PRODUCT BRIEF

Intel® Secure Device Onboard

Automated IoT device provisioning in seconds

Figure 1: Manual Provisioning

Device Onboarding – an Unsolved Problem

Today, the onboarding process for IoT devices typically takes over 20 minutes each[1], involving coordination among installation technicians, IT network/security operations, and operational technology teams. Additionally, manual onboarding approaches are often insecure as they require the installation technician to have access to the passwords and credentials for all of the devices. In conclusion, this costly, insecure manual approach is holding the industry back. It's time for a new way forward.

Zero-Touch. Zero-Worries.

Intel® Secure Device Onboard (SDO) is an automated "Zero-Touch" onboarding service. To more securely and automatically onboard and provision a device, it only needs to be drop shipped to the point of installation, connected to the network and powered up. SDO does the rest.

This zero-touch model simplifies the installer's role, reduces costs and eliminates poor security practices, such as shipping default passwords.

Benefits

- **Zero-Touch Onboarding** - No expertise needed by the installer
- **Fast** - ~1 minute from power up
- **More Secure** – Installer has no access to passwords or credentials
- **Any Processor** – Runs on any hardware - from an Arm* MCU to an Intel® Xeon® processor
- **Any Platform** – Onboard to a cloud or an on-premise server
- **Hardware Root of Trust** – Supports Intel® EPID and ECDSA for maximum device security
- **Late Binding** – bind devices to platforms at installation time, not during manufacturing, to greatly reduce device SKUs
- **Open** – Intel and Arm* are driving SDO as an industry standard

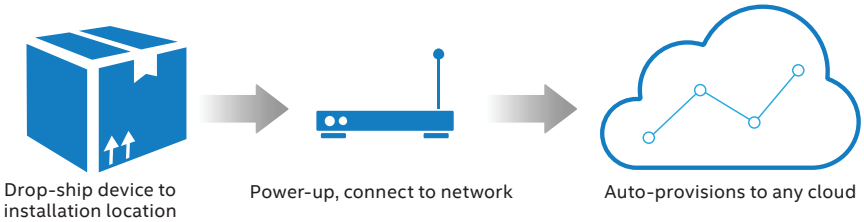

Figure 2: SDO Streamlined Use Case

SDO vs. Other "Zero-Touch" Solutions

Most current "Zero-Touch" solutions in the market today require that operational credentials of the target platform are built into the device at the point of manufacture. Additionally, they may require a discrete secure element be mounted on the device board for safe credential storage. The result of this is that a unique device SKU is needed for each customer/cloud combination. This adds significant friction in the supply chain as devices are effectively unique for a given end customer – requiring products to be built to order or held in inventory.

Late Binding – SDO provides late binding of the device to its chosen platform (cloud or on premise server) i.e., the device's target platform can be selected just before the device is on boarded. This means that original device manufacturers (ODMs) can build identical IoT devices in high volume that can then be targeted to a specific platform at the point of installation rather than at device manufacture. The impact of late binding is significant as it allows ODMs to build-to-plan rather than build-to-order, reducing inventories, supply cycle times and costs. Additionally ODMs can use the same manufacturing process for all platforms (cloud or on premise) rather than needing to set up a unique manufacturing tools for each one.

Arm and Intel Support – Intel and Arm see the onboarding challenge in the same way. Both companies believe the onboarding challenge must be solved at the industry level for the benefit of all. Given this, Intel, Arm and other industry players are working together to make SDO into an industry standard, broadly available to all. Plans are underway, and an industry standards body is expected to announce plans to adopt and evolve SDO later in 2019.

Open – To benefit the whole IoT industry, Intel plans to open source SDO later in 2019. This will allow the ecosystem to readily adopt SDO, knowing that it will not be controlled by a single company. Lastly, the SDO protocol specification is available today to interested customers and the IoT ecosystem.

