Chip to Cloud Security for the Internet of Things (IoT)

Delivered by Device Authority KeyScaler and MULTOS Secure Chip Platform

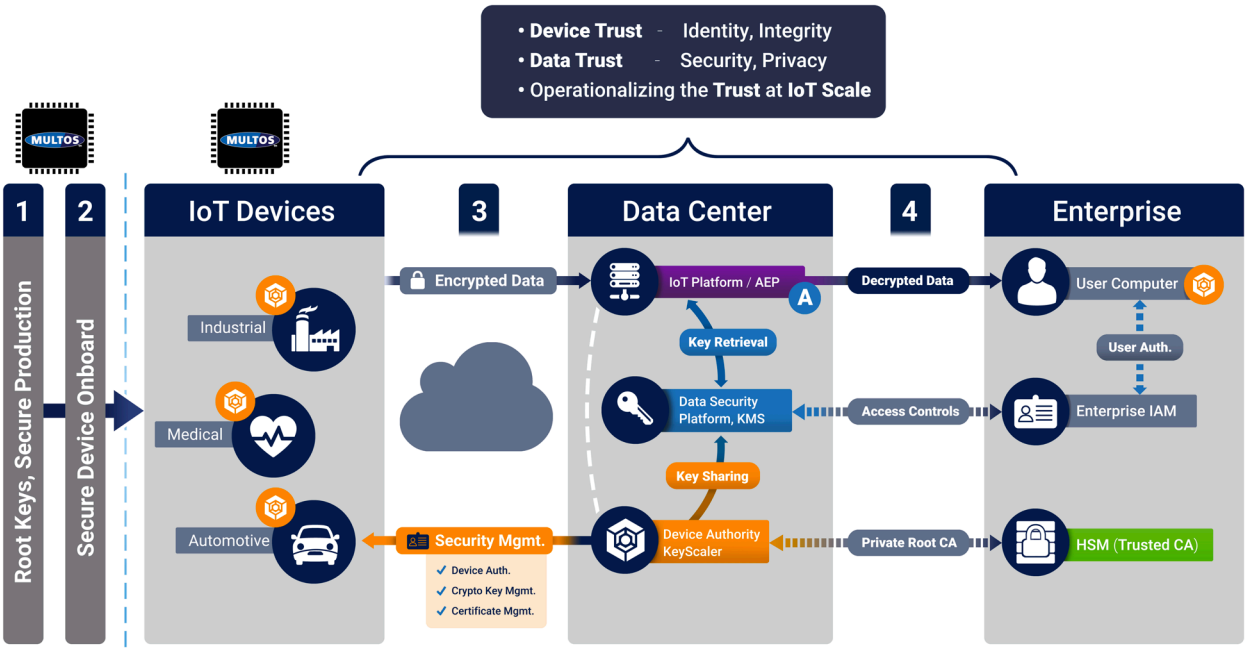
- Build in security and manage it from device to cloud
- Cost-effective, robust security for IoT devices
- Prevention of cyber attacks
- Meets compliance requirements for regulated industries
- Ease of use and deployment for customers

How do you build in and manage security from device to cloud?

Introduction

The Internet of Things presents a huge business opportunity across almost every industry. But to realize that opportunity, enterprise IoT security must become a primary focus. IoT brings new security challenges introduced by the scale and pace of adoption, as well as the physical consequences of compromised security. Until now, security has been treated as an afterthought; by adding layers of security after devices are delivered, with infrastructure and applications already in place. But security for the IoT is too important to be treated as an afterthought. IoT's unique characteristics are also forcing a fundamental rethink about how Enterprises need to implement security management for devices and data.

Device Authority's KeyScaler and MULTOS integrated solution delivers a Secure by Design approach focusing on key provisioning and key insertion for initial device trust, device provisioning and operationalizing trust and security operations into the Enterprise. With the initial key insertion being offered through the MULTOS manufacturer's process and partners.



The Enterprise IoT Security Blueprint above shows 4 steps which product manufacturers and service providers have to manage through the lifecycle of an IoT device or product to be able to automate and operationalize security at IoT scale into Enterprises. These steps include:

1. Provision Root Keys and Certificates at the Time of Manufacturing
2. Secure Device Onboard/Zero Touch Provisioning
3. Provision and Manage Owner-Controlled Security for the Devices
4. Enterprise Integration

Utilizing the MULTOS secure chip solution with KeyScaler enables an “out of the box” approach to IoT security, delivering security from the start of a project.

• Giving customers and product manufacturers flexibility for device security to solve the fundamental steps and challenges outlined above.

• Real use cases require an end to end approach for security to operationalize security at IoT Scale, to meet the demands of business and Enterprise integration, but at the same time meeting the security requirements set out by legislation, compliance and good security practice.

What is the solution and why does my organization need it?

The solution is an implementation of Device Authority’s KeyScaler client-side API for MULTOS high-security Trust Anchor chip solution. It enables organisations to adopt a Secure by Design approach and cost-effectively build IoT devices that meet the security requirements expected by industry and increasingly demanded by consumers. In the near future these security requirements will become mandatory as regulation catches up with the market. Devices connecting to the cloud and enterprise infrastructure employing this technology can be built, programmed, onboarded and managed at scale in a highly secure manner at every stage with a proven hardware root of trust at their core.

