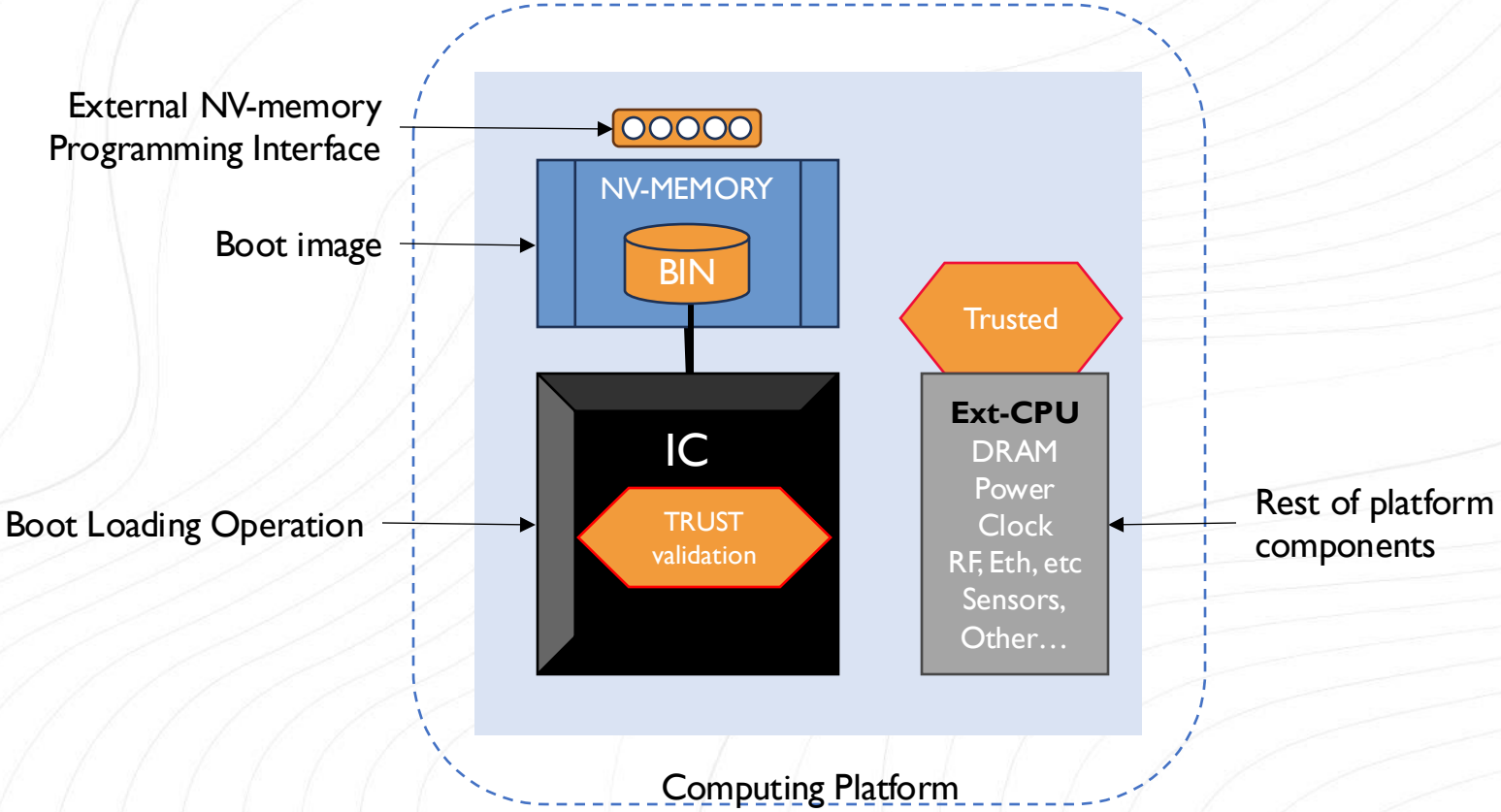
Creating Trust in Computing Platforms



Creating Trust in Computing Platforms



Creating Trust in Computing Platforms



The Imminent Quantum Threat

- Quantum computers of cryptographic significance do not (probably) exist today!
  - **Harvest now, decrypt later**
- Recap: QC attacks influence asymmetric algorithms
- **Key exchange and Digital signatures must be protected today** if the platform operations are to be trusted
- Transition to quantum-resilient cryptography with **hybrid** models

