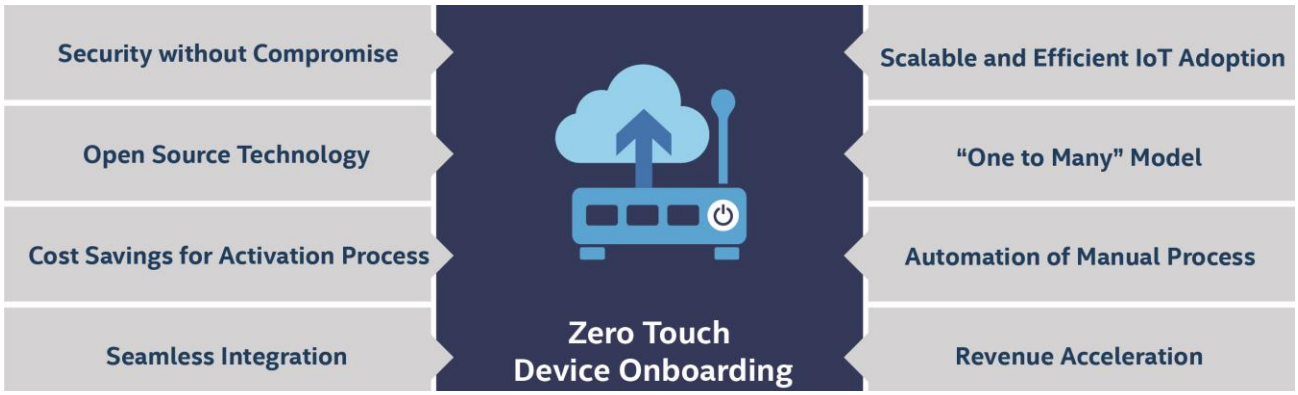
IoT Onboarding

A DEVICE MANUFACTURER'S PERSPECTIVE

Addressing a key customer need to onboard IoT devices securely and efficiently



®

METHODOLOGY

Intel® sponsored a primary research study to gain insights into current and future automated onboarding processes. Kaiser Associates' research methodology for this white paper focused on current processes, challenges, and solutions for onboarding IoT devices in industrials, healthcare, and smart buildings. In addition to a literature review, Kaiser conducted 30 in-depth interviews with experts at ODMs and with end users of IoT devices in these industry verticals.

ABOUT KAISER

Founded in 1981, Kaiser Associates is an international strategy consulting firm that serves as a key advisor to the world's leading companies. We provide our clients with the unique insights to drive critical decision making and solve their most pressing problems.

INTRODUCTION

Experts estimate that over 30 billion devices will be part of the Internet of Things by 2020[1]. However, to achieve the benefits that ODMs and customers envision for IoT, devices must be onboarded efficiently and securely. Today's onboarding systems are

time-consuming, resource-intensive and complex. Fortunately, emerging technologies are looking to address these challenges by automating the onboarding process, thus enabling secure integration with control platforms & corporate networks in seconds rather than minutes.

Intel® Secure Device Onboard (Intel® SDO) addresses this lengthy, often cost-burdened process. It streamlines and automates the onboarding process of headless IoT devices securely, addressing a core customer need and delivering a competitive advantage for IoT device manufacturers with an automated onboarding solution. The Intel® SDO model offers a "one to many" solution that can be integrated into all IoT devices and is compatible with the majority of IoT platforms, enabling device manufacturers to bypass efforts necessary to uniquely configure individual devices. The Intel® SDO solution at its core is based on Intel®'s identity solution, Intel® Enhanced Privacy ID (Intel® EPID) that is an approved ISO/TCG standard.[1] As the foundation of Intel's hardware-enhanced security technologies, Intel® EPID maintains the security and privacy of the device's identity throughout the onboarding process. With the ability to automate onboarding processes and the security infrastructure that Intel® EPID provides, the Intel® Intel® SDO solution alleviates the stress of onboarding preparation and activation for device manufacturers and customers so that they can start deriving insights from device data sooner.

