XIPHERA

CRYPTOGRAPHY UNDER THE HOOD WEBINAR SERIES

Quantum-Resilient Secure Boot

Building Trust from Power-up

Petri Jehkonen

Director of Strategic Programs

Xiphera

Valtteri Allekotte

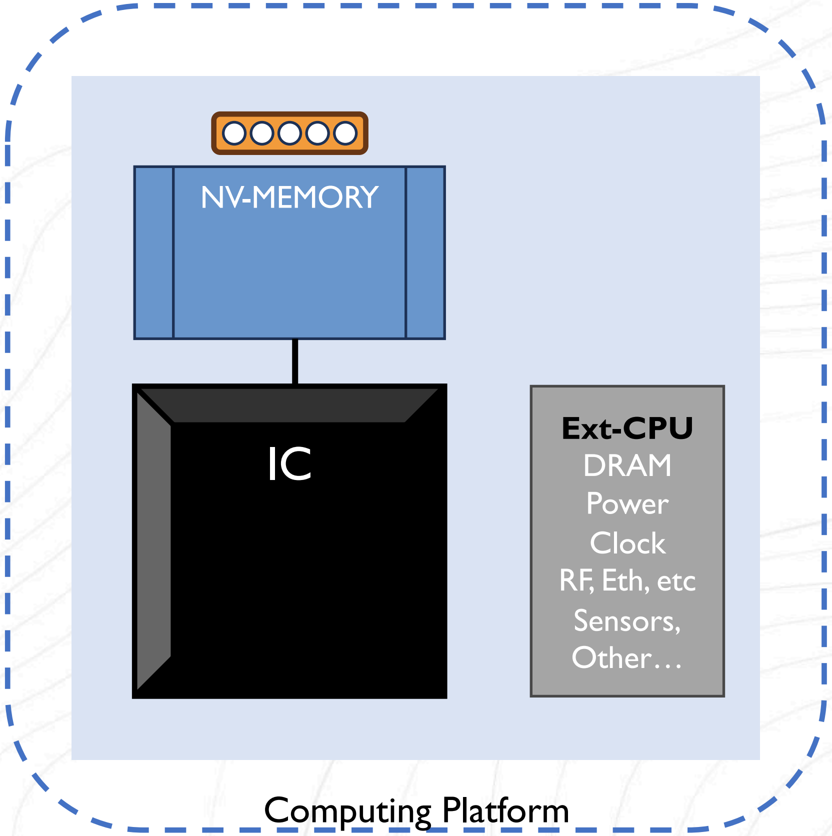