Security via Direct Trust Model – SDO establishes a direct trusted connection using two-way mutual authentication between the device and the IOT platform (cloud or on premise server) at initial boot. Unlike other approaches, SDO doesn't rely on a vulnerable, single-point-of-failure, 3rd-party, centralized registry. Intel SDO also protects against attacks in the supply chain that may intercept the device in transit, attempting to take over the device trust by being the first to use the device before it gets to the final point of installation. Finally, SDO eliminates the insider threat that arises from revealing keys to the Installer. SDO enables loading of a generic (onboarding only) credential in the processor's trusted execution environment or secure element that works for onboarding all SKUs. At provisioning time, the customer's operational credential can be downloaded. In summary, with SDO, there is no potential for insider leaks of keys, device ownership can't be intercepted in the supply chain, and there is no list of all the devices mapped to each platform that could be potentially stolen or compromised.

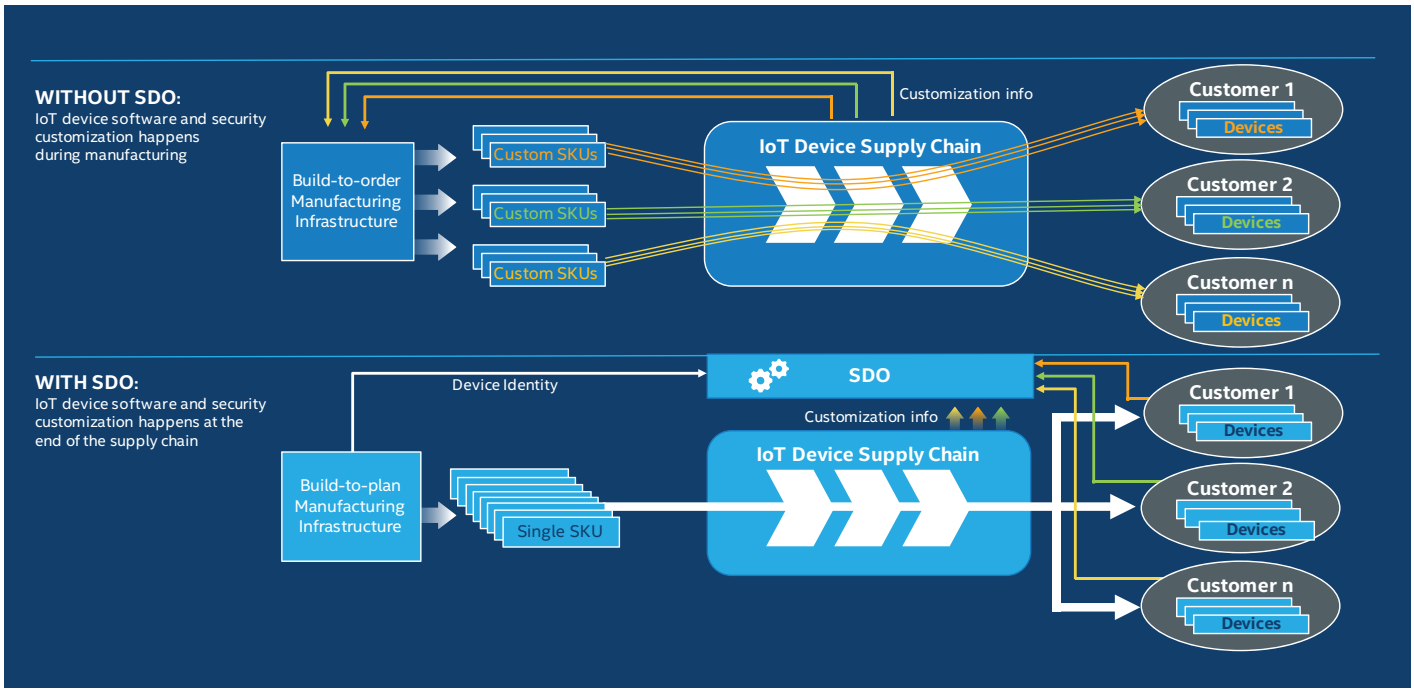

Figure 3: SDO "Late Binding" Simplifies Supply Chains

How SDO Works

To understand how SDO works, we can consider what happens in three phases;

At Device Manufacture

- The processor (Intel or Arm) contains a unique hardware root of trust key (either ECDSA or Intel® EPID)
- The ODM uses the SDO Manufacturing Toolkit to insert generic credentials into the device.
- The ODM installs the SDO Client software on the device.
- The SDO Manufacturing Toolkit creates a digital Ownership Voucher that is sent to the new device owner i.e. VAR, SI or end customer.

