insight.tech
POWERING IoT AND EMBEDDED INNOVATION

"Zero Touch" IoT Security Is Key to Continued Growth

John Blyler

By now it's clear that the IoT will miss the much-touted target of 50B connected devices by 2020. The problem? Security.

IT managers are so worried about security issues that they are requiring manual provisioning of IoT devices. This is leading to a slowdown in installation that cuts into revenues for OEMs, ODMs, and cloud platform providers.

The solution lies in IoT Identity Access Management (IAM). IoT IAM has become so important that MarketsandMarkets predicts the market will grow from $1.1B in 2016 to $4.97B by 2021.

In this article, we will explore:

- How IoT device deployments differ from IT approaches
- Why slow device provisioning decreases revenue
- How a new "Zero Touch" onboarding platform satisfies IT while meeting IoT requirements

Scalability or Security

Early IoT devices relied on self-discovery when installed on a network. This approach was easy for installers but gave IT departments headaches. No IT professional likes to see unsecured devices appear on the network without warning.

IT departments responded by forcing operations departments to secure each device before bringing it online. This improved security of the devices but put the brakes on rapid deployment of IoT systems.

To ensure each IoT device was secure, IT departments have explored a number of solutions—all with serious drawbacks. One option was to stage all IoT devices with uniform images, so that all devices used a known configuration. While this solution works great for generic PCs, it doesn't work well for the highly diverse world of IoT devices.

The second approach was to have the operations person contact IT for a unique key for each IoT device. This manual provisioning was extremely error-prone and time-consuming—often taking an hour per device **(Figure 1)**.

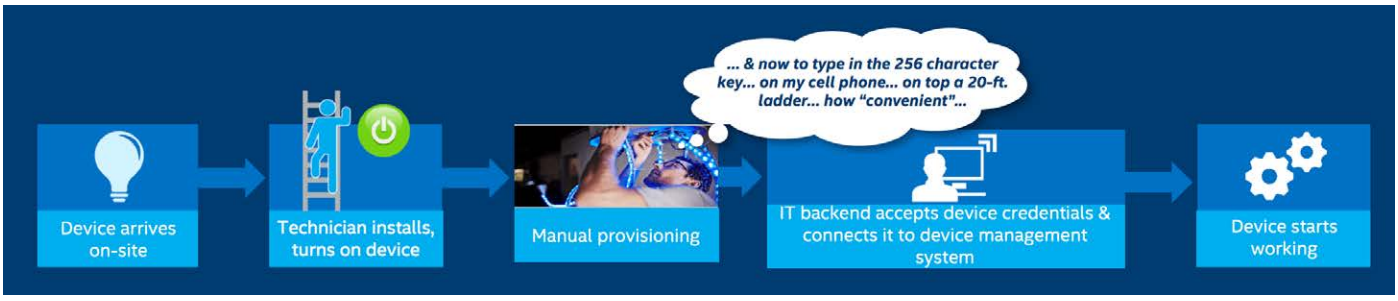

Figure 1. Manual provisioning of IoT gateway devices.

The third solution was to encourage IoT device OEMs and ODMs to pre-configure their IoT devices for specific cloud platform providers. This way, the provisioning burden could be outsourced to cloud providers.

The problem is that there are many cloud providers, including Amazon, Microsoft, IBM, and Honeywell, to name a few. Thus, this approach placed a heavy burden on OEMs/ODMs, which now had to validate, document, and track a unique SKU for each cloud platform.

Motivations: Lost Revenue and Data Protection

Slow rollout of IoT devices means lost revenue for the entire IoT ecosystem.

That includes cloud platform providers. "If the IoT devices aren't getting onboarded, then their monetization is suffering," explains Jen Gilburg, senior director of IoT security at Intel's Internet of Things Group (IoTG). "[That's true] regardless of whether the platform providers monetize on the volume of data or the number of devices under their management."

For OEMs and ODMs, the problem is unpredictable sales. Gilburg illustrates the point with a typical scenario: Suppose a customer requests 100,000 devices. The OEM/ODM gears up for production, but after the first 5,000 devices are delivered, the remainder of the order is delayed due to the slowdown imposed by security concerns. This can throw production schedules into chaos.

Ecosystem-based Solution

Since the original problem was that the IoT deployment model was different from IT models, it makes sense that a new solution is needed—one that combines greater scalability with automated security.

Enter Intel® Secure Device Onboard (Intel® SDO). This onboarding service is designed for rapid, platform-neutral provisioning, and offers:

- Zero-touch onboarding with automatic discovery and provisioning
- Only seconds to run at power-on
- Password-free authentication with Intel® Enhanced Privacy ID (Intel® EPID)
- Ability to support multiple cloud platforms with a single SKU
- Digital ownership traceability from manufacturer to customer

With this new platform, OEMs and ODMs need create only a single image for their devices. Then the device will become fully provisioned on initial power-up by the installer and ready for handoff to a back-end platform provider for operation **(Figure 2)**.