Developer

Xiphera

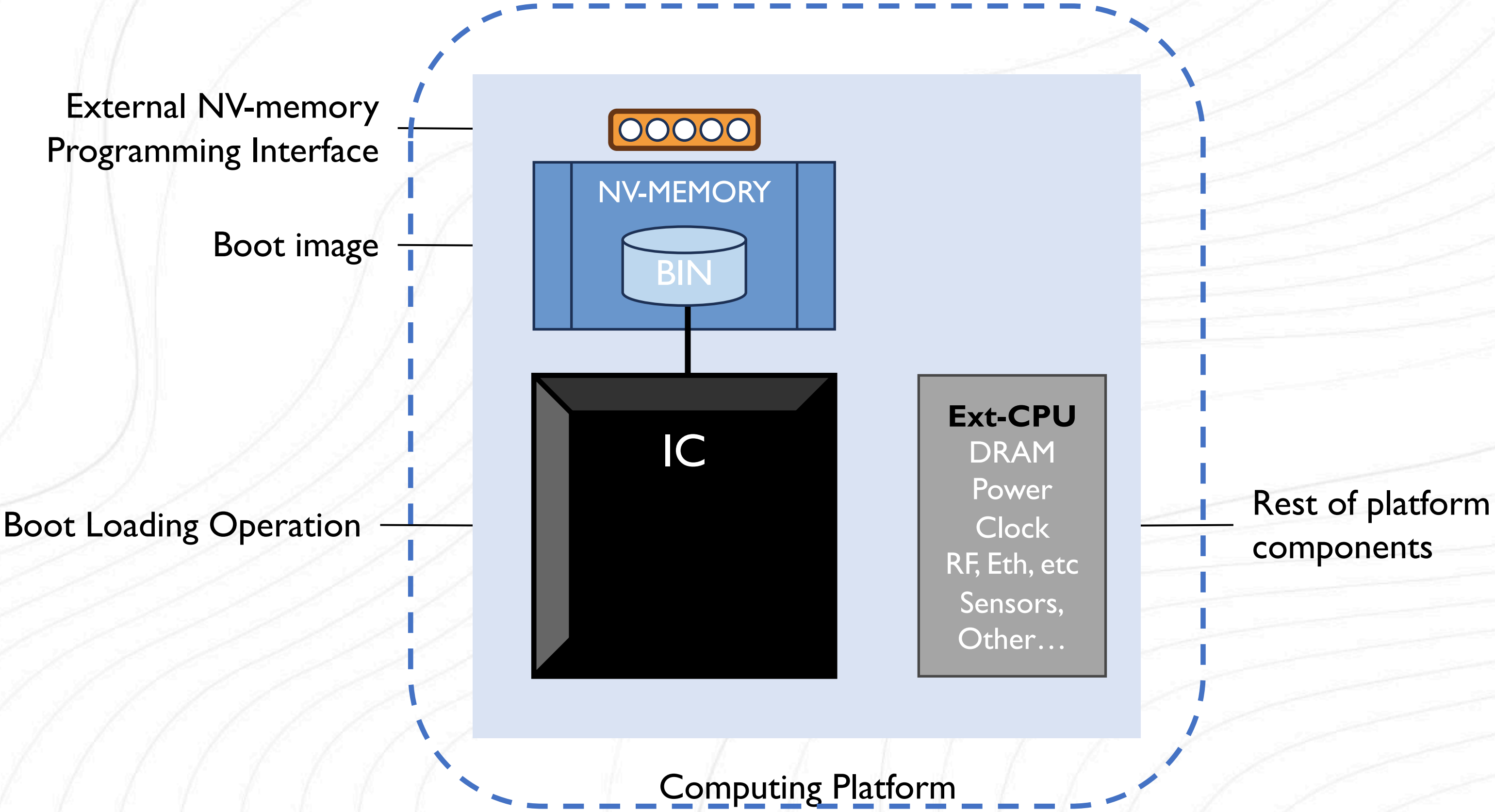
Agenda

1. Creating Trust in Computing Platforms
2. Secure Boot and Building Blocks
3. Real-life Example: nQrux® Secure Boot
4. Discussion

