9 Core Capabilities For Zero Trust in IoT

DEVICE AUTHORITY™

Automating Zero Trust for IoT

> 83% of organizations have improved their efficiency by introducing IoT technology. *

*dataprot.net

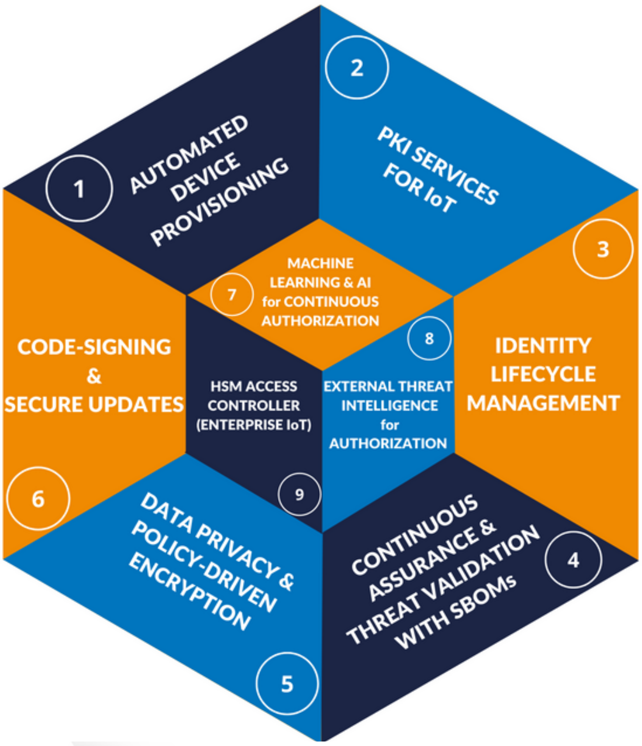
But are those devices secure...?

DEVICE AUTHORITY™
Automating Zero Trust for IoT

DEVICE AUTHORITY™
Automating Zero Trust for IoT

9 Core Capabilities For Zero Trust in IoT

Device Authority's KeyScaler platform delivers the **Nine Core Capabilities essential for the automation of Zero Trust for IoT**. Device Authority KeyScaler, and KeyScaler Edge, provide patented Dynamic Device Key Generation (DDKG) technology for establishing device to KeyScaler trust to uniquely deliver the following:


1
AUTOMATED DEVICE PROVISIONING
2
PKI SERVICES FOR IoT
3
IDENTITY LIFECYCLE MANAGEMENT
4
CONTINUOUS ASSURANCE & THREAT VALIDATION WITH SBOMs
5
DATA PRIVACY & POLICY-DRIVEN ENCRYPTION
6
CODE-SIGNING & SECURE UPDATES
7
MACHINE LEARNING & AI for CONTINUOUS AUTHORIZATION
8
EXTERNAL THREAT INTELLIGENCE for AUTHORIZATION
9
HSM ACCESS CONTROLLER (ENTERPRISE IoT)

1. Automated Device Provisioning

The initial onboarding and provisioning of IoT devices must be secured and controlled to protect the integrity of the IoT applications to which they connect, and the data that they are processing. If left unsecured, the chances of a Threat Actor entering the network through compromised device credentials is greatly increased and can result in significant financial loss, brand impact, or physical damage.

2. PKI Services for IoT

Automated Public Key Infrastructure (PKI) is the foundation for IoT Security. PKI is a set of proven technologies that have solved identity, authentication integrity, and privacy challenges for the Internet and Cloud for many years. Standards-based PKI certificates, or alternatively tokens, provide trust for devices, data, and connections between machines. However, for most IoT deployments, certificates alone cannot address the multiple levels of authorization, role-based policies, and complex, sensitive information flow across platforms, including from the Internet's Edge. Automated PKI services designed specifically for devices are essential and are the only option available to deliver device and data trust required for IoT.

3. Identity Lifecycle Management

Managing PKI for enterprise services is already a challenging and time-consuming operation. For IoT deployments, the complexities are even greater: the scale and context of most IoT deployments make managing a device's identity throughout its entire lifecycle impossible to accomplish through manual methods. During the effective lifetime of a device, failure to store and protect encryption keys and certificates properly could result in unintended parties gaining access to your network. Further, many IoT devices operate at the Internet's Edge without consistent access to network-connected resources normally utilized for managing identities.

4. Continuous Assurance and Threat Validation with SBOMs

White House Executive Order 14028B introduced in 2021 was aimed at strengthening the nation's cybersecurity and introduced a Software Bill of Materials ('SBOM') requirement. Alongside this, the EU Cyber Resilience Act (in proposal phase) has also called for SBOM vulnerability management and remediation. As a result, organizations need a more proactive approach to ensure their devices and accompanying software are compliant and validated throughout the entire device lifecycle, confirming they are Trustworthy & Authorized.

27 Billion *

It is estimated that there will be around 27 billion IoT devices by 2025

39 Seconds **

There is a hacking attack every 39 seconds

75% Poor Identity Management ***

75% of security failures will result from inadequate management of identities

5. Data Privacy and Policy-Driven Encryption

HIPAA and GDPR are two examples of data privacy regulations that affect IoT deployments. Sensitive data residing unencrypted on devices is a frequent target of cyberattacks and merely encrypting data as it is transmitted to the cloud does not provide enough protection. The scale and complexity of IoT require automation to enforce privacy policy and encrypt protected data while at rest, in transit, and in use. Further, managing which applications and users have access to that data through Privileged Access Management capabilities has become an important part of an overall security strategy. The ability to quickly check policy and accurately apply it to different devices and services at scale is critical.

6. Code-Signing and Secure Updates

Unauthorized software and firmware updates are a major threat vector for IoT cyber-attacks. IoT breaches can have physical consequences that result in loss and can also introduce substantial legal liability and erode brand reputation.

There are three critical security requirements for delivering updates securely to IoT devices:

1. Securing access to the updates
2. Verifying the source of the updates
3. Verifying the integrity of the updates

*IDC, IoT Analytics
**University of Maryland
***Gartner

7. HSM Access Controller

When deploying and integrating a Hardware Security Module (HSM), there are three main security points to consider:

1. Authentication – How do I trust the client making the request to use a key?
2. Authorization – Is the requestor allowed to use this key for this HSM function?
3. Network Security – Is my HSM in a secure location in my network?

8. External Threat Intelligence for Authorization

The NIST (National Institute of Standards and Technology) Cybersecurity Framework includes 5 stages:
Identify – Protect – Detect – Respond – Recover

Threat detection platforms such as Microsoft Defender for IoT provide Detect and Respond capabilities by continuously monitoring devices on the network and capturing rich information, highlighting anomalous behaviors, out-of-date firmware, known vulnerabilities and more. This threat intelligence data can be used to produce risk scores that should be considered when authenticating an IoT device.

KeyScaler's Authorization Service Connector allows for real-time querying of these external threat intelligence platforms and applying known CVE's, threat scores, and other data to a device's authentication and authorization process. Based on the device's risk score, changes can be made to the device authorization such as limiting the length of an authentication session, restricting authorization functions, or even blocking authentication altogether by denying or revoking certificates.

9. Machine Learning and AI for Continuous Authorization

Machine Learning and Artificial Intelligence technologies have fundamentally changed what's possible for IoT security. Machine Learning can leverage the power of large datasets created during the continuous authorization process to learn from observed behaviors and feed those learnings to an Artificial Intelligence engine with the ability to predict future adverse events at any point during the device's identity lifecycle. Based on the AI output, actions such as enforcing a device check-in, updating a device's firmware, or revoking credentials can be automated to proactively prevent compromise.