SOLUTION BRIEF

Service Providers
Internet of Things

‘Zero-touch’ IoT Onboarding

Intel® Secure Device Onboard enables Communication Service Providers to more securely scale the Internet of Things to millions of devices, supporting the delivery of differentiated IoT-based services

Author

Steven Graham, Solution Architect, Intel Group

Executive Summary

Communication service providers (CSPs) must find new revenue streams to maintain and grow their share of the market. One way they can do this is by offering differentiated, end-to-end services for the burgeoning Internet of Things (IoT). Secure, scalable services for IoT device provisioning offer particular promise.

Current methods for onboarding IoT devices are costly, time-consuming and do not scale easily. Security is also a concern as key data about each device can be exposed during the authentication process.

Intel® Secure Device Onboard (Intel® SDO) offers CSPs a ‘zero touch’ approach designed to keep up with forecasted demand for IoT devices, while keeping deployment costs to a minimum and providing a simple out-of-box experience for the customer. Direct, remote attestation built into the hardware anonymously authenticates each IoT device and opens a private encrypted channel to the IoT platform, improving security.

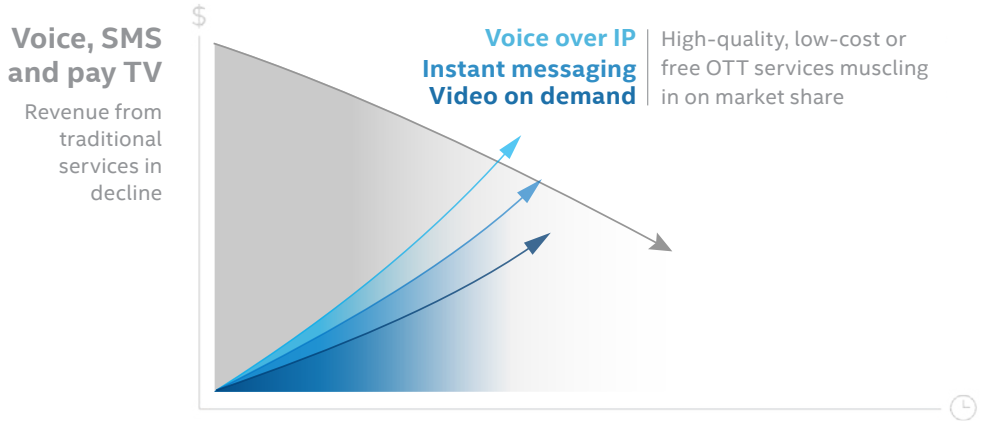

Figure 1. Traditional CSPs revenues are in decline, while providers of OTT services move in on market share.

Solution Benefits

- Faster IoT provisioning. Intel® Secure Device Onboard reduces the time taken to onboard each IoT device from 20-50 minutes, typical of today's semi-automated methods, to just a few seconds
- More secure onboarding. Intel® Enhanced Privacy ID provides a secure hardware-attested baseline for IoT platform and service offerings
- Greater competitiveness. This 'zero-touch' approach opens up new revenue streams for CSPs, since they can now cost-effectively provide customers with hardware-based secure onboarding to millions of IoT devices

Business Challenge: Seeking out new revenue streams

CSPs operate in an intensely competitive market segment. As revenues and margins from traditional services such as voice, SMS and pay TV decline, CSPs are looking for alternative revenue streams and ways to reduce costs while maintaining their high levels of service quality. Meanwhile, over-the-top (OTT) services, such as voice-over-IP (VoIP), instant messaging and video on demand (VoD), that ride on top of CSP networks, continue to cut into revenue share by offering low-cost or free alternatives with corresponding acceptable service quality - see figure 1. To grow and retain their share of the market, increase average revenue per user (ARPU), and fend off the competition, CSPs must seek out new revenue streams.

The increasing integration of digital technologies into everyday life is creating opportunities for CSPs to build on their traditional voice and data revenues by providing value-added digital services on top of their network infrastructure. Driven by increasing availability of cost-effective IoT devices, together with the emergence of new low power wide area (LPWA) technologies that complement existing WiFi and cellular communications, traditional machine-to-machine (M2M) offerings are evolving into a complete IoT offering.

CSPs can play a vital role in providing the 'dial tone' that helps boot strap the connectivity between the edge and the control platforms over either their existing wireless or fixed line networks. Many CSPs are already building out their network capability to support the forecasted demand for IoT devices and high volumes of data, and are investigating ways of further monetizing IoT models and services.

The IoT marketplace has spurned a vibrant ecosystem of niche players, as well as incumbents offering platform-oriented and vertically-focused products, applications and services. CSPs can capitalize on this fragmented market segment by offering differentiated, end-to-end services for the IoT.