Secure Boot

- Combination of **confidentiality**, **integrity**, and **authenticity**
- Some **CPU/FPGA** vendors provide protection to boot-image:
  - Efficient, secure (to the point)
  - Pre-defined, neither versatile or agile
  - Typically not PQC
  - May require deep 3rd party SW-stack
- Agility is needed for platform protection
- PQC is needed for platform protection

To enable secure boot (a contemporary view)…

… Use **established** cryptographic algorithms

… Adopt **new** quantum threat mitigation schemes

… Deploy **hybrid** cryptographic protection!

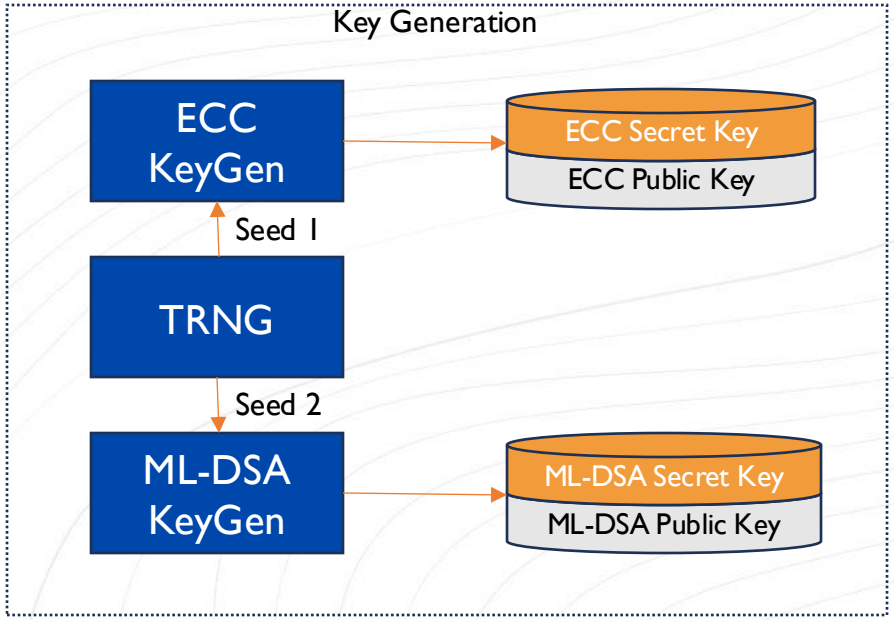
… Use **verified**, validated implementations of IP cores

… Go for **hardware** based solution

Real-life example:
nQrux® Secure Boot

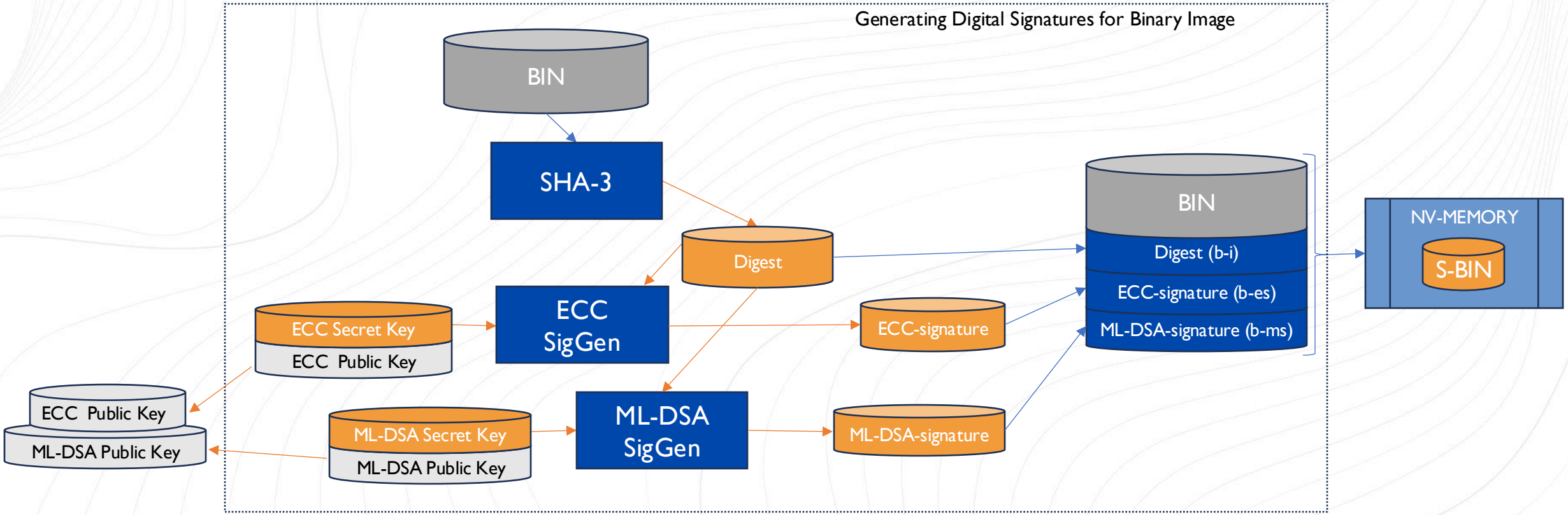
***We need** asymmetric key pair in association of high quality entropy source.*