Before Installation

1. **Step 1:** The Ownership Voucher is passed to target IoT platform, e.g. Arm Pelion*.
2. **Step 2:** The new device is registered in the SDO Rendezvous Service together with the URL for the target IoT platform.

At Installation

3. **Step 3:** Device powers on and contacts the SDO Rendezvous Service which authenticates the device and then points it to its target platform using the URL from Step 2.
4. **Step 4:** The platform and device mutually identify each other using the root of trust and Ownership Voucher. An authenticated tunnel is established between the device and platform.
5. **Step 5:** The provisioning payload for the target platform is transferred to the device. This can be credentials such as passwords or can be a complete platform agent.

   Now the platform takes control of the device and SDO shuts down. SDO remains dormant for the remainder of the life of the device unless a specific decision is made, e.g. to re-sell the device and onboard it to a new platform.

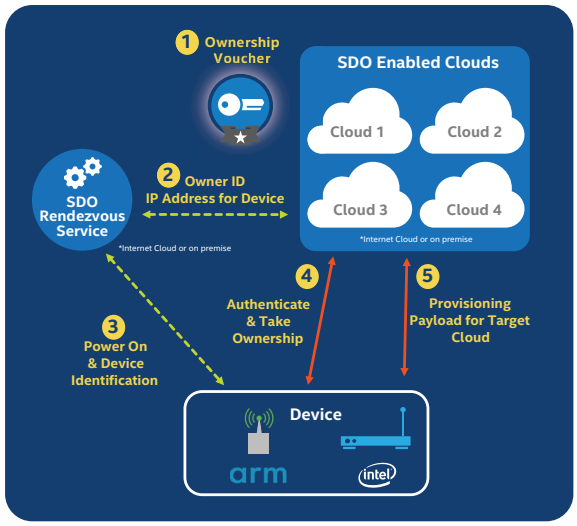

Figure 4: SDO Processing

The Ownership Voucher & How it Fits into the Supply Chain

A unique part of the SDO solution is the Ownership Voucher. The Ownership Voucher is how the platform proves to the device that it is its rightful owner. The Ownership Voucher is created originally by the ODM. It then passes through the supply chain until it arrives at the end user who registers it with their desired target platform (cloud or on premise).

Each party in the supply chain uses the SDO Reseller Toolkit to countersign the voucher to create an auditable traceability log embedded in the voucher. Furthermore, it maintains integrity of the signatures and does so without having to power on the device.