More secure scaling for the IoT

Gartner's IoT Backbone Survey showed that 32 percent of IT leaders cite security as the top barrier to IoT success. With ever-increasing cybersecurity attacks posing a threat to consumers and businesses, maintaining security is paramount. When it comes to the IoT it is not just data that may be compromised. The physical and operational aspects of IoT mean that a security breach can have far reaching consequences, for example on industrial control systems, or medical devices, or automotive solutions.

While cybersecurity poses a threat to IoT adoption, it also presents an opportunity for CSPs. By providing a trusted communications infrastructure from the IoT devices at the edge of the network to the data center, CSPs can create a more secure foundation on which to build a technology stack, that includes service functions, applications and an IoT ecosystem. By doing this, CSPs are in a position to offer customers differentiated, end-to-end IoT-based services.

To meet consumer and specific industry needs, CSPs will need to manage a diverse set of IoT devices. Typically, these devices will be sourced through a complex supply chain of partners including manufacturers, distributors, resellers, solution providers, and system integrators. Furthermore, CSPs will need to securely and remotely provision and manage these devices to minimize operational and service assurance overheads.

Following typical semi-automated methods, it takes roughly 20-50 minutes to onboard one headless IoT device. This time-consuming process also involves shipping the device through its distribution chain where it changes ownership until it is ready to be installed by a highly skilled technician who can key in authentication credentials to get the device on the network. As Mirai and other IoT attacks have proved, such methods are fraught with security holes.

Scalability is also a concern. Today's costly, time-consuming and proprietary onboarding methods do not scale easily across different ecosystem providers, so it is hard for the industry to hit mass deployment of the IoT. Since revenue per connection for IoT services is expected to be much lower than that of existing voice and data connections, CSPs need a secure, low-touch IoT onboarding method to meet forecasted demand, and keep deployment effort and costs to a minimum.

Solution Value: Superior out-of-box customer experience

Intel SDO automates a trusted IoT device provisioning process for CSPs and provides a secure hardware-attested device baseline for their IoT platform and service offering. This 'zero-touch' process takes seconds and adheres to security best practices by separating the roles of installer, who may be a low skilled technician, from the security experts who want to ensure a validated device on network.

The solution utilizes digital 'ownership' credentials that are signed by the owner and are proof of entitlement. These digital ownership credentials are automatically uploaded to the CSP IoT Platform and removes the need to ship or configure default user credentials or other distribution paperwork.

Once securely provisioned using Intel SDO the CSP network operations team is able to manage a hardware-attested verifiable device, which as a by-product, has opened a private secured channel between the device and operational and business systems. They can then use this tunnel to push secure software updates or other PKI credentials to the device.

Intel SDO provides a simple superior out-of-box experience for the customer. CSPs and IoT service providers are gravitating to this model as an essential scaling mechanism to go from proof of concepts and live trials to production deployment volumes where manual onboarding is prohibitively expensive.

Solution Architecture: Intel® Secure Device Onboard

Intel SDO uses Intel® Enhanced Privacy ID (Intel® EPID) to anonymously authenticate a device and open a private encrypted channel to the IoT platform.

Intel EPID is one of the essential root of trust capabilities designed into the majority of Intel® processors since 2009. Unlike many IoT identity schemes, Intel EPID is a production proven model that has issued 2.7 billion keys and is used widely as a core element of Intel's security solutions including Intel® Software Guard Extensions (Intel® SGX), and Intel® Identity Protection Technology (Intel® IPT). It is the only industry ID solution where a device can be cryptographically proven to be a member of a valid group, but generates a unique signature every time, ensuring nobody can uniquely identify a specific device. Intel EPID is based on one public key that can be used to verify one or millions of member private keys.

Intel EPID is an approved ISO, TCG (Trusted Computing Group) standard for DAA Direct Anonymous Attestation. This remote attestation protocol opens an authenticated encrypted channel to remote platforms, which is useful beyond the initial device authentication as it also enables software or ID updates to devices in operation. Intel EPID is highly complementary to use with other PKI-based ID schemes for devices.

Figure 2 shows the architecture supporting zero-touch onboarding with Intel SDO using Intel EPID. The device's identity 'key' or Intel EPID is inherently distributed in the processors' protected hardware root of trust as it is manufactured. ODMs or OEMs drop in their own Global Unique Identifiers (GUIDs) and SDO-enabling software into protected boot code. At power on, the device opens an anonymous encrypted channel to the Intel SDO service which rendezvous the device to the customer's IoT device management platform. The device management platform utilizes this anonymous channel to push down a secure software update with operational PKI-based known identities. Finally, the device is securely onboarded, and is verified to forward secure data to the CSP's IoT service platform and applications.