"The demand to deploy new devices is increasing exponentially every year and the technology is not there. The work that we need to do for preparing devices is continuing to improve, but everything should be done virtually in the future."
– Digital Product Manager, Fortune 500 ODM

BARRIERS TO EFFICIENT AND SCALABLE IoT ADOPTION

BARRIERS

With the expansion of IoT and the knowledge of its benefits in multiple industries, enterprises and providers are utilizing billions of IoT devices to enhance their operations and service offerings. To achieve the benefits of IoT utilization, devices must be activated efficiently and securely across a wide array of control platforms, corporate networks and complex, interdependent infrastructures and industries. Onboarding devices requires significant collaboration with multiple parties. While IT departments focus on taking the necessary security precautions, operations and end users are more concerned with getting devices up and running as quickly as possible. With an onboarding process that takes an average of 20 minutes, tension between groups is often unavoidable.

The process to onboard an IoT device is time consuming and highly manual, requiring significant amounts of time and focus for device provisioning and authentication along the value chain: 1) Given the wide variance in customer infrastructures and needs, silicon and device manufacturers must first collect customer requirements, 2) Devices must then be configured to specific customer needs, requiring multiple rounds of testing and unique instruction preparation, and finally, 3) The customer must complete a long list of manual steps to activate the device. With this level of complexity and manual variability of configuration, it is virtually impossible to efficiently onboard every device securely, resulting in the high potential for security risks and opportunity for hackers to take advantage of vulnerabilities to infiltrate and disrupt even the most protected infrastructures.

"If everyone has a unique and different configuration – you need to build logic and code for all the things it attaches to."
– IoT Solutions Architect, Major Industrials Manufacturer

A SECURE DEVICE BASELINE STARTS WITH SILICON

In order to develop devices that can be onboarded successfully, careful attention must be paid to customer platforms, industry requirements, integration needs, and unique customer use cases. Silicon suppliers provide critical hardware security features that provide a root of trust to isolate, protect, and securely store identities, security keys and other essential data device manufacturers and end customers depend on for secure activation in the field.

"One of the biggest barriers to efficient adoption and implementation of IoT devices is the lack of standardization. Each device that we put out has a unique configuration."
– Senior Solutions Architect, Major Smart Building Device Manufacturer

DEVICE ENABLEMENT

Once the silicon is prepared, the ODM is responsible for device enablement. As the ODM builds the boards and preloads the system with software and configurations they can enable critical features in the silicon providers' protected zones to ensure protected boot and remote attestation of the software and hardware by third parties. ODMs in this stage are responsible for making security decisions. Often, ODMs leverage software and OS layers for security and do not fully realize the security potential of the hardware of the device.

IoT Platforms providers often require device manufacturers to preload onboarding agents or credentials/keys prior to delivery to obviate the need for end users or OEM installers to have to engage in this step themselves during the field activation process. In addition, customers themselves may also have custom requirements for the ODMs that must be pre-loaded. The identification of all requirements can commonly take weeks to complete and require the engagement of multiple parties.

VALIDATION, TESTING AND TRAINING

Once the required information is preloaded, the complete system can be integrated by device manufacturers. Upon integration, device manufactures allocate a significant amount of time and effort to test the device's security and ability to be onboarded in the manner expected by the customers' IoT control platform. This step is extremely important, as ODMs can be held liable for devices that are not secure when shipped to customers. There is inherent risk in these devices for data hacking, which can lead to recall expenses and potentially legal action.

Validation requires rounds of testing with various parties within the company, such as internal technical experts and corporate-level security teams, often taking up to three weeks to complete.

"You're going to spend a lot more time planning a roll out of devices - once you've been burned once or twice, you realize you really have to think this through."