Here's how the platform works:

- **Silicon Provider**—Embeds an Intel EPID identity in the silicon's trusted execution environment (TEE) at manufacturing, using an Intel EPID 2.0 open source SDK.
- **Gateway/Device Manufacturer**—Uses a toolkit to insert client software into boot code to support a direct anonymous attestation communication channel to the IoT platform, which passes the device GUID, Intel SDO service URL, and digital ownership credential.
- **Device Owner**—After the distribution change of ownership, the final owner can automatically load its digital ownership receipt into the IoT Platform.
- **IoT Platform**—Uses an API to enable the platform or VM marketplace containers to register the device to the owner's account and enable rendezvous protocols that share the destination IP address.
- **Device Activation**—The powered-on device contacts the Intel SDO service to prove authenticity, and it receives the URL where it meets the new owner for provisioning.

To create the platform, Intel worked with numerous silicon, equipment, and platform providers **(Figure 3)**. The first equipment to support the platform is expected to come from members of the Intel® Internet of Things Solutions Alliance such as Nexcom.

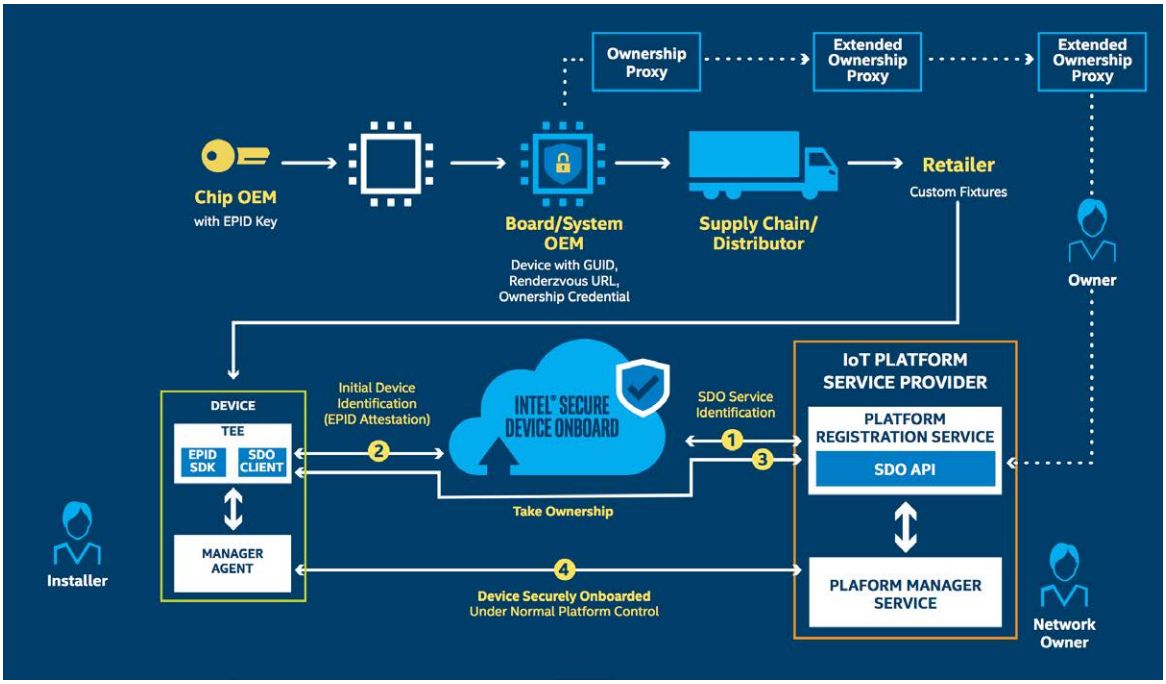

Figure 2. Intel® Secure Device Onboard (Intel® SDO) streamlines provisioning.