Reminder:
Asymmetic cryptography uses key pair:
secret key and public key



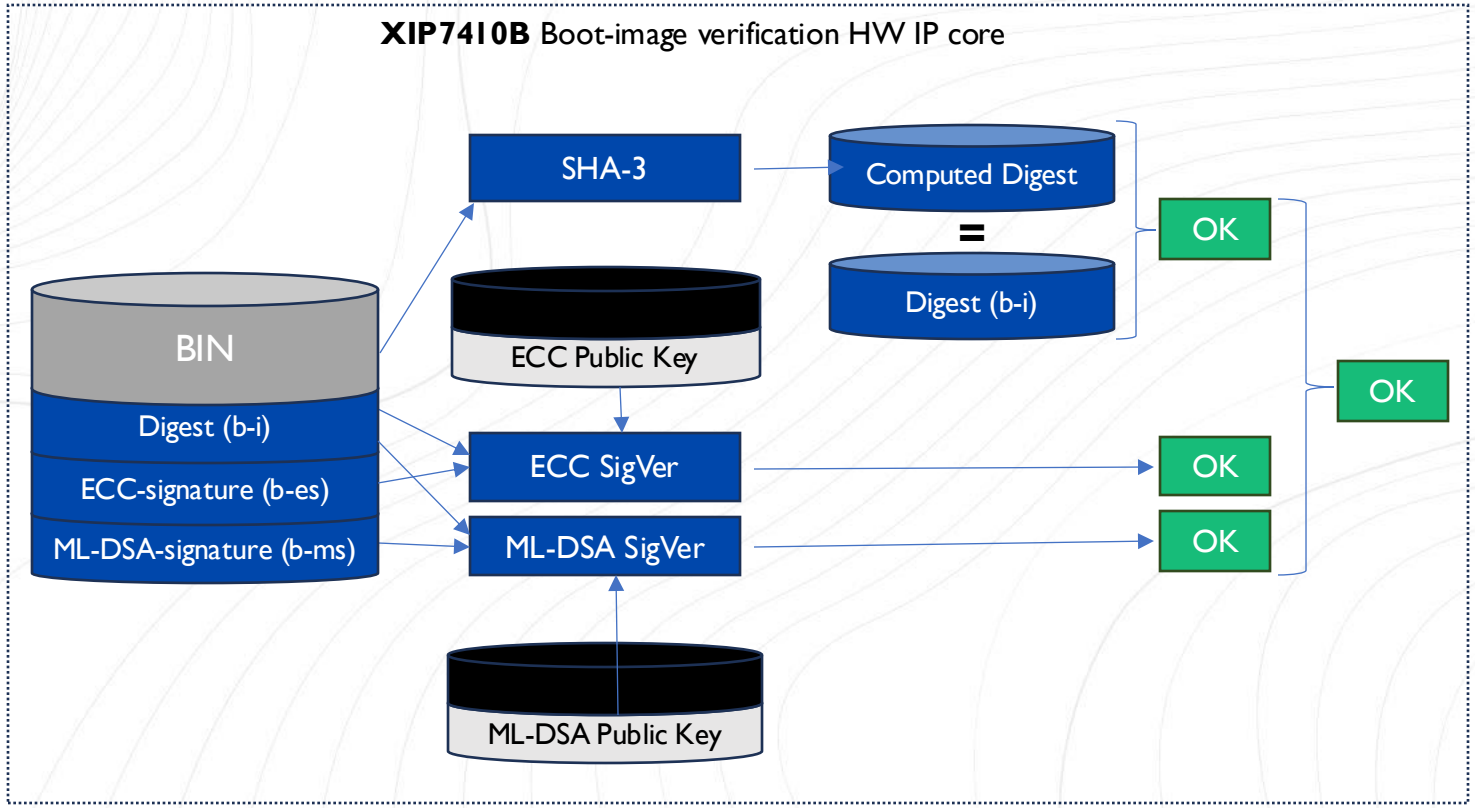
nQrux® Secure Boot

