SOLUTION BRIEF

Intel IoT Technology
Security Automation

Managing the Internet of Things (IoT) Device Authentication Life Cycle

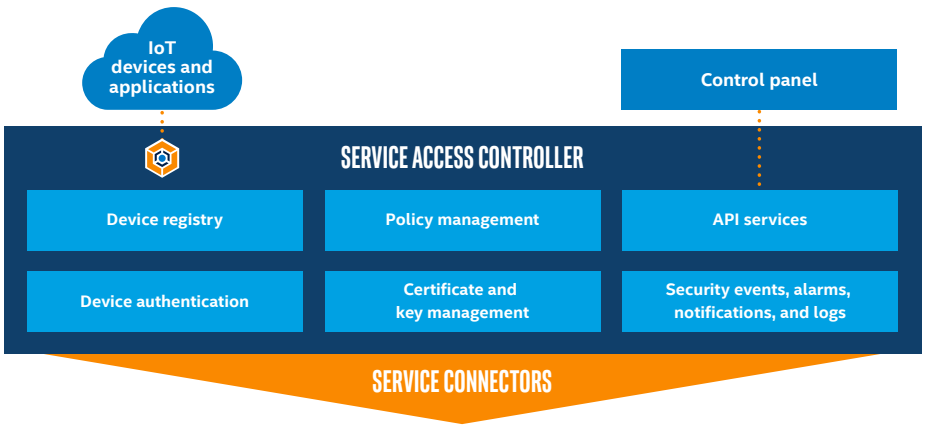
IoT devices require secure onboarding and security provisioning tied to hardware roots of trust

Intelligent Intel® IoT Gateway Technologies perform critical functions within many IoT environments, providing a natural bridge between operational technology (OT) and information technology (IT) systems. IoT promises countless efficiencies, increased competitiveness, improved customer service, and even brand-new market opportunities—and Intel® IoT technology-based solutions play a key role in turning the potential of IoT into reality.

However, deploying strong security is hard and always has been. Deploying strong IoT security is even harder. According to Gartner, by 2020, around 25 percent of all identified security breaches will involve IoT. New security challenges have been introduced in IoT applications due to the scale and pace of adoption, as well as the physical consequences of compromised IoT security. These challenges cannot be effectively addressed by traditional IT security solutions.

To address this, Device Authority has introduced a new paradigm of IoT security automation that accelerates and simplifies the deployment of strong IoT security. We help our partners and customers simplify the process of establishing a robust, end-to-end security architecture within the IoT and deliver efficiencies at scale through security automation that integrates and interoperates with Intel®-based IoT gateways, Intel onboarding solutions, and core hardware root of trust security technologies in silicon.

Device Authority delivers an operational security framework to manage the identity and authentication life cycle for a device. It integrates with Intel-based IoT gateways and device onboarding services at activation and brokers credential updates from third-party platform providers. Device Authority delivers the security control plane that can be integrated with IoT operational systems and cloud-based analytics providers to secure all IoT device data flows.



The Device Authority KeyScaler™ IoT Security Automation platform provides active device authentication and policy enforcement to deliver four mission-critical IoT security solutions: device provisioning, credential management, secure updates, and end-to-end data protection.

Device onboarding and security provisioning

Today, a manual process exists where devices are activated in the field, configured on the network with IT, and registered with the device owner in an IoT management platform. This time-intensive process is fraught with security holes, as exemplified by recent large-scale attacks in which device manufacturers have shipped default credentials that were co-opted for botnet-style DNS attacks.

Device Authority supports the Intel® Secure Device Onboard model through which "headless" devices can be powered on to locate and automatically onboard to IoT management platforms. Intel delivers the open software, onboarding protocols, and ecosystem enablement solutions that are based on Intel® Enhanced Privacy ID (Intel® EPID), a privacy-preserving authentication scheme. Leveraging the zero-touch model from Intel, Device Authority will receive the anonymous, attested device identity and IoT platform registration. Device Authority will then manage the overlay and other security provisioning tasks such as swapping in a PKI credential, default passwords, or delivering a secure software update to the device.

