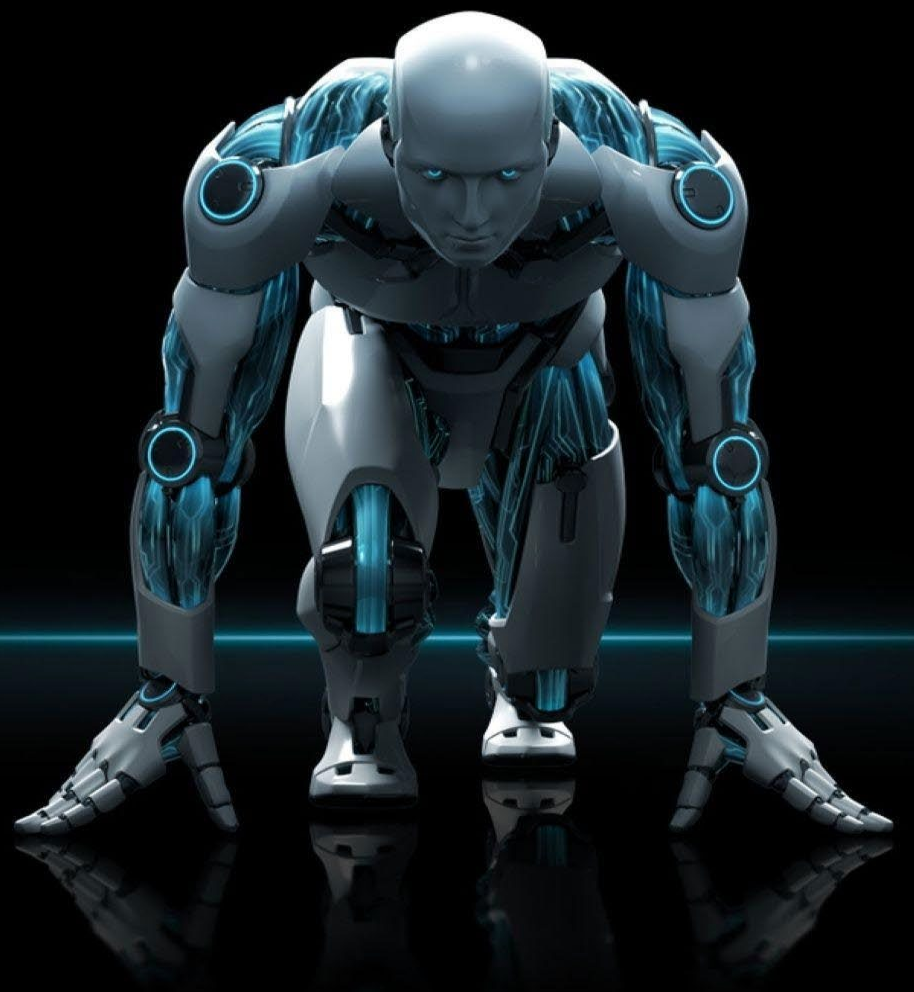
WISeKey

TRUST STARTS HERE

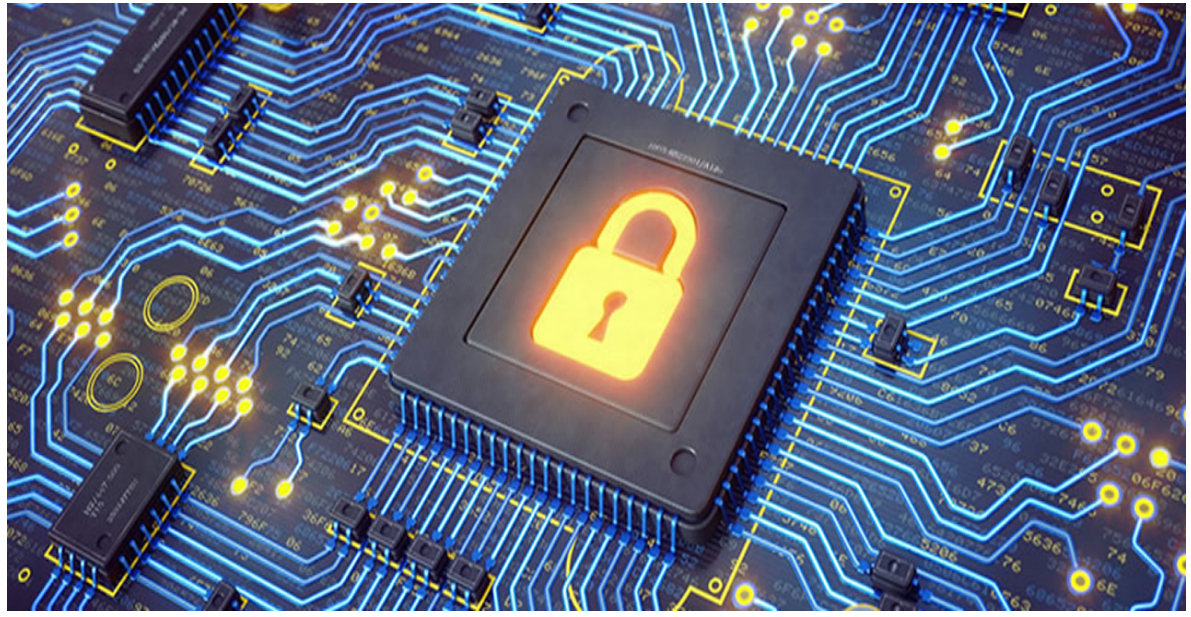
Enhancing IoT Device Security for Trusted Network-Layer Onboarding