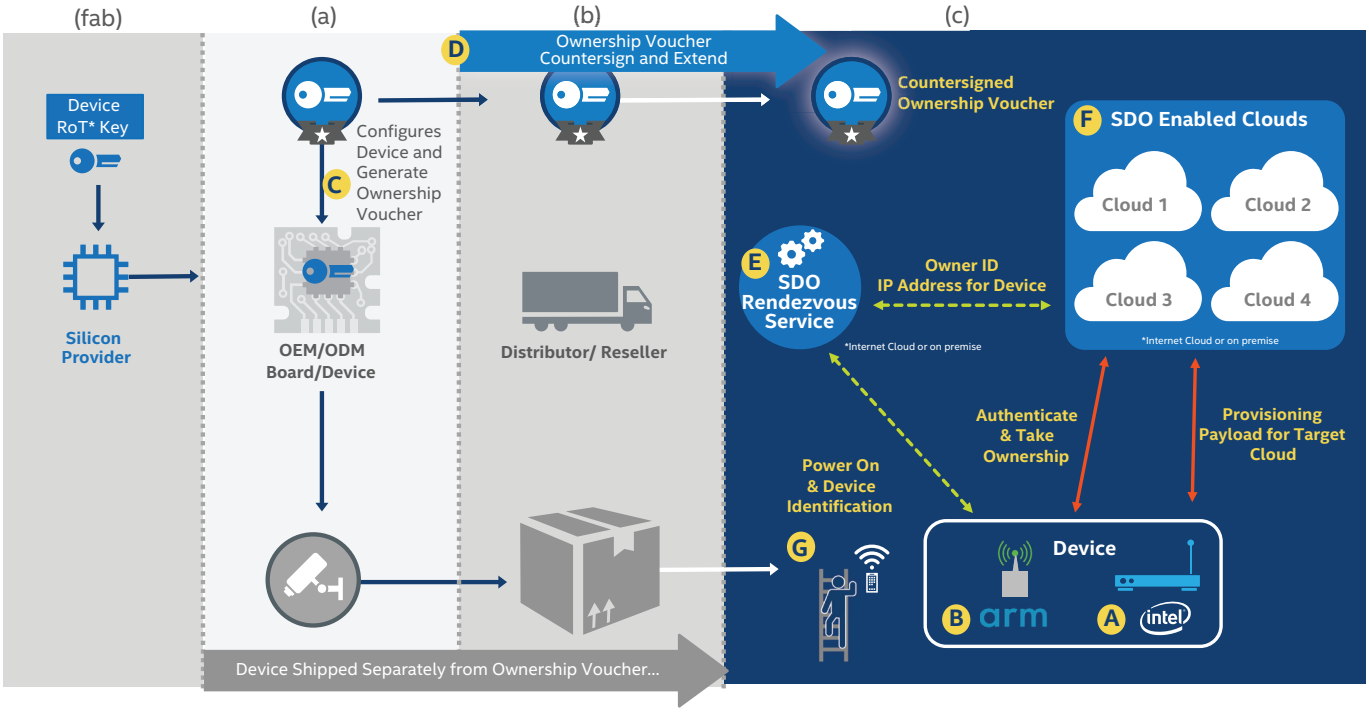

Figure 5: Ownership Voucher Flow and SDO Solution Components (See Table 1)

CATEGORY	DESCRIPTION
A SDO Client-Intel (Intel CPU based devices)	SDO secure client application that uses Intel hardware root of trust. Ready to be packaged with your OS to run automatically at device initialization time. Validated with following OSs: Win10 IoT Enterprise, Yocto Linux, and Pulsar Ubuntu. Supported Hardware: Skylake, Kaby Lake, Coffee Lake, Bay Trail-I, Apollo Lake based platform architectures. Intel® Xeon® processor platforms with TPM planned for 2019. Additional Intel platforms in development.
B SDO Client-SDK (e.g. Arm A & M class based devices)	Portable generic device C-based SDK that can run on range of processors. Source code. Integrates with standard crypto libraries.
C SDO Manufacturer Toolkit	Set of software tools deployed in manufacturing station (on factory line) to initialize and enable SDO on the device. Or can be run by a supply chain partner post manufacture. Integrates with OEM/ODM's ERP system. Allows provisioning SDO artifacts and credentials to the device's trusted execution environment and creating digital Ownership Voucher ('proves' ownership). OS: Ubuntu Linux*.
D SDO Reseller Toolkit	A tool used by resellers, VARs, Distributors, or SIs. Enables supply chain entities to countersign and extend the Ownership Voucher. Opens up new use case efficiencies such as Distributors breaking pallets, centralized warehousing, and centralized cold spares. OS: Ubuntu Linux
E SDO Rendezvous Service	An automated standalone service to redirect the device towards its target IoT platform. It can be run in the cloud or on premise if required. Intel hosted service available. OS: Ubuntu Linux/Java source code
F SDO SDK - IoT Platform Integration	Provides SDO onboarding capability to the IoT device management platform. SDO protocol implementation hosted within IoT platform. Allows the IoT platform to use SDO Ownership Voucher to register new devices as assets (representation of device or "digital twin") within the IoT Platform. As a part of onboarding process, SDO protocol allows downloading target credentials and native platform software agents. SDK written in Java with Docker encapsulation.
G SDO Installer Tools	Enables network admission and troubleshooting - e.g. wifi enabled device, corporate proxy, Android based app, and additional networking protocols TBD. Creates independent channel for device to onboard. OS: Android and Linux.

Table 1: SDO Solution Components[2]

Learn More

1. See demo or gain overview: Visit www.intel.com/securedeviceonboard
2. To gain access to the SDO software and documentation (https://software.intel.com/en-us/secure-device-onboard):
   a. Register for an IDZ account
   b. Request access to SDO Materials
3. SDO Program-Business
   c. Contact Iotonboarding@intel.com for a discussion.

[1] Kaiser Associates Research and Analysis, IoT study, August 2017

[2] Contact Intel for latest specification