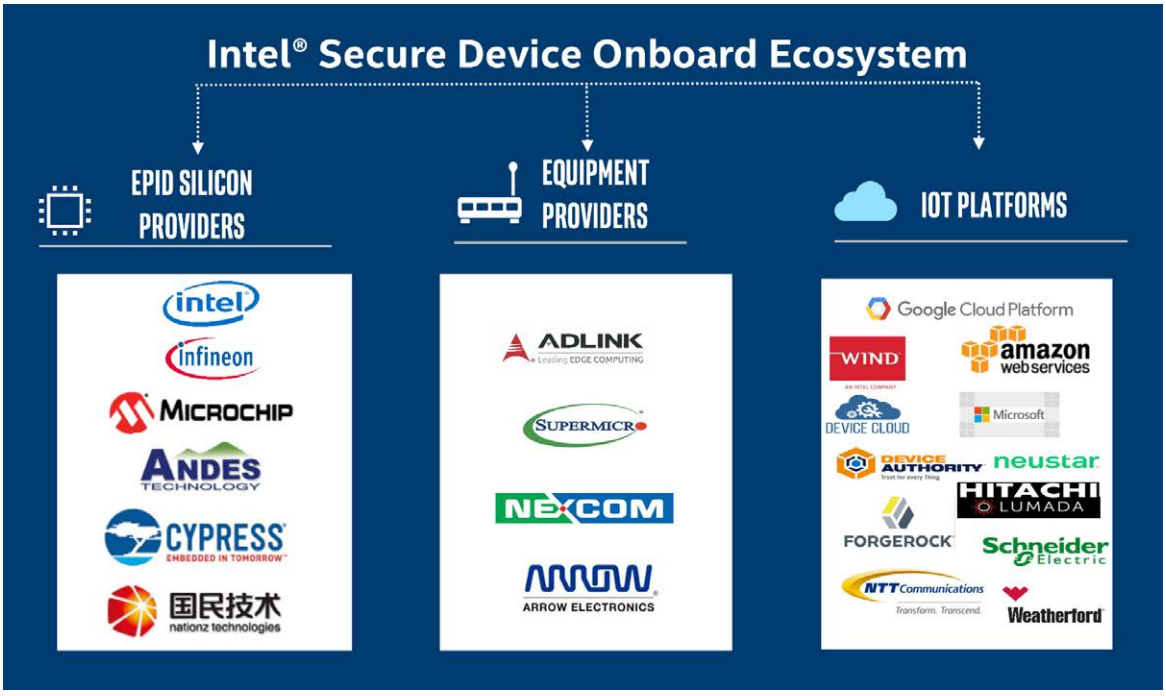

Figure 3. Ecosystem support is essential for a comprehensive IoT device onboarding system.

Further, Intel is working with the Open Connectivity Foundation (OCF), the IoTivity project, and other IoT standards organizations to contribute concepts and toolkits based on their real-world experiences with onboarding devices.

In addition to security, the global ecosystem-based approach must also adhere to privacy concerns. For anyone dealing with the European Union, this means adhering to the upcoming General Data Protection Regulation (GDPR). This regulation requires that any company collecting any type of data must ensure its protection and security.

That's one reason Intel SDO uses Intel EPID. This authentication method allows devices to access a system based on their approved level of access and not any identity information like a MACID. In other words, if 100 authentic signatures are verified, the verifier would not be able to determine whether 100 devices were authenticated, or if the same device was authenticated 100 times.

Traditional digital certification and authentication techniques like public key infrastructure (PKI) cannot remain anonymous while granting access **(Figure 4)**. A given public certificate contains the key owner's name and information, thus making the ownership of the secured information known. If the same device is verified multiple times, its activity could be tracked, which would allow hackers to create a threat map from which denial-of-service attacks could be launched—among other things.

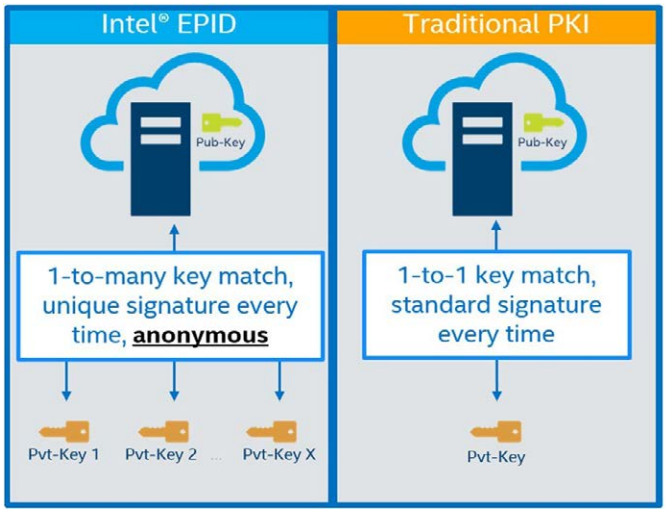

Figure 4. Unlike traditional PKI, Intel® Enhanced Privacy ID (Intel® EPID) is anonymous.

Intel EPID, on the other hand, collects no such identity data. Aside from dissuading hackers, the lack of identity data means Intel EPID is not affected by the GDPR initiative.

"As the industry moves to address the privacy of data with regulations like the GDPR, Intel EPID will gain a lot of additional use cases," says Gilburg. "It will then become more of an industry standard beyond just Intel and our partners."

From Fab to End Product Provisioning

To see how this all fits together, consider the scenario illustrated in **Figure 5**. The Intel EPID identity is burned into the trusted execution environment during chip fabrication.

The chips then go to the OEM/ODM, which stores a unique identifier known as a GUID and a public key in its board. The public key contains the chain of signatures that establishes device ownership.

