Security Foundation

BUILDING A SYSTEM OF TRUST: THE POWER OF DEVICE IDENTITIES

IOT SECURITY FOUNDATION WHITE PAPER

Prepared by

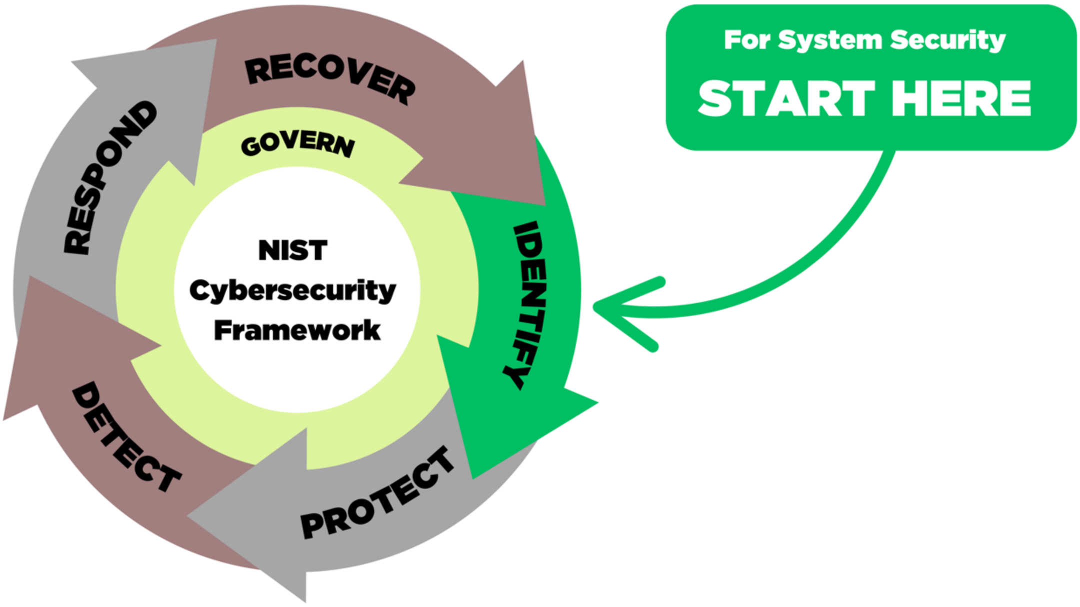
Michael Richardson, Tyler Gannon, Nick Allott, John Moor & Richard Seward

MAY 2025

Solving the IoT Security Puzzle

The Internet of Things (IoT) is transforming our world, linking devices like thermostats, industrial sensors, and connected vehicles into a vast, interdependent network. Yet, this connectivity comes with a catch: the system is only as secure as its weakest link. Many IoT devices—low-cost, always-on, and often overlooked—are prime targets for cyberattacks. With global regulations tightening and organisations like the IoT Security Foundation (IoTSF) leading the charge, the stakes are clear: IoT security is a significant challenge that demands robust solutions.

So, where do we begin? The answer lies in trust. Every device must reliably declare, “I am who I say I am,” and “I’m safe to connect.” Device identities—unique, hardware-rooted identifiers—provide this foundation, enabling a "chain of trust" that spans from silicon to cloud. This white paper explores why device identities are critical, presents a simple supply-chain model for their real-world application, and showcases how IoTSF members are strengthening this chain, yet recognising significant future potential that needs coordinated effort.



Why Device Identities REALLY Matter

Think of a device identity as a digital passport. Without it, a network can’t distinguish friend from foe. Ideally embedded in hardware at the point of manufacture, these identities allow devices to securely join systems, safeguard data, and block impostors. In a world of billions of interacting devices, they’re the essential ingredient of a secure, scalable IoT ecosystem.

Device identities deliver:

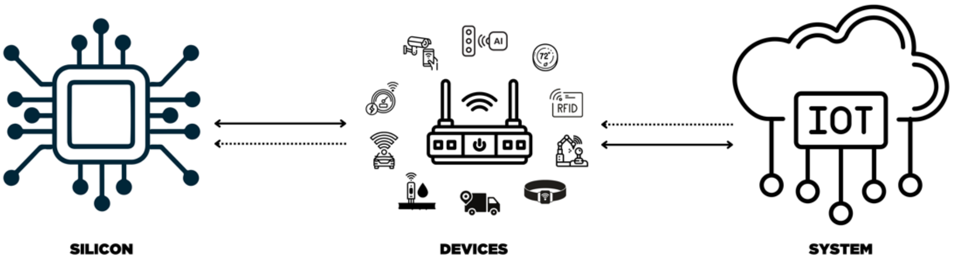
- **Authenticity**: Prove a device is genuine, not counterfeit.
- **Security**: Provide protection against unauthorized access from the ground up - a foundation for Zero Trust.
- **Interoperability**: Enable seamless, trusted connections across networks and applications.
- **Lifecycle**. Device identities can be revoked when the device has been decommissioned or resold.

