PRODUCT BRIEF

Intel® Secure Device Onboard

More secure, automated IoT device onboarding in seconds

Scale IoT Deployments to Put More Devices into Service Faster

Device Onboarding – an Unsolved Problem

Today, the onboarding process for IoT typically takes over 20 minutes per device.[1] This involves coordination among installation technicians, IT network/security operations, and operational technology teams. This costly, manual process is holding the industry back from the promise of tens of billions of devices.

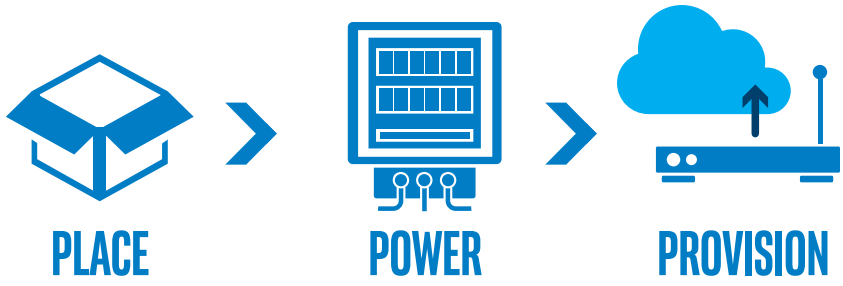
The core challenges within the overall process include device identification, data privacy, tracing ownership during distribution, secure communications from edge to cloud, and configuration with the IoT management platform that will command the device and forward data to the cloud.

Zero-Touch. Zero-Worries.

Intel® Secure Device Onboard (Intel® SDO) is an automated service that enables a device to be drop-shipped and powered on to dynamically provision to a customer's IoT platform of choice in seconds. This zero-touch model simplifies the installer's role and scales the number of devices that can be secured and automatically be deployed in production. Intel SDO eliminates poor security practices, such as shipping default passwords, and delivers an innovative device privacy model for IoT. With a single imaging step for zero-touch onboarding, device makers can mass produce devices and leave configuration to Intel SDO.

Benefits

- **Automated from minutes to seconds –** Break free from hard-coded or manual activation methods with dynamic discovery of the customer's IoT platform for fast onboarding at power on.
- **Hardware Protected Onboarding –** Eliminate passwords with Intel® Enhanced Privacy ID (Intel® EPID) to anonymously authenticate devices. Helps to prevent hackers from tracing the device from factory to owner.
- **Streamline Distribution –** Digitally trace ownership from manufacturer to customer, and provide a rendezvous point in the IoT platform where the owner can claim the device.
- **Ecosystem Accelerator –** Eliminate expensive customer configuration pre-loads with a zero-touch experience that differentiates your solution.



Onboarding Friction

As IoT use cases gain in popularity, Operational Technology (OT) teams increasingly request to provision devices onto corporate networks. Information Technology (IT) security experts want to slow down this process to ensure devices have been authenticated properly. This is causing friction and slowing down Proofs of Concept (PoC) as they strive to achieve production scale.

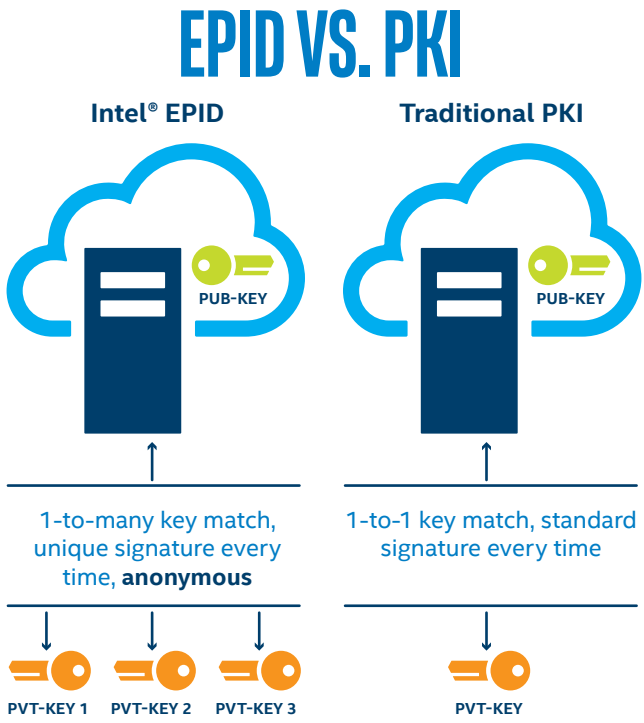
From a field installation perspective, manual onboarding activation is often problematic with potentially thousands of "headless" IoT devices that require re-keying and authentication of device credentials to get on to the network. Misconfiguration, shipping of default credentials, and use of software-only security mechanisms can further introduce security risks.