Steve Clark
+1 719 600-8476
sclark@wisekey.com

SECURE ELEMENT BENEFITS

- Trust for Both the Home User and the Enterprise User
- Secure storage of private keys
  - Bootstrapping key pair (Immutable)
  - Network-Layer key pair
  - Cloud / Application key pairs
- Secure storage of Trust Anchors
  - Birth Certificate Authority (Immutable)
  - Secure Boot
  - Secure Firmware Update
  - Mutual Authentication
- Secure storage to enable trusted data
  - MUD URL
  - Ownership History
  - Other trusted data requirements
- Crypto coprocessor
  - Important for resource limited IoT Devices
- Secure Element can be part of the onboarding-chipset to make the IoT device “Onboarding-Ready”



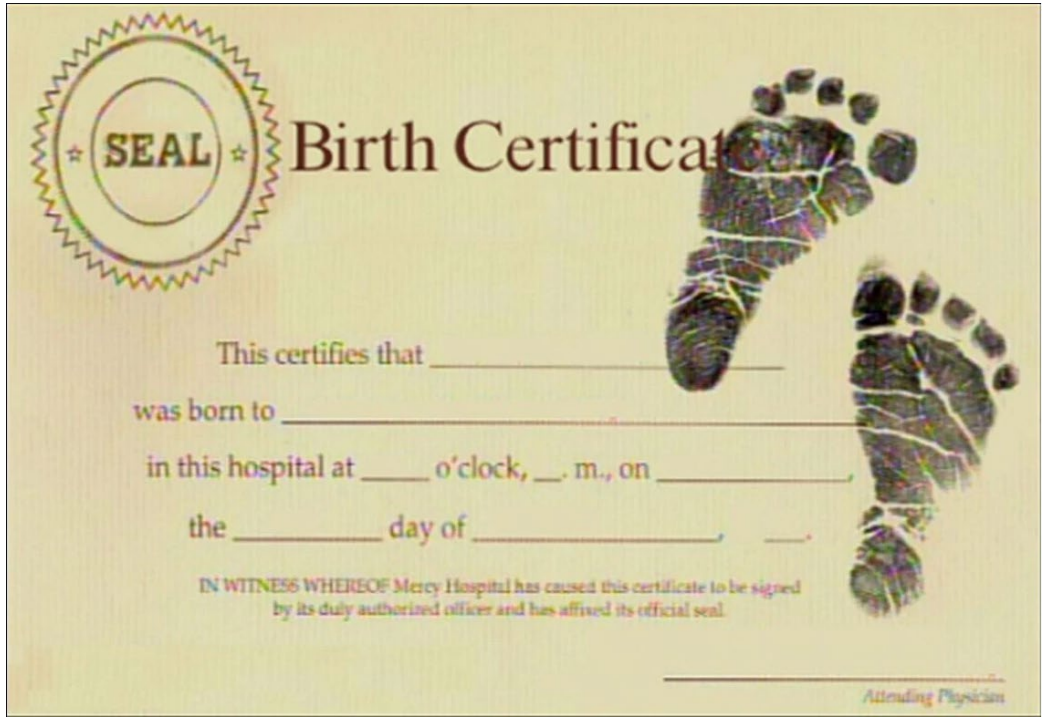
WISeKey

THE NEED FOR IMMUTABLE IDENTITIES

- Birth Certificate Analogy
  - Identifies name, location of birth, parents, time, certifying authority
  - Guarantee of validity (3rd Party Authority Signature and Seal Establishes Trust)
  - Becomes the basis for trust for all other permissions throughout the lifetime
  - Identity is immutable

- Trust is essential
  - IoT devices can be ***dangerous*** as soon as they are onboarded to a network.
  - Need trusted identity
  - AI and Blockchain data integrity