– Senior Systems Architect, Major Industrial Manufacturer

After validation and testing, training is necessary to ensure that business units are knowledgeable of configurations and onboarding processes that are unique to each customer and platform. This is reported to be a significant time commitment that is unavoidable in the majority of device deployments with new customers. Not only does this require effort from the business units themselves, but also from the individuals familiar with the solutions who are responsible for developing the training or even other channel partners such as Distributors. Multiply all of these processes by dozens, if not hundreds, of devices that need to be onboarded at a specific site and the challenge increases exponentially.

CUSTOMER ACTIVATION

Once a customer receives the pre-configured device, the activation process begins. Not only is the process highly manual and lengthy, often taking between 10-45 minutes to complete per device, but it is also highly dependent on the contracted installers or the end user tasked with the responsibility of activating the device. While some customers are familiar with device integration, others are completely new to the idea of connected devices. In addition, even when customers are capable of onboarding these devices successfully, it can be a question of bandwidth and ability to allocate time.

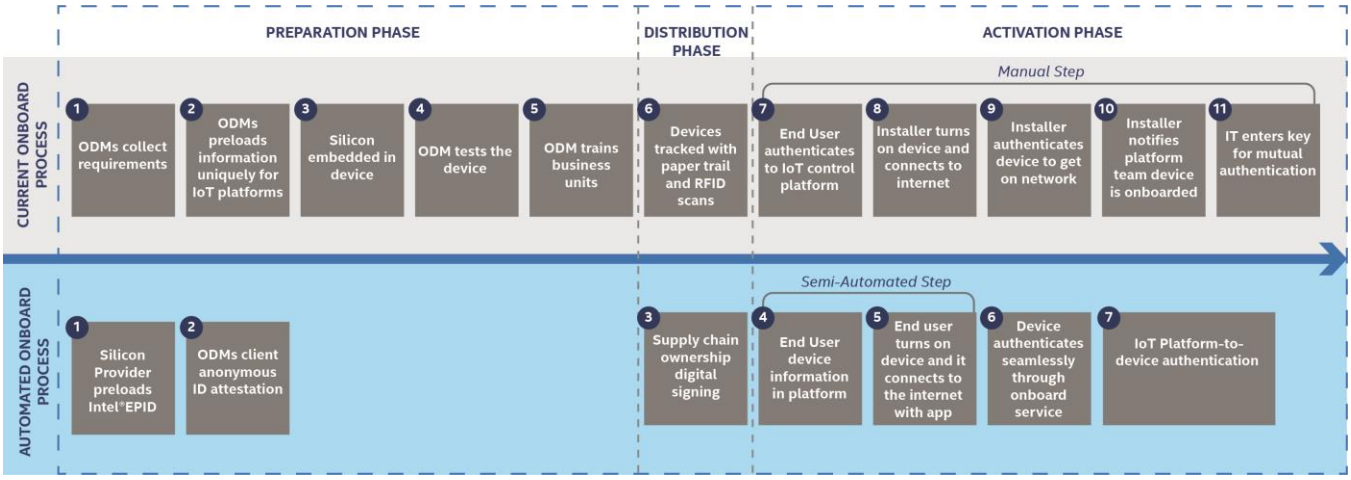


Figure 1

Intel® SDO dramatically reduces the number of steps in the preparation and activation phases of device onboarding and authentication.

INTEL® Secure Device Onboard

A SECURE, AUTOMATED SOLUTION

With Intel® SDO, the onboarding process is decreased to mere seconds, eliminating the risk of errors made during the manual process steps and enabling the end user to realize the potential of its IoT device sooner. Easily implanted into any IoT device and already a part of Intel® Architecture (IA) and or provided by other MCU providers, Intel® SDO is compatible with the majority of IoT platforms, making it a "one to many" solution. This enables silicon and device manufacturers to bypass efforts necessary to uniquely configure devices for customer use cases and platforms. In addition, Intel® SDO streamlines the process end users must go through to onboard devices.