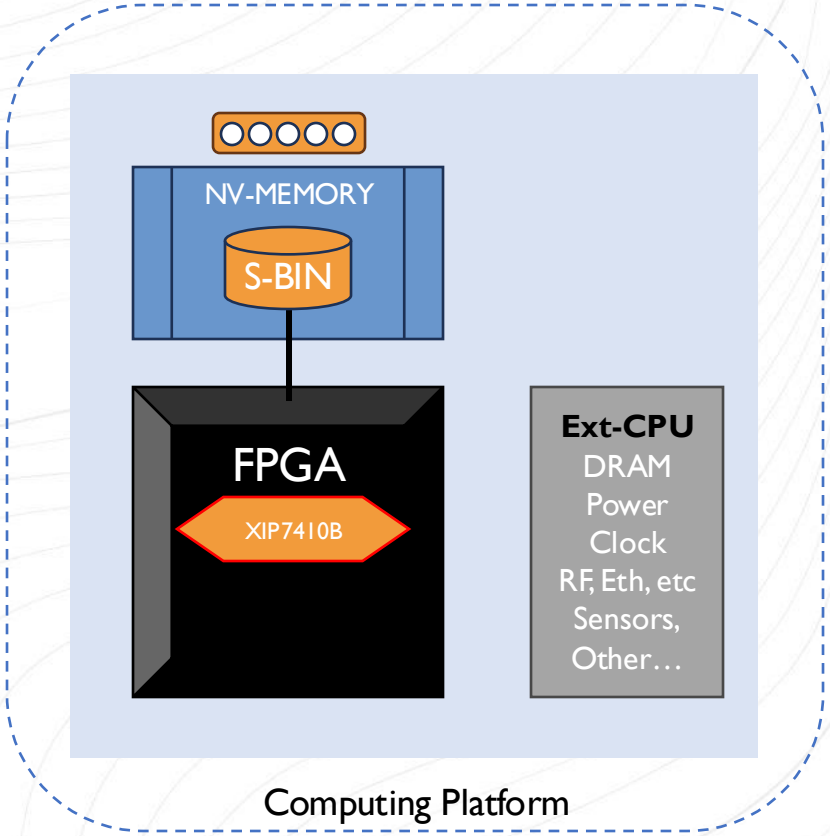
***Offline** tool for creating digital signatures for a system binary-image.*