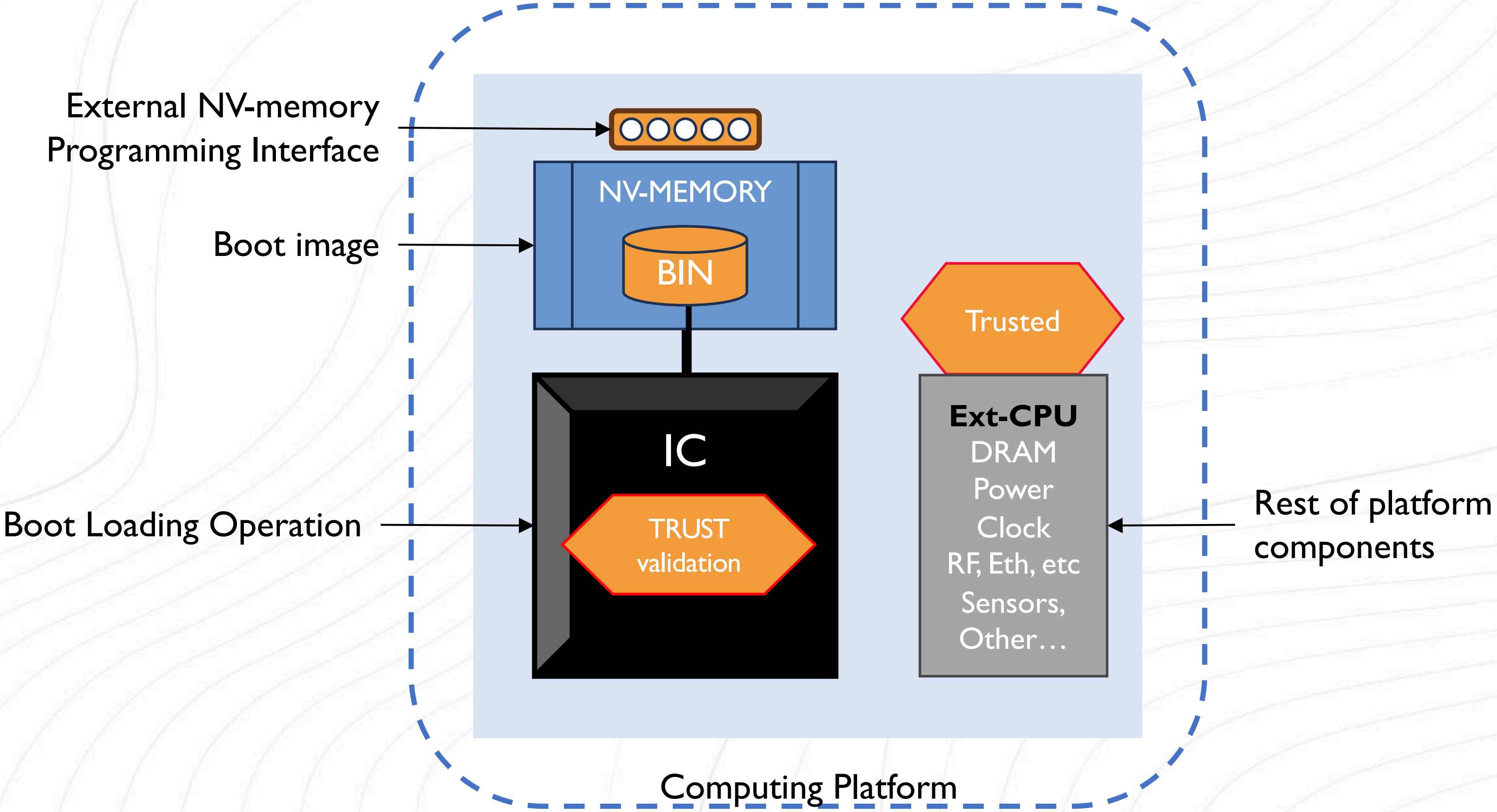
Creating Trust in Computing Platforms



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 protected 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