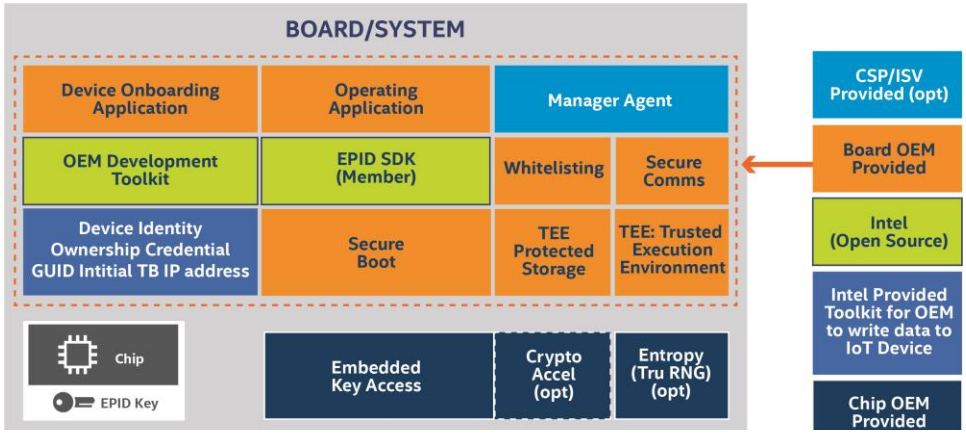
Intel® SDO is an open standard technology and a feature of Intel®'s identity solution, Intel® EPID. As the foundation of Intel®'s hardware-enhanced security technologies, Intel® EPID maintains the privacy of the device's identity throughout the onboarding process. Privacy is maintained as Intel® EPID sets up a direct anonymous communication channel that is only visible to the device endpoint and the IoT Platform. It is a best practice to use Intel® EPID for the initial anonymous attestation of the device identity versus a PKI credential that reveals authentication endpoint data that can be used to build attack maps that compromise the device. It is up to the owner if they wish to push down or swap in a traditional PKI credential to the device for further communications after the onboarding process or maintain usage of the Intel® EPID credential. With the ability to automate onboarding processes and the security infrastructure that Intel® EPID provides, Intel® SD is a unique solution device manufacturers can adopt to differentiate themselves from competitors.

ENABLEMENT METHOD FOR DEVICE MANUFACTURERS

Irrevocable immutable Identity is one of the five basic tenents to hardening an IoT Device. Intel® EPID is Intel's implementation of ISO/IEC 20008 standardized Direct Anonymous Attestation (DAA) that provides identity that scales with the IoT, as well as preserves privacy. It is immutably written into Intel® processors and enabled in select 3rd-party processors (Intel® announced in December 2013 that it is enabling all processors in IoT with Intel® EPID).

Intel® SDO takes advantage of the privacy properties to establish attestation with the IoT device from first boot. It does so in a way that – unlike PKI certs which are public and visible from both ends in clear text – cannot be tracked by malicious entities lurking on the internet. In addition, Intel® SDO's protocol is available as an SDK both for IoT devices (as open source) and services (as a licensed toolkit). Thus, putting Intel® SDO's onboarding solution into your IoT devices or services is a simple matter of using an Intel® EPID-enabled processor for the IoT Device and integrating the SDKs into your application on the device or in the service. Should your processor not be Intel® EPID enabled yet, Intel® is actively seeking to enable that.

