NCCoE IoT Onboarding Project

Factory Provisioning Use-Case

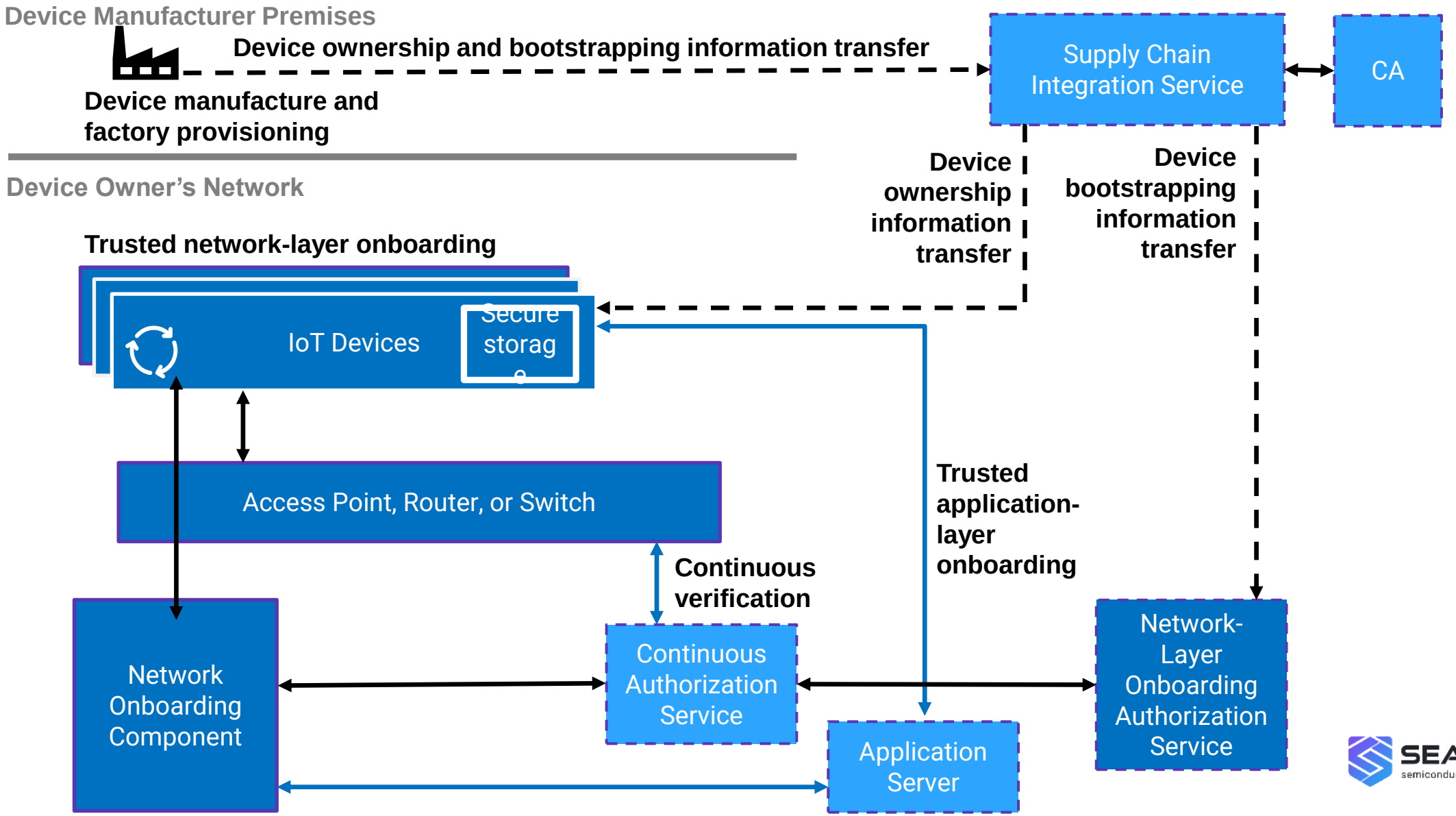
Minerva.Sandelman.ca
Sandelman Software Works

SEALSQ
- Steve Clark
  - Security Technologist
  - sclark@sealsq.com

Sandelman Software Works
- Michael Richardson
  - Chief Scientist

April 17th, 2025

High Level Architecture



The Factory Provisioning Use Case

- Objectives:
  - Demystify manufacturer provisioning
  - Simulate the pre-provisioned Secure Element scenario
  - Advocate that the identity of devices be **provisioned by the manufacturer**
  - Demonstrate online Certificate Management Service (CMS)
    - Using Trusted Certificate Authority (CA)
  - Document one or more flows involving BRSKI and DPP that uses a pre-provisioned secure element