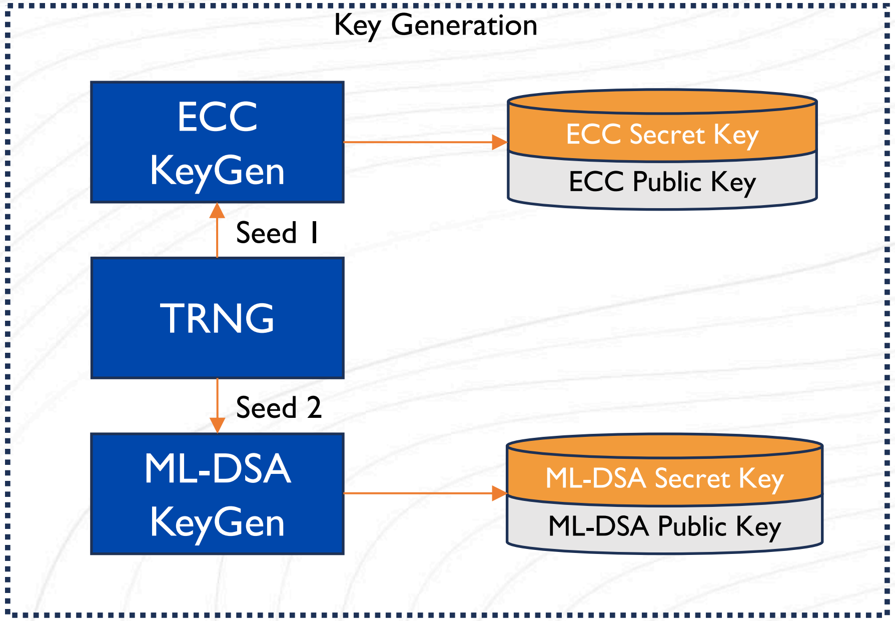
… Go for **hardware** based solution

Real-life example: nQrux® Secure Boot

***Creating trust** starts from creating asymmetric key pair with high quality entropy source.*

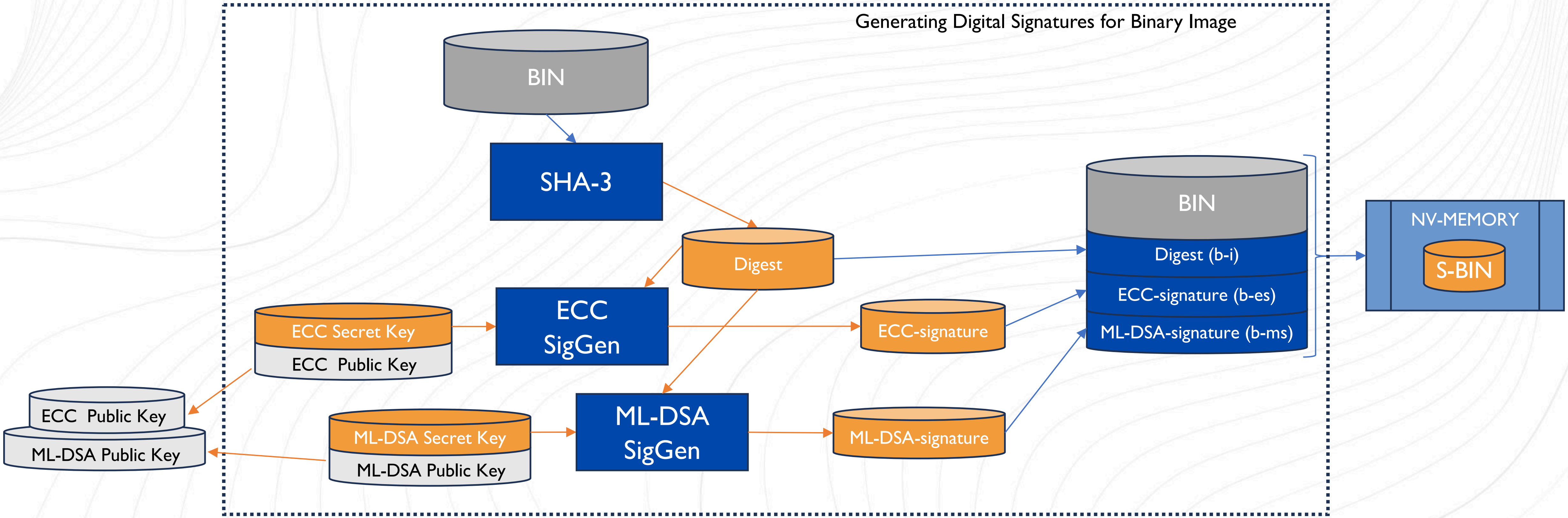
Reminder:
Asymmetic cryptography uses key pair:
secret key and public key