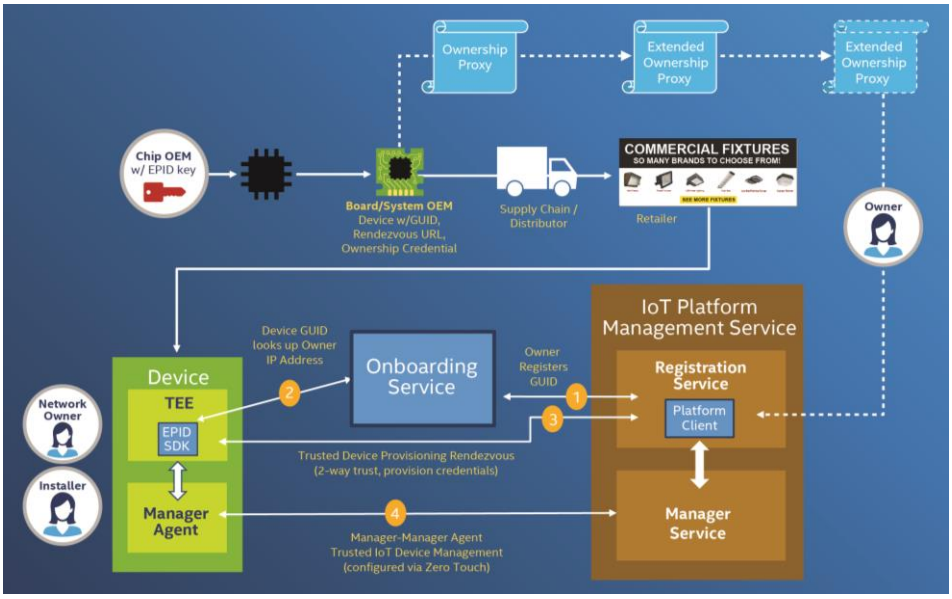
Intel® SDO AND Intel® EPID STACK ON AN IoT DEVICE



THE VALUE OF AUTOMATION FOR DEVICE MANUFACTURERS AND THEIR CUSTOMERS

Secure and automated approaches to onboarding lead to numerous benefits for device manufacturers and their customers. For device manufacturers, configuration time will significantly decrease, if not be eliminated altogether, with Intel®'s "one to many" SDO solution. Field costs are also significantly reduced by streamlining the process and eliminating the number of parties responsible for the success of implementation. In addition, an automated onboarding solution is an attractive and differentiated feature for customers, increasing revenue potential for device manufacturers. Customers achieve significant cost savings when they eliminate the manual processes and opportunities for delays in onboarding while also gaining higher levels of security due to the more automated and centrally administered onboarding approach.

FEATURES AND BENEFITS: "ONE TO MANY" MODEL



INTEL® SDO'S "ONE TO MANY" MODEL

Whether requirements are collected from customer business partners, customer IT departments, or unique industry specifications, silicon and device manufacturers are faced with countless requirements that need to be taken into consideration. Unique configurations are created to increase device interoperability with specific corporate networks and IoT platforms, other IoT devices on the premises, and security standards enforced by the customer or industry. The necessary steps to build unique configurations, however, are costly and time consuming, taking up to a month to complete and costing ODMs potentially thousands of dollars. Intel® SDO offers a "one to many" model, eliminating the steps necessary to uniquely configure devices to enable onboarding for each customer and use case. Upon completion of onboarding processes, customers can then push down special configurations they may want with their Platform provider as part of the agent provisioning process that comes after onboarding.

ELIMINATION OF SILICON AND DEVICE PREPARATION TIME

Currently, configuring devices to be compatible with customer platforms and requirements can take anywhere from seconds to over 10 minutes per device. As customers can order in lots of 1-1,000+ devices, this can add up to a significant time commitment and burden. The success and efficiency of initial configuration steps are highly dependent on acquiring the right information from platform providers and customers. This step alone can be time consuming, as collaboration with IT departments can often be a challenge to ensure data correctness. Once the right information is acquired, internal software teams get to work on configuring the devices, often taking up to two weeks to complete and test.

With Intel® SDO's "one to many" model, these steps are unnecessary. The open source enablement toolkits are compatible with virtually all IoT devices and provide integration to a majority of customer platforms, eliminating the need for one-off configuration.