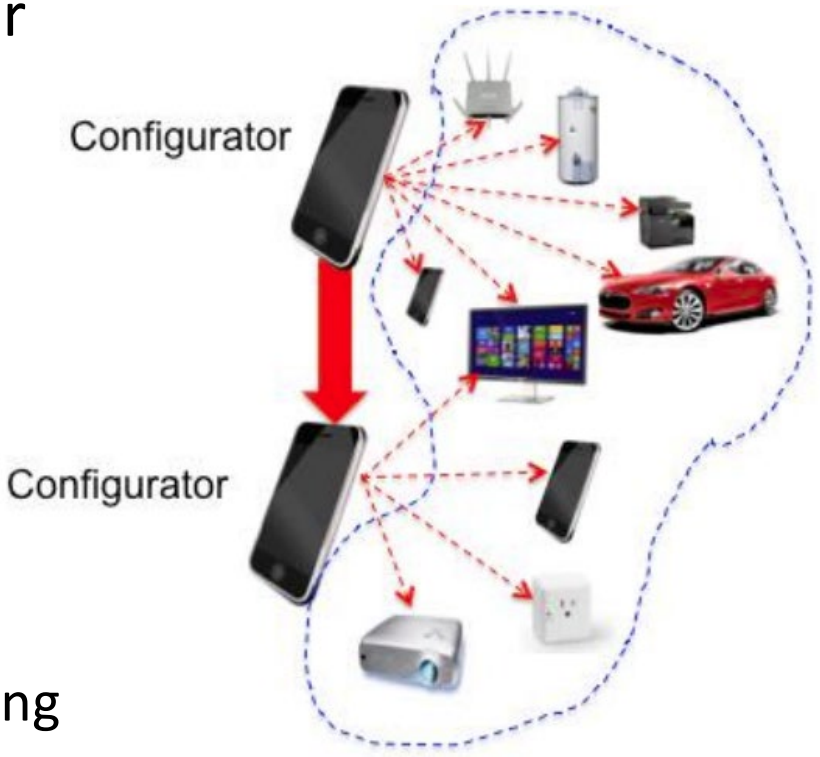
- Verification in 2 Steps:
  - Reason to trust Public Key
  - Verify possession of Private Key



WISeKey

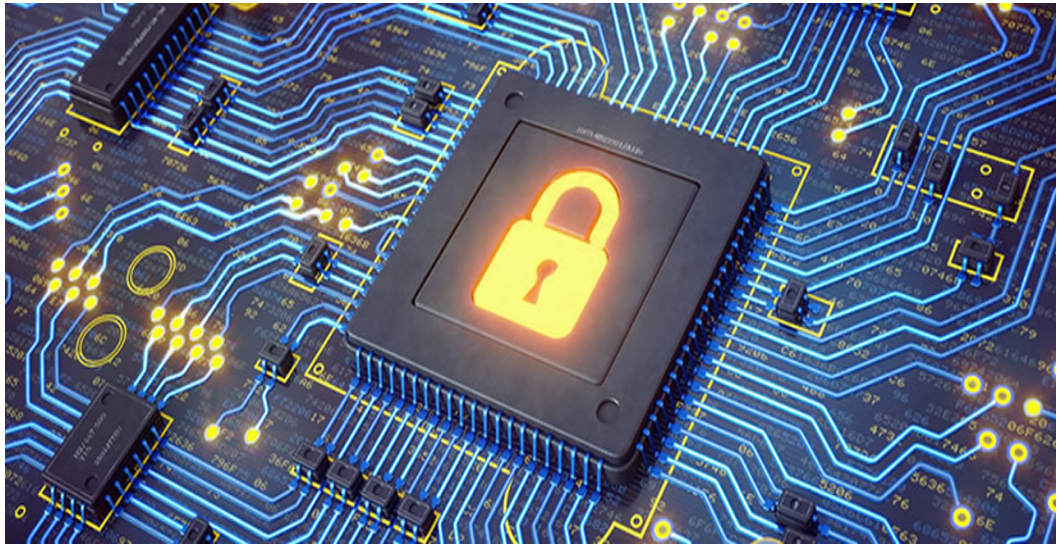
USE CASES

- DPP Onboarding and provisioning to network-layer
  - Use Bootstrapping Private Key
  - Establish trust with QR code or NFC
- Trusted storage for MUD URL
- Onboarding and provisioning to cloud & apps
  - Establish trusted connection for subsequent provisioning
- Transfer of Ownership / Decommissioning
  - Current owner can return factory state



DEVICE LEVEL SECURITY

- Secure Firmware Boot / Secure Firmware Update
  - Use manufacturer “Trust Anchor” to verify code at boot time
- Trusted Communication to Cloud and Applications
  - Mutually authenticated connections
- Trusted Data from IoT Device
  - Ensure data integrity with signature




THANK YOU