SEAL SQ
semiconductors + quantum

Different Approaches to Provisioning

- Key-Pair Generated on IoT Device
- Key-Pair Generated in Secure Element
- Key-Pair Loaded into IoT Device
- **Key-Pair Pre-Provisioned onto Secure Element**
- Private Key Derived from Shared Seed

SEAL SQ
semiconductors + quantum

Typical Model of IoT Device Production – without Secure Element

- Device Board is Assembled
- Board is connected to “Bed of Nails” for setup and provisioning
- Diagnostic firmware is loaded
- Basic functionality is tested
- Keys and Certificates are loaded
  - This step requires a secure facility
- Production firmware is loaded
- Final test of IoT device

https://en.wikipedia.org/wiki/Bed_of_nails_tester

SEAL SQ
semiconductors + quantum

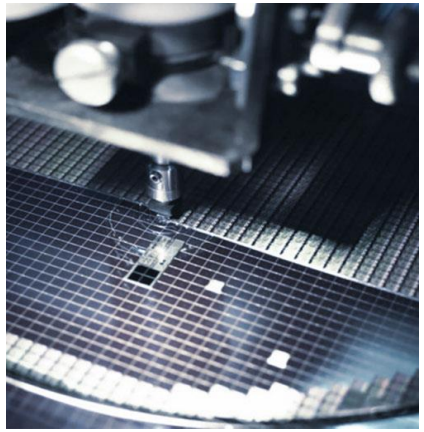
Typical Model of IoT Device Production – with Pre-Provisioned SE

- Device Board is Assembled
  - SE protects keys and certificates – secure facility requirement is minimized
- Board is connected to “Bed of Nails” for setup and provisioning
- Diagnostic firmware is loaded
- Basic functionality is tested
- Production firmware is loaded
- Final test of IoT device

https://en.wikipedia.org/wiki/Bed_of_nails_tester

SEAL SQ
semiconductors + quantum

Why Secure Chips?



- Host Companion - Crypto Co-Processor
  - Reduced requirements on the host processor (memory, speed, …)
  - Trusted Execution Environment (TEE)
  - Stored secrets are never exposed off the chip
- Hardware Based Security
  - Protect from side-channel, fault injection, probing, …
- Secure Storage
  - Secure key (secure identity)
  - Secure certificate & configuration
- Crypto Agility
  - Optimized crypto algorithms
  - PQC Implementations
- Secure Communication
  - Support for TLS/DTLS
- Secure Platform
  - Secure Update
  - Secure Boot
- Certifications & Compliance
  - FIPS140-3
  - Common Criteria EAL5+
- Pre-Provisioning
  - Simplified manufacturing security

Solutions for a Resource-Constrained Environment

- TPM
  - Wide range of cryptography supported
  - PQC support in next release of specification
  - Firmware update supported
  - Most (all?) security use cases for constrained devices supported.
  - Pre-provisioning

- Secure Element
  - Specialized secure devices
  - Usually a subset of TPM capabilities
  - Lower cost and size
  - Can support traditional crypto and PQC
  - Pre-provisioning varies by vendor

Solutions for a Resource-Constrained Environment

- Secure PQC MCU
  - Custom applications
  - Optimized crypto algorithms
  - Large crypto libraries available
  - PQC Optimization
  - Pre-Provisioning

- ASIC
  - Customizable – Ideal for specific use cases
  - Traditional crypto IP
  - PQC IP
  - Asynchronous TRNG
  - Certifiable
  - Pre-Provisioning