Hardware-Enabled Chain of Trust from Silicon to Customer Activation

Intel SDO takes a new approach where Intel EPID, a TCG/ISO identity and authentication standard, is embedded in silicon before it is assembled into a device. The Intel SDO service leverages Intel EPID to cryptographically validate the device.

Unlike typical PKI based authentication methods, Intel SDO does not insert Intel into the authentication path. Intel brokers a "rendezvous URL" to the Intel SDO service, where Intel EPID technology opens a private authentication channel between the device and the customer's IoT platform.[2]

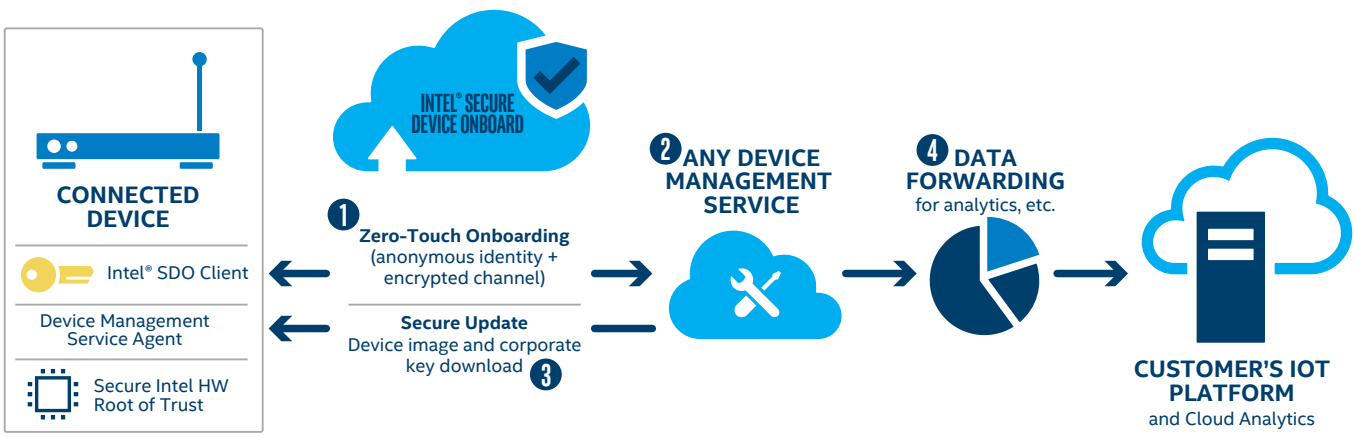
Intel EPID solves the privacy dilemma for IoT to ensure device onboarding and software provisioning updates are kept anonymous and more secure. Intel EPID establishes a best-practice identity model for IoT onboarding, and it is a proven method with over 2.7 billion keys distributed in Intel and non-Intel MCU processors since 2008.