Once the board is built into a product (say, a smart light bulb with GUID 123), it ships through various channels, eventually reaching the end customer. At each step, the signature chain grows.

Finally, the IoT device is installed. At this point, Intel SDO provides a broker service—really just a rendezvous point that is typically a URL, where the device can discover the owner's IP address. At this point, both the device and the owner prove themselves to each other.

"Intel isn't actually authenticating trust in the cloud," explains Gilburg. "Instead, we are simply rerouting devices to their intended new owner, where authentication will occur via the original Intel EPID signature. Once both agree, then an encrypted secure tunnel can be established between the device and the platform from which operational provisioning can occur."

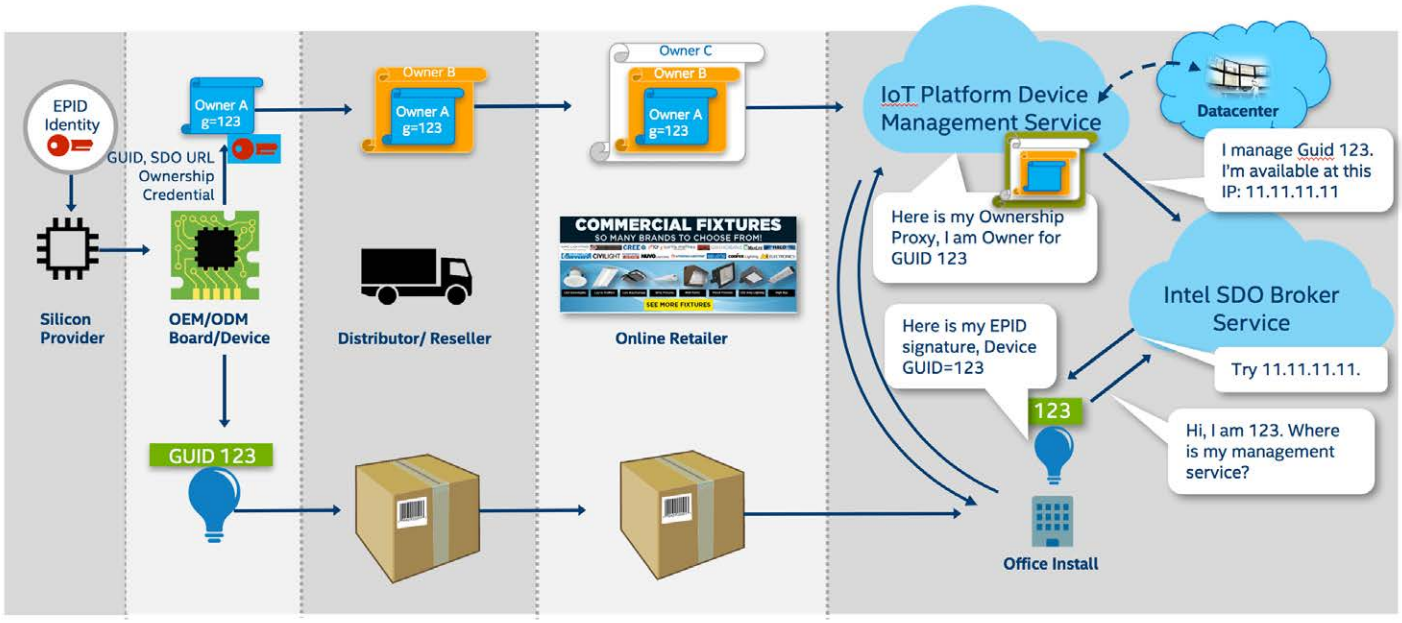

Figure 5. A smart light bulb illustrates a typical scenario.

Provisioning is an important step that balances the security with the constraints of the device. For example, if the device is an embedded system with an RTOS, then the IoT platform management system might use a simple RSA key.

If the device is a full gateway with greater memory and processing power, then a more secure image of the gateway can be used. Whatever is needed for that device to be operational, the platform management service makes that determination.

Scalable Security

This "zero touch" onboarding concept allows installers to simply plug in the device and verify its location. From there, network administrators can then take control of the device.

Authentication and security are established by a cloud-based proxy service connected to one of many IoT cloud-based platform providers. Once securely connected, the device is automatically provisioned by the user's account in the cloud service—users don't need to configure passwords, keys, or unique identifiers.

This last point is an important differentiator for Intel's approach, as it ensures privacy of the device. Potential hackers cannot create an attack map by tracing devices from owner to owner. Intel EPID technology establishes an anonymous secure channel where endpoint authentication is hidden, unlike traditional public key methods (like PKI) where ownership is traceable.

In short, Intel's approach to onboarding of IoT devices is both secure and easily scalable to the quick deployment of millions upon millions of devices.