In short, they’re the key to a dynamic digital future where IoT thrives safely.

Simplifying Trust: The Silicon-to-Systems Model

IoTSF’s "supply chain of trust" concept can be distilled into a practical "silicon-to-systems" model with three core stages:

1. **Silicon**: Device identities begin in a chip—a unique identifier forged at the factory.
2. **Device**: Manufacturers integrate these chips into products (e.g., smart meters, routers), tying identities to firmware and software.
3. **System**: Networks and applications leverage these identities to connect and operate devices securely (e.g., a smart grid).



DEVICE IDENTITY

This chain of trust hinges on each stage verifying the one before it. The device identity is the thread that binds them, ensuring security from creation to retirement. This silicon-to-systems model starts with raw device identities, but its potential extends further—supporting ownership, software, network roles, and more. These broader dimensions of identity are topics with significant opportunity for innovation and exploitation, building a comprehensive foundation for trust.

The Root of Trust (RoT)

At the heart of every device identity lies the Root of Trust (RoT). This "vault" locks away the identity and cryptographic keys, making them tamper-proof and unforgeable. The RoT is the anchor for trust, enabling:

- Verification that a device is authentic.
- Protection against attacks at the earliest stage.
- A foundation for security that scales to entire systems.

For example, a smart meter’s RoT ensures its identity can’t be spoofed, guaranteeing accurate billing and grid reliability.

The Chain of Trust in Action

Device identities turn trust into practice:

- **Uniqueness**: Every device carries its own immutable ID—no duplicates, no confusion.
- **Verification**: The RoT proves authenticity, blocking clones or fakes.
- **Secure Onboarding**: Networks validate IDs for safe integration e.g., using the Internet Engineering Task Force (IETF) BRSKI protocol, the Fast Identity Online (FIDO) IoT onboarding protocol, Open Platform Communications (OPC) Unified Architecture (OPC UA Part 21), Connectivity Standards Alliance (CSA) MATTER, Enrolment over Secure Transport (EST RFC7030), etc.
- **Ongoing Oversight**: Systems monitor behaviour and isolate threats e.g., via the Manufacturer Usage Description (MUD) framework.
- **Validation:** Devices can be validated to further issue operational credentials e.g. certificates owned and managed by the device operator.

Built on a foundation that endures, this chain adapts to new devices and evolving risks.

IoTSF Members: Powering the Model

IoTSF members exemplify the silicon-to-systems model, adding value at every stage:

- Silicon:
  - Microchip: Embeds unforgeable IDs in chips with a secure RoT.
  - Position: Trust starts here—hardware-level security for all.

- Device:
  - IAR/Secure Thingz: Provisions IDs into products (e.g., with Renesas MCUs), bridging silicon to firmware.
  - EPS Global: Programs IDs, preparing them for manufacturers.
  - Position: Transforming raw identities into scalable, device-ready security.

- System:
  - Device Authority: Manages IDs in live systems, extending device and data trust to applications.
  - Vodafone: Secures devices across its network using ID-based authentication.

    - Position: Ensuring systems stay trusted—IDs as the connective tissue.

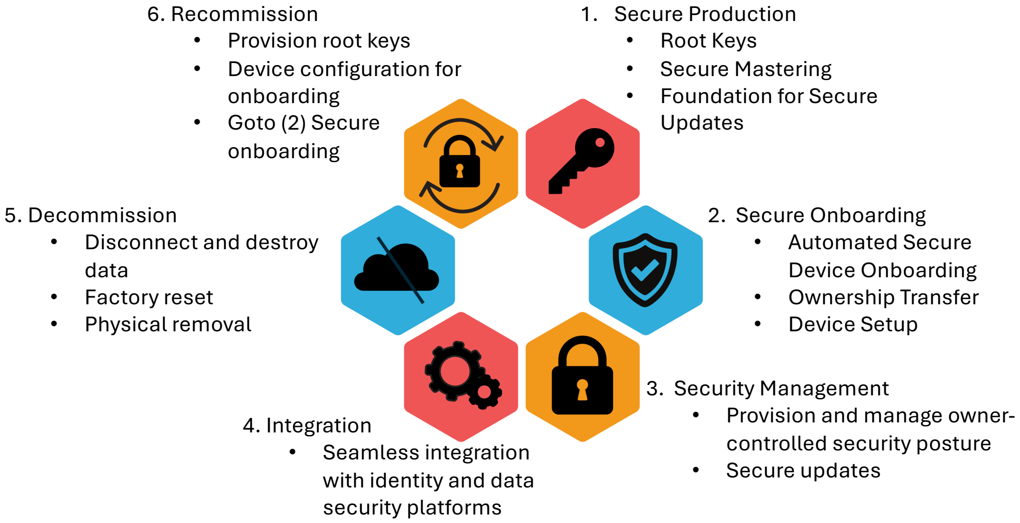
- Security Enhancement:
    - Quantum Dice: Bolsters IDs with quantum-random keys, future-proofing against emerging threats.
    - Position: Strengthening trust for the long haul.