Asymmetric Secret Key
Asymmetric Public Key



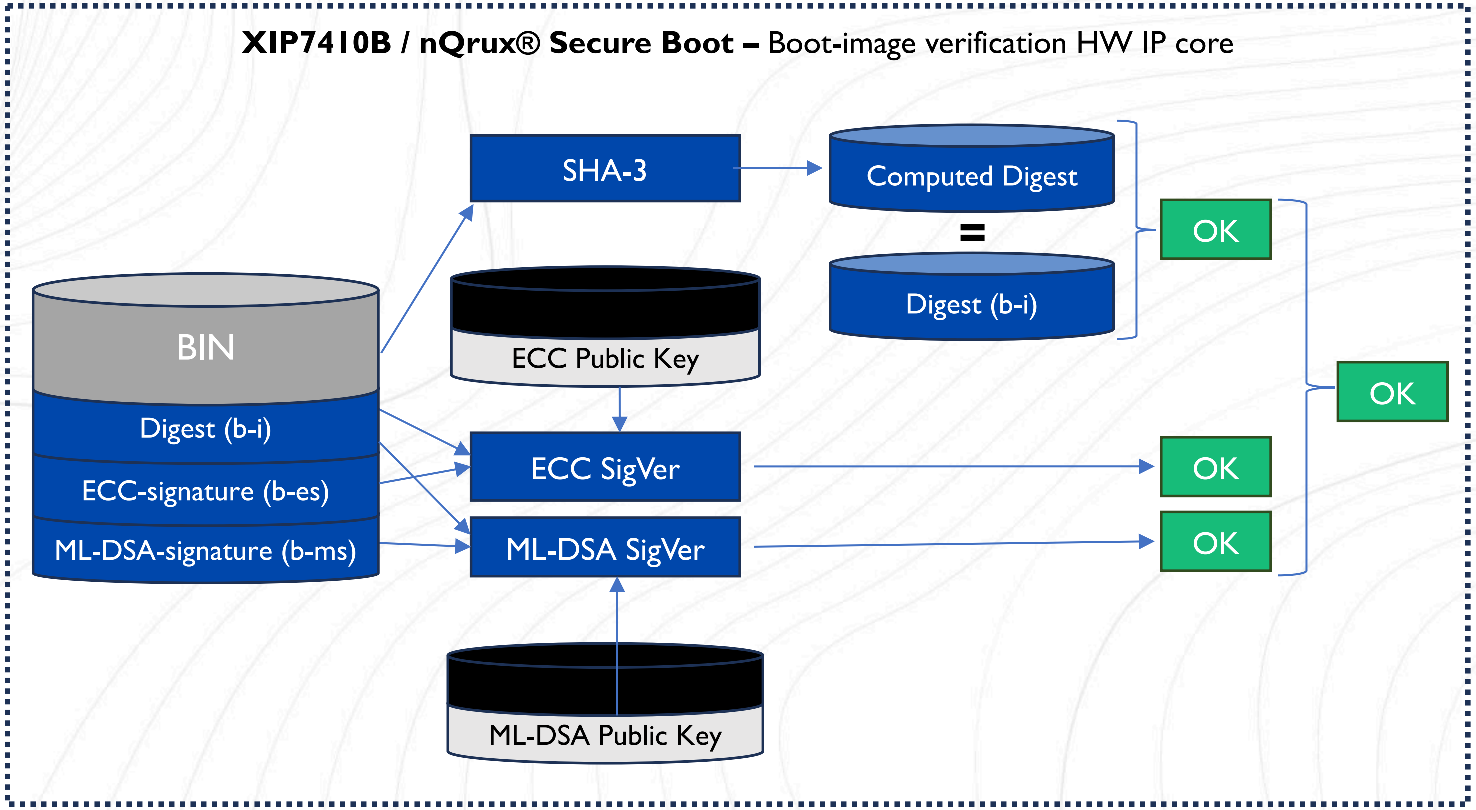
nQrux® Secure Boot

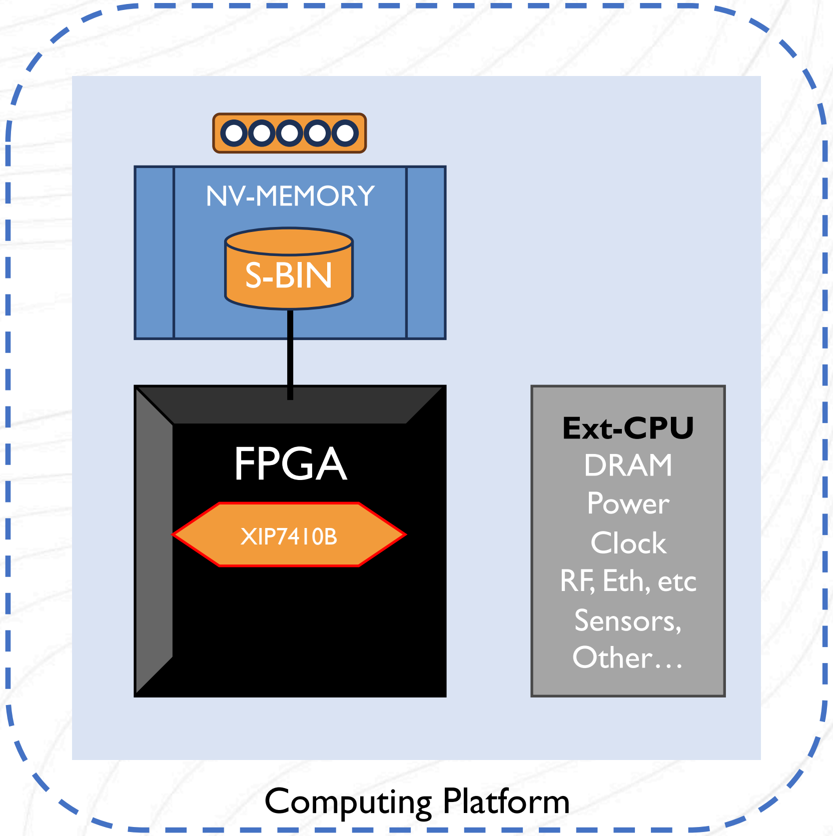
Offline *tool for creating digital signatures for a system binary-image.*