nQrux® Secure Boot

IP core for FPGA or ASIC *to verify binary integrity and authenticity.*

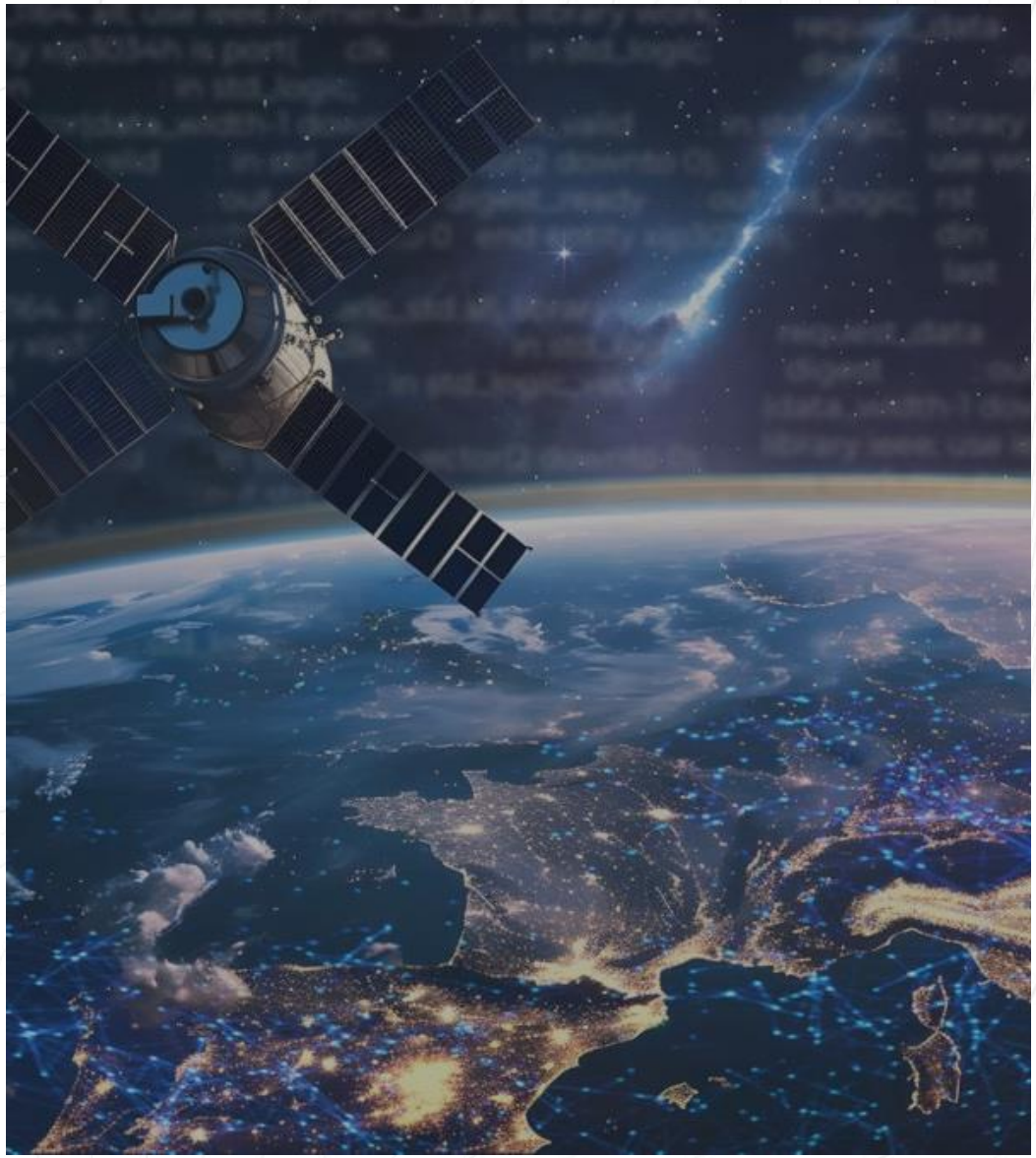




Sept 10, 2024:

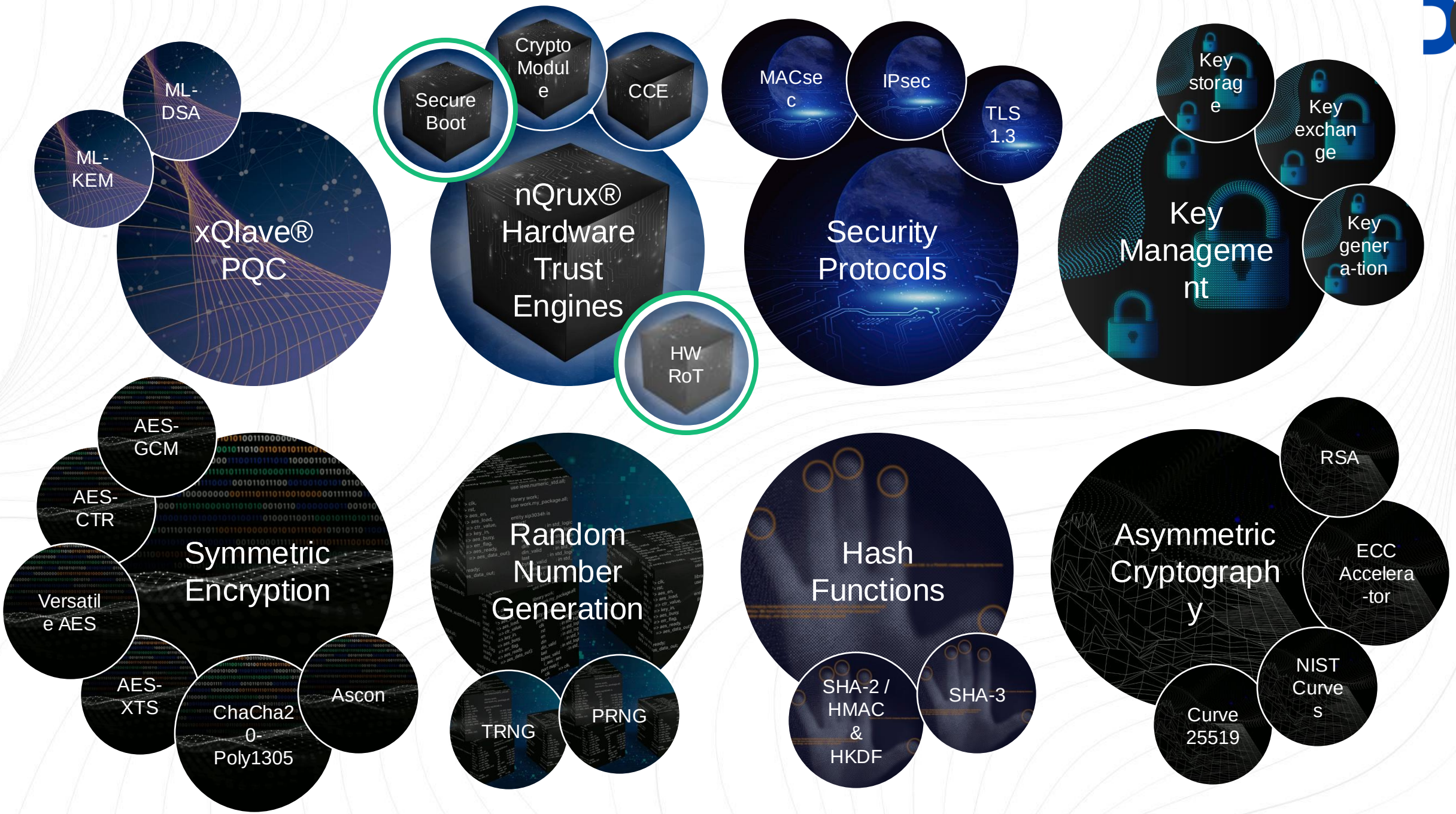
“Quantum-resilient Authenticated Boot for space-grade semiconductor architectures”

- Trust in the digital hardware components and system configurations in space and satellite infrastructures
- Development project partially financed by the European Space Agency, as part of its General Support Technology Program
- Integration into Frontgrade Gaisler’s space-grade GR765 processor



Hardware Root-of-Trust

- Trust is as good as its foundation
- Agility cope with changing requirements
- Immutable system level trust anchors


ML-DSA
ML-KEM
xQlave® PQC
Secure Boot
Crypto Module
CCE
nQrux® Hardware Trust Engines
HW RoT
MACsec
IPsec
TLS 1.3
Security Protocols
Key storage
Key exchange
Key Management
Key gener a-tion
AES-GCM
AES-CTR
Versatile AES
Symmetric Encryption
AES-XTS
ChaCha20-Poly1305
Ascon
Random Number Generation
TRNG
PRNG
Hash Functions
SHA-2 / HMAC & HKDF
SHA-3
RSA
Asymmetric Cryptography
ECC Accelera-tor
NIST Curves
Curve 25519

XIPHERA

PEACE OF MIND IN A DANGEROUS WORLD

Thank you!

Any questions?

Xiphera Ltd.

petri.jehkonen@xiphera.com

https://xiphera.com