Demo Board

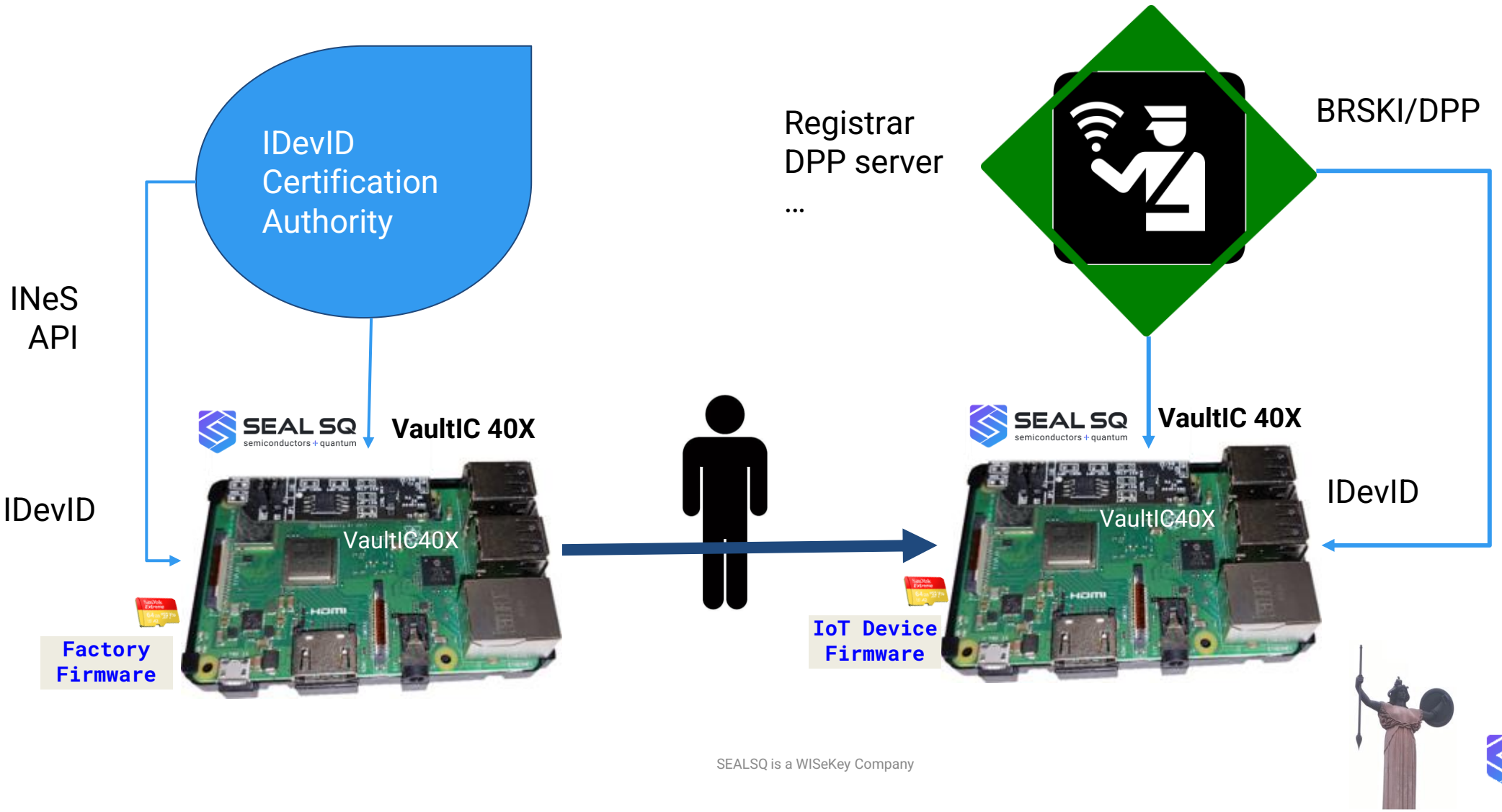
SEAL SQ
semiconductors

The Demo

- Implementation
  - Pre-provision a secure element with an immutable Identity
    - Key-Pair / Certificate
  - Install the secure element on an IoT edge device to establish the platform hardware root of trust and Identity
- Technologies
  - Raspberry Pi Platform
  - VaultIC40X Secure Element from SealSQ
  - INeS Certificate Management System API
  - INeS-Hosted Certificate Authority

SEAL SQ
semiconductors + quantum

Overview Factory Provisioning Use-Case Demo



SEAL SQ
semiconductors + quantum

Links to the Demo

- Get the Kit:
  - https://www.digikey.com/en/products/detail/sealsq/VIC408-TLS-RPI-STK/25701053?s=N4IgTCBcDaIM4FMCGAbOBHEBdAvkA
- Get the Source Code:
  - https://github.com/sealsq/NCCoE-Factory

Demo

SEAL SQ
semiconductors

Q & A

THANK YOU

Steve Clark
Security Technologist
sclark@sealsq.com

SEAL SQ
semiconductors