Proving the model works - as exemplified above - the future supply chain must cooperate and collaborate in an end-to-end system of trust fully leveraging the power of device identities.

Your Role in the Chain

Wherever you fit—chip maker, device manufacturer, or network provider—device identities offer a chance to lead:

- **Silicon**: Forge the strongest foundation.
- **Device**: Provision security seamlessly.
- **System**: Deploy and maintain trust at scale.
- **Security**: Innovate for tomorrow.



1. Secure Production
    - Root Keys
    - Secure Mastering
    - Foundation for Secure Updates
2. Secure Onboarding
    - Automated Secure Device Onboarding
    - Ownership Transfer
    - Device Setup
3. Security Management
    - Provision and manage owner-controlled security posture
    - Secure updates
4. Integration
    - Seamless integration with identity and data security platforms
5. Decommission
    - Disconnect and destroy data
    - Factory reset
    - Physical removal
6. Recommission
    - Provision root keys
    - Device configuration for onboarding
    - Goto (2) Secure onboarding

This model is flexible, robust, and collaborative—a framework to secure IoT and position your organization as a leader.

Challenges Ahead

It's a great model and progress has been commendable, however, we're not done yet, and many hurdles remain:

- **Complexity:** Multiple technologies (e.g., certificates, MUD) can overwhelm stakeholders.
- **Legacy:** Significant investments exist in brownfield environments where devices have been created and deployed without strong identities, and new identities need to be applied.
- **Economic:** Many see unique identity per device as an avoidable expense, rather than an opportunity to grow more value and fortify systems.
- **Scale:** Managing billions of IDs demands streamlined processes.
- **Privacy:** Identities must protect users, not expose them.
- **Skills:** Available know-how and a global shortage of skilled personnel present an adoption barrier.

Addressing these requires vigilance and cooperation - you can benefit and help at the same time.

A Call to Action: Let's Build Together

A Foundation for the Future

IoT continues to grow at pace and weak security invites a plethora of problems for commerce, industry and infrastructure from botnets, data breaches, and critical failures. Device identities, rooted in silicon's RoT, are the foundation of IoT security. From chip to network, they establish trust, verify authenticity, and enable resilience.

IoTSF members show it's achievable and we're inviting you to join our effort to shine a light in this vital area of cybersecurity as we have done before. Help develop and deliver greater awareness, understanding and opportunity for a system of trust that truly lasts.

Join the IoTSF Device Identity Forum

IoTSF is launching a working group to advance this vision. Together, we will:

- **Raise Awareness**: Highlight why device IDs and RoTs are vital for trust.
- **Simplify**: Security doesn't have to be complicated. We will clarify the model (silicon, device, system) and tools (BRSKI, FIDO IoT, OPC UA, CSA MATTER, MUD) for all.
- **Collaborate**: Unite members and newcomers to innovate and solve challenges.
- **Develop best practices** for provisioning device identities, offering clear, industry-standard guidance for all stages of the supply chain.

Our Aim: Deliver security - utilise device identities as a basis of trust for a robust, future-ready IoT ecosystem.

How to Get Involved?

It’s simple - make contact, and we’ll take good care of you.

Email: contact@iotsecurityfoundation.org

Appendix

Examples Vendors in the Silicon to Systems Model	
Silicon	ARM, Codasip, Crypto Quantique, Infineon Technologies, Microchip, NXP, Rambus, SCI Semiconductor Ltd, Synaptics Inc., Tropic Square etc.,
Devices	Arcelik, Crane NXT, Honeywell, Huawei technologies, Kubu Smart Ltd, Radiomotive, IAR Systems/Secure Thingz, SPS Europe
Systems	Cisco, Device Authority, Enevo Group, Gridmerge Ltd, HomeLink Technologies Ltd, NquiringMinds, Thales, Tosibox, Vodafone
Security	Cetome, Keysight, MultOS Ltd, NquiringMinds, PQShield Ltd, Quantum Dice, Red Alert Labs,Skills DA, Xitex, Zaya

This white paper can be downloaded from https://tinyurl.com/IoTSF-Publications