nQrux® Secure Boot

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

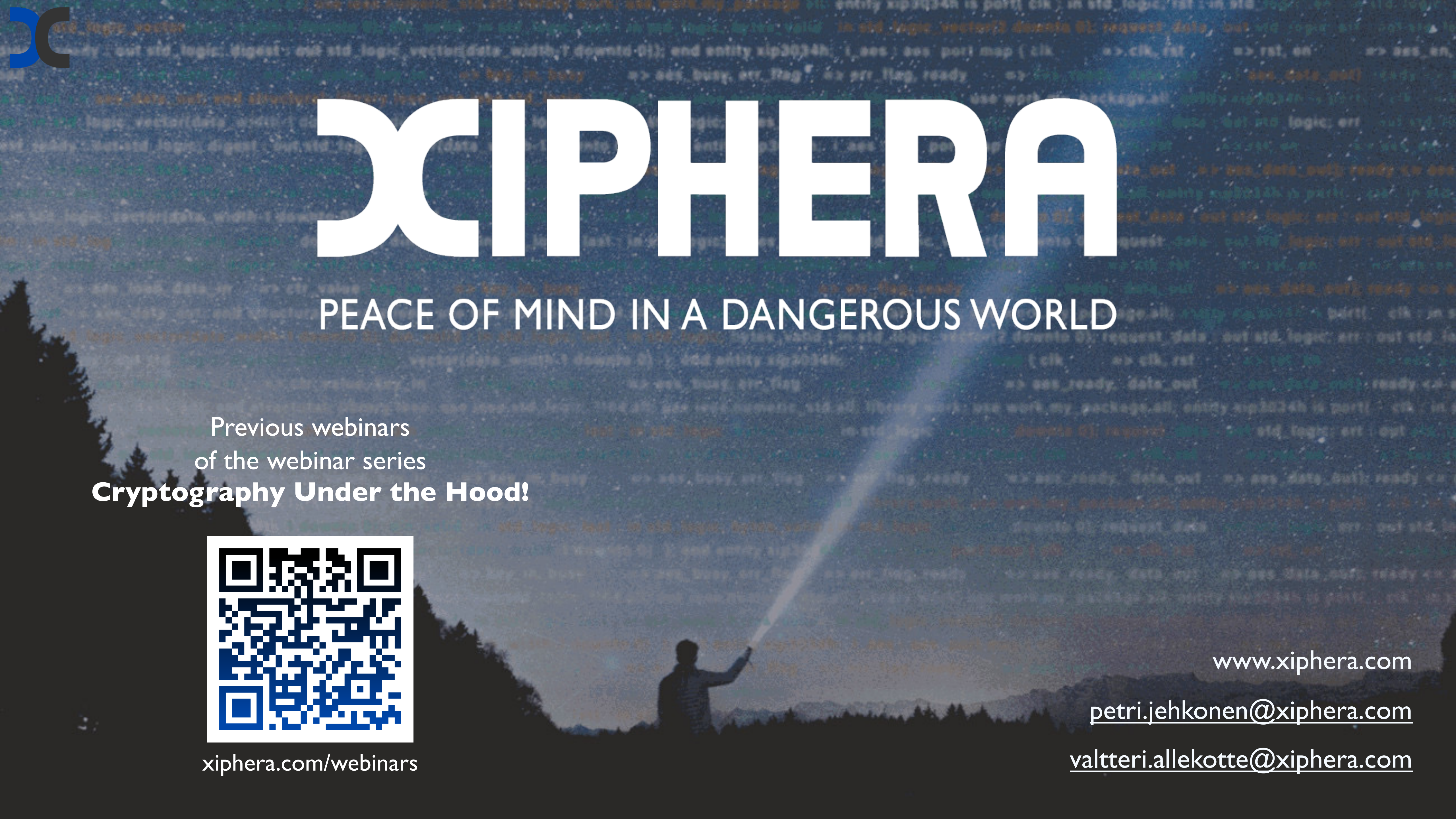




Sept 10, 2024:

“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



XIPHERA

PEACE OF MIND IN A DANGEROUS WORLD

Previous webinars
of the webinar series
Cryptography Under the Hood!

xiphera.com/webinars

www.xiphera.com

petri.jehkonen@xiphera.com

valtteri.allekotte@xiphera.com