The security provisioning life cycle involves Device Authority's patented, dynamic device key generation process that builds on the attested secure hardware baseline established via Intel at activation time. Device Authority regenerates unique encryption keys for each communication session. This forms a continuous hardware-enforced security model that spans the device life cycle, from activation to operation.

Secure credential management

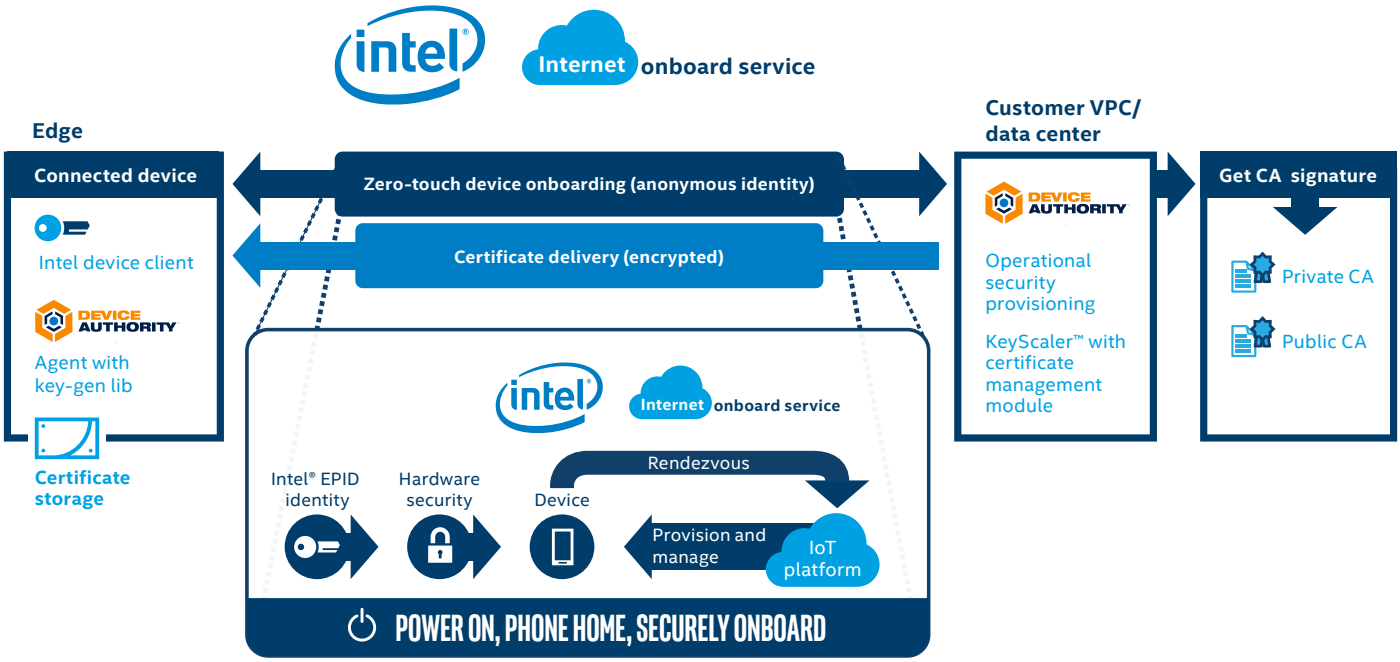
Managed PKI services from companies like DigiCert have revolutionized the cost and complexity of digital certificate infrastructure. Many of these services now include support for smaller, lightweight, IoT-style certificates to help deliver stronger security to a wider range of devices. In order to take full advantage of these services while addressing the challenges of deploying and managing PKI at IoT scale, Device Authority's Secure Credential Management* solution directly integrates with DigiCert to securely automate certificate provisioning, revocation, and renewal processes. It supports private PKI, so customers can generate their own internal private root certificate authority and key to enable provisioning of self-signed certificates to devices. Most importantly, the solution creates a direct, authenticated, policy-enforced binding between devices and the credentials that are assigned to them. This prevents the use of certificates and keys from unauthorized devices. Another important feature is the automated authentication and crypto key rotation for stronger security achieved through frequent key rotation.