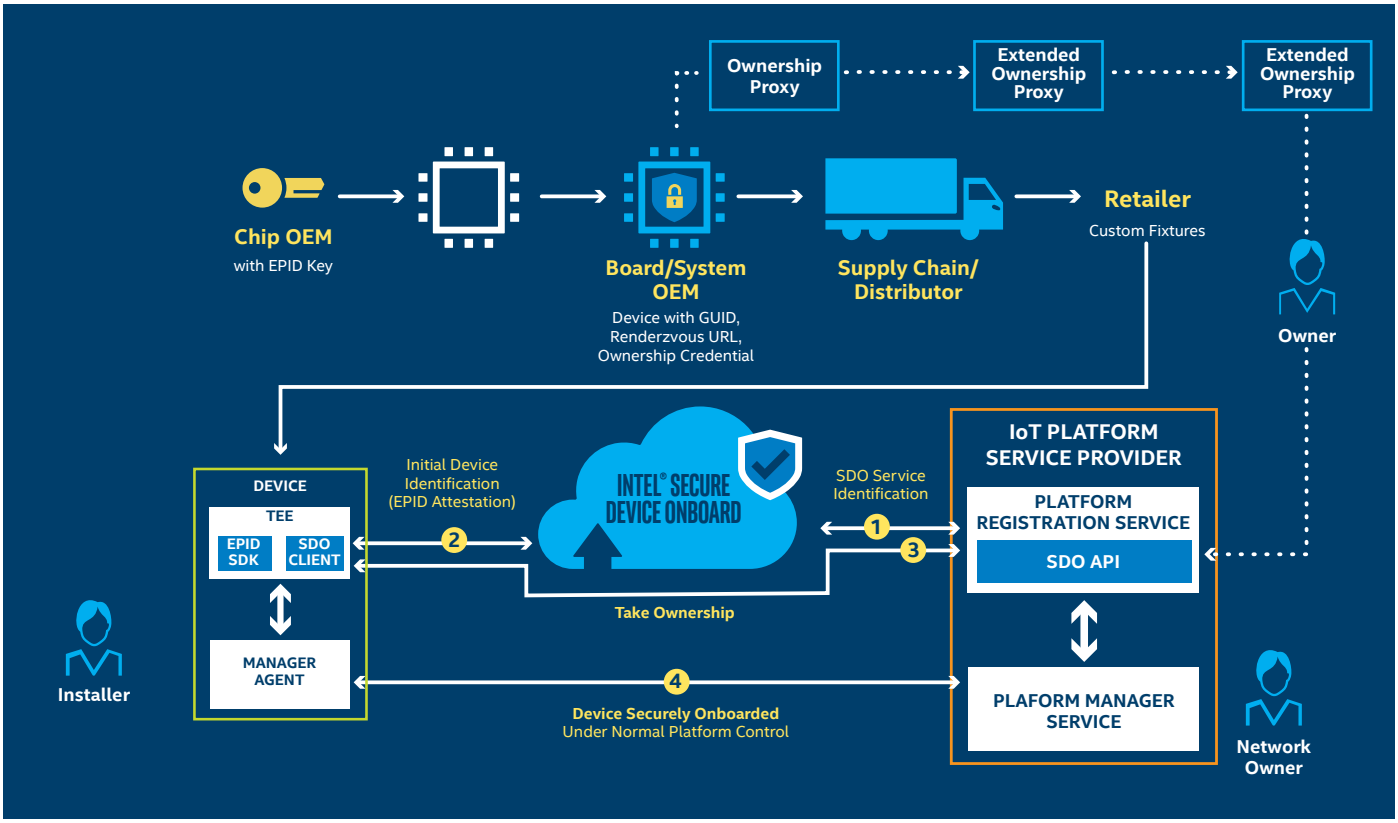
Intel® EPID, Privacy-Preserving Identity

Scalable Device Enablement

In a typical scenario, a device manufacturer will build and sell a large quantity of devices through multiple distribution channels. This means that the manufacturer isn't going to know where a device will ultimately be deployed, what cloud it will connect to, or how the device is going to be used. This causes one-off staging and expensive pre-loading costs for device manufacturers in order to support customer orders. Alternatively, shipping a standard image increases the manual provisioning configuration for the installer in the field. Intel SDO solves these problems by providing a rendezvous service where transfer of ownership can be established dynamically after the first boot of the device.