"To configure devices to specific hospitals, we often ask customers to dedicate an IT resource to collaborate with our teams. It requires a significant amount of effort from both sides to configure these devices properly."
– Product Manager, Major Healthcare Device Manufacturer

REMOVAL OF EXCESSIVE TESTING AND VALIDATION

Currently, once the initial configuration and testing is completed, additional security and onboarding tests must be conducted to ensure the device is customer-ready. Internal teams unfamiliar with the configuration are often tasked with attempting to onboard the device with provided instructions to verify that the customer will be able to do it themselves. In addition, corporate-level security teams also test the devices through the onboarding process to ensure that security policies are being upheld. Business units are then trained to be equipped with platform- and customer-specific onboarding knowledge.

"A significant part of business engagements is insuring our teams are trained in the current infrastructure. This is a significant time commitment that's unavoidable right now."
– IoT Solutions Architect, Major Smart Building Device Manufacturer

Because Intel® SDO can be compatible with virtually all IoT devices (Intel and non-Intel processors and devices) and can be integrated seamlessly in varying customer environments, these steps are eliminated altogether. Once the Intel® SDO solution and Intel® EPID are enabled by device manufacturers, ODMs can develop devices efficiently to meet a wide variety of customer needs.

INTEL® SDO ONBOARDING PROCESSES FOR END USERS AND THEIR INSTALLERS

Manually onboarding headless IoT devices can only be as successful as those responsible for the integration. Due to varying priorities among departments, conflict often arises between the multiple parties involved. While IT departments focus on taking the necessary security precautions, operations and end users are more concerned with getting devices up and running as quickly as possible, opening the door to compromise. With an onboarding process that takes an average of 20 minutes, tension between groups is often unavoidable. Intel® SDO eliminates this tension by upholding security standards with Intel® EPID identity features and eliminating the manual, arduous onboarding process that frustrates operations and end users.

Claiming the device is a part of the process that often causes significant frustration for customers. To complete this step, customers must claim the device by manually entering information from the device into a web-based application or calling a 1-800 number to directly contact the device manufacturer. This process step can take anywhere from 10 minutes to over a day to get in touch with the right representative and complete. Intel® SDO removes this responsibility from the end user. The device is tracked while maintaining privacy as it changes ownership during distribution with a proxy. Intel® EPID authenticates platform identity through remote attestation using asymmetric cryptography. The process is entirely automated.

"Any time you have an opportunity during provisioning process with someone having to type something in you are setting yourself up for failure."
– Senior Systems Architect, Major Industrial Manufacturer