Automated password management

Cybercriminals and attackers are increasingly exploiting weaknesses in IoT device identities. Manufacturer-set default passwords that remain unchanged are proving to be responsible for the recent Mirai and BrickerBot attacks.

Device Authority KeyScaler™ has unique automated password management (APM) technology at its heart and effectively removes the associated human risk of manually updating credentials at scale.

The APM element automatically sets and manages local account passwords from manufacturer default on devices. Password rotation policies are enforced, which dramatically reduces the attack surface of using static passwords.



Policy-driven encryption

Data-transfer mechanisms utilizing transport-based security protocols have been substantially compromised and do not guarantee end-to-end data security. IoT data requires advanced, policy-driven, end-to-end security to protect data—in motion and at rest—as it moves between devices and applications.

Device Authority's policy-driven encryption solution utilizes our patented dynamic key generation, device-derived key technology, and crypto-policy agents to provide "drop-in," application-level crypto that is configurable for specific data payloads and transmissions. Dynamic keys ensure that each data payload can be encrypted with one-time-use keys that are not shared or stored. Individual data elements can also be encrypted for specific recipients, independently from data transport protocol security. Using Device Authority's "set and deploy" policies to determine precisely what data needs to be encrypted, our smart agent technology takes care of processing and encrypting the vast quantities of data generated at the device or network edge. This ensures regulatory compliance and the mitigation of risk and data loss.

Target audience

With device provisioning, a reliable, policy-enforced trust anchor is required to establish a trusted security baseline and end-to-end protection for IoT applications that are being protected with an IoT gateway edge control point.

Utilizing Intel IoT Gateway Technology, Device Authority delivers this critical trust anchor to:

- Enable organizations to focus on delivering core business value without the distractions, learning curves, and technical expertise required for in-house security development and maintenance
- Provide automation and scalability that are unattainable with manually intensive security deployments
- Effectively manage IoT application risk and compliance while increasing brand protection

Industry verticals

Key industry verticals require advanced security solutions to mitigate risk and reduce the threat-surface exposure of mission-critical IoT applications. These verticals can be broadly identified as:

1. Those regulated by privacy legislation, such as healthcare, financial services, or even automotive (consider pay-as-you-drive insurance, for example)
2. Those driven by competitive pressure to protect intellectual property or control processes such as industrial, manufacturing, or engineering design
3. Critical infrastructure projects where a cyberbreach would have significant socioeconomic impact on entire cities or countries, such as smart utility grids, smart cities, and connected transportation
4. IoT platform providers and PaaS and IaaS providers who must be trusted to provide access and data security for their enterprise customers

The IoT security imperative

The competitive benefits of IoT will go to the organizations that can most rapidly achieve and support IoT enablement, while ensuring that what they have enabled is secure and protected. Intel IoT Gateway Technology, together with Device Authority, provide a critical foundation for competitive IoT enablement.

Learn more

For more information about the Device Authority KeyScaler platform, visit **deviceauthority.com**.

To enable your IoT solution for the Intel Secure Device Onboard model, email **iotonboarding@intel.com** to get enablement tools for the pilot program.

Intel and the Intel logo are trademarks of Intel Corporation or its subsidiaries in the U.S. and/or other countries.
*Other names and brands may be claimed as the property of others.
© Intel Corporation
KeyScaler™ is a trademark of Device Authority Ltd.
0917/DW/CMD/PDF ♻ Please recycle 334934-003US