Intel provides a suite of low touch enabling software development kits (SDK) and application programing interfaces (API) to rapidly enable the device ecosystem for this zero-touch model. Intel also operates a behind-the-scenes rendezvous service for the CSP's IoT platform to coordinate the bootstrap onboarding event for the first few activation moments of the IoT device lifecycle. Intel designed this rendezvous process to stay out of the direct authentication line for the device with the Intel SDO merely providing the methods or hand off for the customer and device to authenticate.

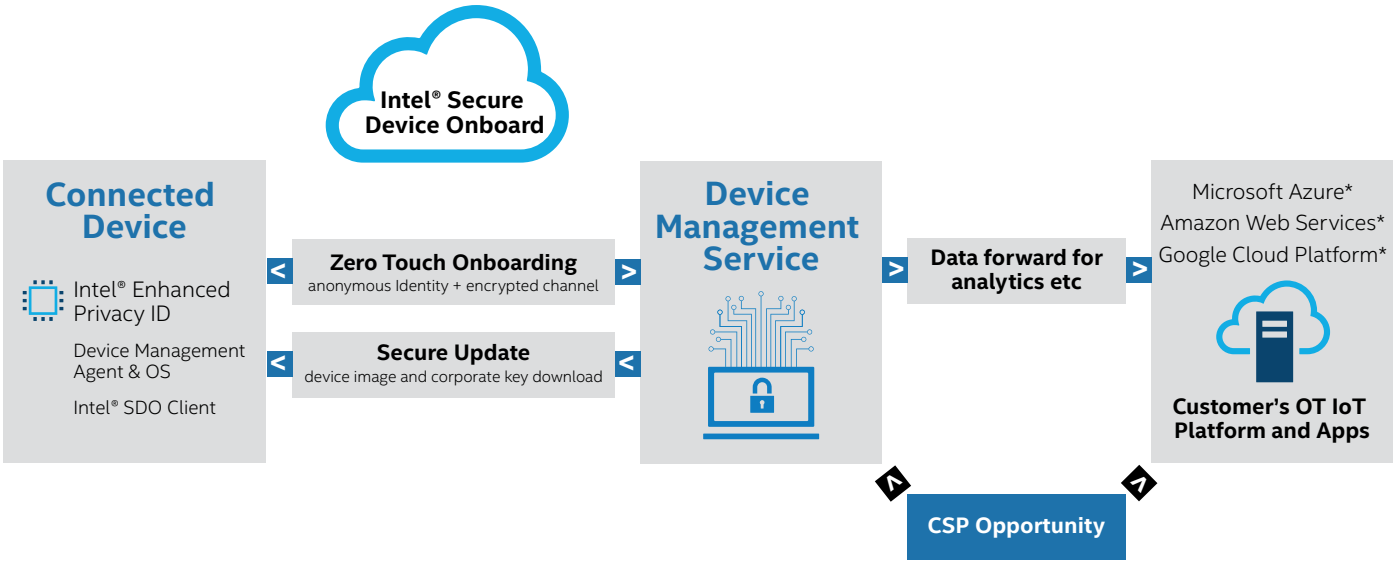

Figure 2. Zero-touch onboarding with Intel® Secure Device Onboard

"Intel® EPID uniquely combines verifiable hardware-secured identity with privacy preserving capabilities and the flexibility to meet the needs of chipmakers, OEMs, channel partners, and users. We see Intel EPID as applicable to many different IoT use cases and identity scenarios."

Steve Hoffenberg
Director of Industry Analysis for IoT, VDC Research

Conclusion

CSPs can offset the decline in traditional voice and data revenues by providing differentiated, end-to-end IoT services. Since they provide the communications infrastructure from the IoT devices at the edge to the network through to the data center, CSPs can add value by creating a more secure foundation for IoT platforms and services. This is particularly beneficial for more quickly and more securely onboarding IoT devices.

Intel SDO allows CSPs to automate IoT device provisioning, dramatically reducing the time it takes to onboard each device. Meanwhile, Intel EPID is used to anonymously authenticate each device and open a private encrypted channel to the IoT platform. Ultimately, this approach enables CSPs to cost-effectively provide customers with a service for more secure scaling of the IoT to millions of devices.

Solutions Proven By Your Peers

Intel Solutions Architects are technology experts who work with the world's largest and most successful companies to design business solutions that solve pressing business challenges. These solutions are based on real-world experience gathered from customers who have successfully tested, piloted, and/or deployed these solutions in specific business use cases. Solutions architects and technology experts for this solution brief are listed on the front cover.

Learn More

You may also find the following resources useful:

- **Intel® Secure Device Onboard:** www.intel.com/securedeviceboard

Solution Provided By:

0917/CAT/CBS/PDF 336530-001EN