What functionality and benefits will it deliver for us?

The solution has the ability to generate all the JSON formatted secure messages an IoT endpoint needs to send to Device Authority's KeyScaler platform, process the replies and store keys and confidential data securely. All this is done within the secure environment provided by MULTOS.

The solution is used to:

1. Automate the secure registration and onboarding of devices without human intervention.

2. Obtain and maintain the credentials needed to authenticate the IoT endpoint device to IoT platforms and services such as KeyScaler itself, AWS IoT, Microsoft Azure IoT and PTC ThingWorx.

3. Obtain and maintain an encryption key used to encrypt data generated by the device.

4. Provide a Secure by Design approach for device manufacturers.

5. Enable chip to cloud security, leveraging Enterprise security technology such as HSMs.

6. Quarantine devices when necessary, revoking their credentials.

The solution can be used as a companion security microcontroller in an IoT endpoint device or as the main microcontroller (in which case it fulfils both the device control and security functions).

As well as supporting Device Authority, an IoT endpoint may make use of the MULTOS chip for other security features as MULTOS provides a safe multi-application environment.

What do I get when buying the solution?

The solution provides three programming APIs:

1. APDU (Application Protocol Data Units) commands that can be called through the serial, i2c or smartcard interfaces or by other applications running inside the MULTOS chip,

2. a 'C' API (example implementation available for Raspberry Pi, Arduino and MULTOS) and

3. a Python API (an example implementation for Raspberry Pi is available which can be built for Python 2 or Python 3)

Example drivers are also available for interfacing with Raspberry Pi and Arduino.

About Device Authority KeyScaler and MULTOS

MULTOS and Device Authority have partnered to provide a combined solution which enables organisations to adopt a Secure by Design approach and cost-effectively build IoT devices that meet the security requirements expected by industry, legislation and customers. In the near future these security requirements will become mandatory as regulation catches up with the market.

The combined value from Device Authority and MULTOS offers a Chip to Cloud solution and brings together a rich set of features and benefits to solve real problems for IoT applications and product manufacturers, including:

- Secure by design approach for chip to cloud security
- Secure MCU With Secure boot, secure key management, trusted firmware execution
    - Proven technology, shipped in over 1 Billion products
- Automated secure registration and onboarding of devices without human intervention
- Automate security into various IoT platforms with “out of the box” connectors, including:
    - Microsoft Azure IoT Hub, PTC ThingWorx and AWS IoT
- Flexible architecture to enable custom integration using extensible Enhanced Platform Integration Connector (EPIC)
- Obtain and maintain the credentials needed to authenticate the IoT endpoint device to IoT platforms and services such as KeyScaler itself, Amazon AWS IoT, Microsoft Azure IoT and PTC ThingWorx
- Provide flexibility for IoT Platform choice and Security operations integration
- Obtain and maintain an encryption key used to encrypt data generated by the device
- Enable chip to cloud security, leveraging Enterprise security technology such as HSMs
- Quarantine devices when necessary, revoking their credentials

For more information or to find out how you can get started using Device Authority and MULTOS’ Chip to Cloud solution, please contact robert.dobson@deviceauthority.com or chris.torr@multos.com

About Device Authority

Device Authority is a global leader in Identity and Access Management (IAM) for the Internet of Things (IoT); focused on medical / healthcare, industrial and smart connected devices. Our KeyScaler™ platform provides trust for IoT devices and the IoT ecosystem, to address the challenges of securing the Internet of Things. KeyScaler uses breakthrough technology including Dynamic Device Key Generation (DDKG) and PKI Signature+ that delivers unrivalled simplicity and trust to IoT devices. This solution delivers automated device provisioning, authentication, credential management and policy based end-to-end data security/encryption. With offices in Fremont, California and Reading, UK, Device Authority partners with the leading IoT ecosystem providers, including AWS, DigiCert, Gemalto, HID Global, Microsoft, nCipher Security, PTC, Sectigo, Thales, Wipro and more. Keep updated by visiting www.deviceauthority.com, following @DeviceAuthority and subscribing to our BrightTALK channel.

About MULTOS

MULTOS has been at the heart of secure devices for 20 years, and over 1 billion secure MULTOS tokens have been shipped. Based on Public Key Infrastructure (PKI) it is industry renowned and has obtained the highest band of security approval, the Common Criteria EAL7 certification. Solution and service providers can leverage MULTOS Trust Anchors, comprising embedded tamper-proof integrated circuits with the loaded MULTOS Operating System, which provides an ultra-secure execution environment, protecting the device from malware and other digital attacks. Critical data transmission can also be secured to and from the device using application based encryption. As well as providing traditional smart-card interfaces (including NFC support), MULTOS Trust Anchors have GPIO, i2c, SPI and software serial support. The device can therefore be used in the place of equivalent-performance traditional microcontrollers or can be easily integrated into larger designs as an on-board Hardware Security Module (HSM). General information about MULTOS can be found at www.multos.com and details of the Trust Anchor development kit can be found at www.multos.com/trust_anchor