Intel® SDO + Device Management delivers a complete onboarding and security channel



Broad Ecosystem of Devices for IoT Platforms

Customers will have a broad array of Intel and non-Intel devices that need to be provisioned to an IoT platform. But, Intel has a rich ecosystem of device partners that have enabled SKUs for the zero-touch onboarding method. Intel freely provides Intel SDO SDKs, enablement APIs, and support to speed onboarding and usage of IoT Platform services. Thus, Intel SDO is capable of onboarding an Intel SDO-enabled device to any IoT device management platform.

For customers without a device management platform, or for IoT platform providers that want full device lifecycle management capabilities, Intel can offer Intel SDO that comes pre-integrated with Wind River Helix* Device Cloud. The combination of the two solutions enables a complete hardware-secured device lifecycle—from onboarding a clean device baseline to delivering a secure software update.

Steps to a Complete Implementation

The entire value chain is involved in the Intel SDO process.

1. **Silicon Provider –** Embeds an Intel EPID identity in the silicon's trusted execution environment (TEE) at manufacturing, utilizing an Intel EPID 2.0 open source SDK.
2. **Gateway/Device Manufacturer –** Utilizes 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.
3. **Device Owner –** After the distribution change of ownership, the final owner can automatically load their digital ownership receipt into the IoT Platform.
4. **IoT Platform –** Utilizes 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.
5. **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.

Intel SDO vastly accelerates trusted onboarding of IoT devices—from minutes to seconds—with a zero-touch, automated process that begins when the device is first powered on and ends when the IoT service provider of choice takes control with a baseline chain of trust from the silicon provider through to the IoT control platform.

Specifications

Category	Description
Device Hardware Identity	Crypto to sign DAA (Direct Anonymous Attestation) protocol. Intel® EPID 2.0 key (also EPID 1.1 on select IA devices). SDK and keys available from Intel for IA and non-IA devices. Requires 144 bytes of non-volatile, one-time programmable memory in trusted execution environment.
Device Platform	CPU – Intel Atom® E3800 series processors. Firmware – Intel Atom processor with latest Intel TXE firmware. OS – Ubuntu 16.04. Windows® 10 IoT Ent, Yocto, and Pulsar. Intel Software – DAL applet, provisioned at manufacturing. ARM Device Software – C-based OS-level implementations of Intel® SDO device code, with source code available.
Device Credentials	Credentials Tool Machine BOM: integrated on assembly line to use Intel® SDO Cred Tool software to initialize device at manufacturing for transfer of ownership proxies and credentials stored in secure hardware/memory on device.
Supplier Cred Tool Software	Cred Tool software to create ownership proxies signed to supplier's RSA or ECDSA public key. Enables supply chain entities to countersign that they have taken ownership of device through to the end customer's procurement.
IoT Device Management Platform	Intel SDO API integrated to the IoT platform device management that is used to register customer's ownership proxies with the Intel SDO service. Create onboarding script that mimics manual set up for devices. Script sent to devices during the Intel SDO onboarding process.
Protocols: Device & IoT Platform	Device initialization and transfer of ownership. Implemented as JSON message and transport HTTP/HTTPs and REST. Able to use a HTTP proxy to get to the Internet.

Learn More

Solution overview and collateral: **www.intel.com/securedeviceonboard**

Ecosystem enablement tools: **https://software.intel.com/sdo**

For go to market partner inquiries: **iotonboarding@intel.com**

[1] Kaiser Associates. "IoT Onboarding, A Device Manufacturer's Perspective," 2017.

[2] Technically, you can verify a device with group, anonymous identity, just knowing that it is trusted for a given purpose with the EPID attestation. Then you can establish identity known to just the two parties afterwards, using the private authentication channel.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at www.intel.com.

* Other names and brands may be claimed as the property of others. 1017/JAS/HBD/PDF Please Recycle 336540-001US