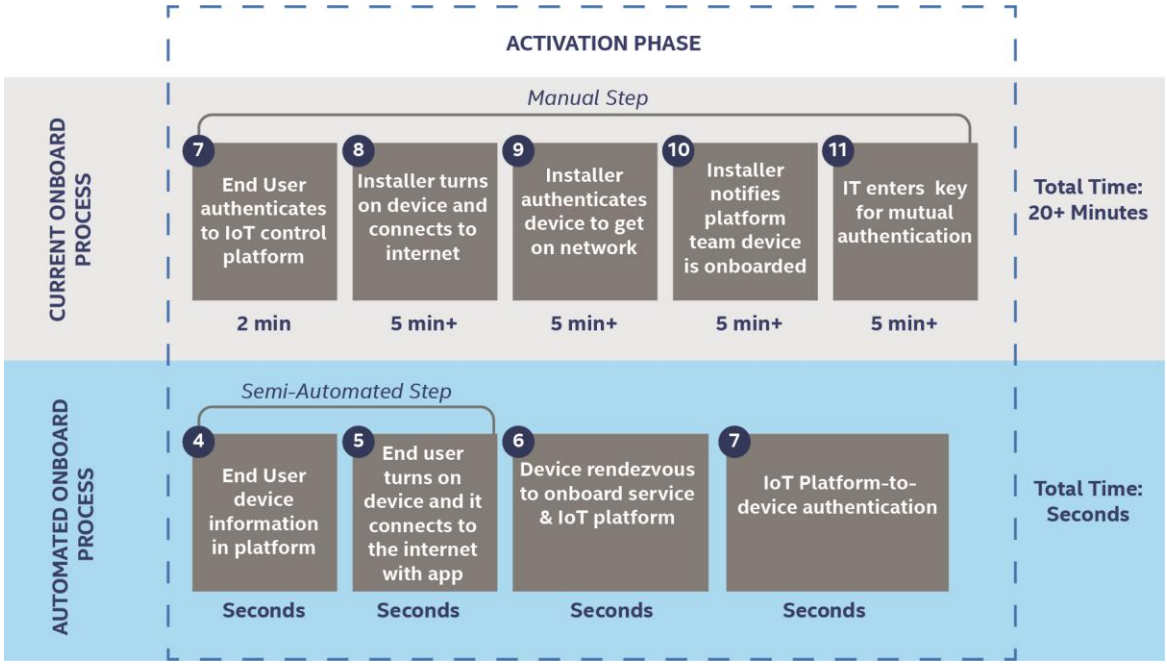


Figure 2

Intel®'s SDO solution decreases the onboarding and authentication process for customers from 20 minutes to mere seconds

STANDARDIZATION WITH THE FLEXIBILITY FOR CUSTOMIZATION

Although devices with Intel® EPID and Intel® SDO are standardized to be onboarded in any environment and to any platform, these devices can still be configured with different images during the agent provisioning phased once onboarding is completed. Rather than having to download drivers for every cloud manager, devices can be programmed to download agent drivers automatically after onboarding and mutual authentication are completed. Intel® SDO enables customers to onboard devices efficiently while also possessing the capability to customize devices to best meet customer needs.

"There's a big difference between onboarding legacy machines and onboarding newly designed devices. Each requires significant variation in configuration, but they all need to connect. Interoperability is key."

– Senior Systems Architect, Major Industrial Manufacturer

Interoperability and Integration For Industrials

Capturing and analyzing data from industrial machines has created the ability to attain new insights and enable predictive maintenance for factories and manufacturing plants. Ranging from long-standing, mom-and-pop factories to newer, high-tech manufacturing facilities, industrial companies can highly benefit from the utilization of IoT. Unfortunately, this variation requires a wide range of configurations from ODMs to enable interoperability. With the ability to be utilized in a wide variety of products, machinery, and devices, ODMs can bypass unique configuration and differentiate themselves in this market with quick and easy onboarding processes. Intel® SDO and Intel® EPID enable interoperability amongst all aspects of the production process and a smooth transition from simple manufacturing to smart automated operations.

FEATURES AND BENEFITS: SECURITY WITHOUT COMPLEXITY

SEAMLESS ONBOARDING WITH THE STRONGEST LEVEL OF SECURITY

Regardless of the use case, security is top-of-mind for adopters of IoT solutions. Intel® SDO offers an onboarding solution that is not only efficient, but one that is also more secure than other solutions on the market. With Intel® EPID, a single public key can have millions of private keys, maintaining the anonymity of the device and its user. As the foundation for Intel®'s hardware-enhance security technologies, more than 2.5 billion Intel® EPID credentials have been issued in the past 10 years.[2]

"To convince companies to automate their buildings, we have to demonstrate our ability to do it securely."

– UX/UI Development Manager, Major Healthcare Device Manufacturer

TRACKING THROUGH DISTRIBUTION SECURELY

Unlike the current distribution process in which devices are tracked with paper bills of lading and RFID scanning, Intel® SDO enables device manufacturers and distributors to track ownership of the device while maintaining privacy by providing a temporary proxy that cryptographically signs for ownership at each step of the distribution process. The signature chain of each owner is loaded into the IoT platform which is used to trace back ownership to the Intel® EPID key in the device. At the end of the distribution process, the customer enters the proxy to notify Intel® SDO's onboarding service of the customer's IP address. Intel® SDO's service stores this information so that it can automatically provision the device when the device is turned on. [3]

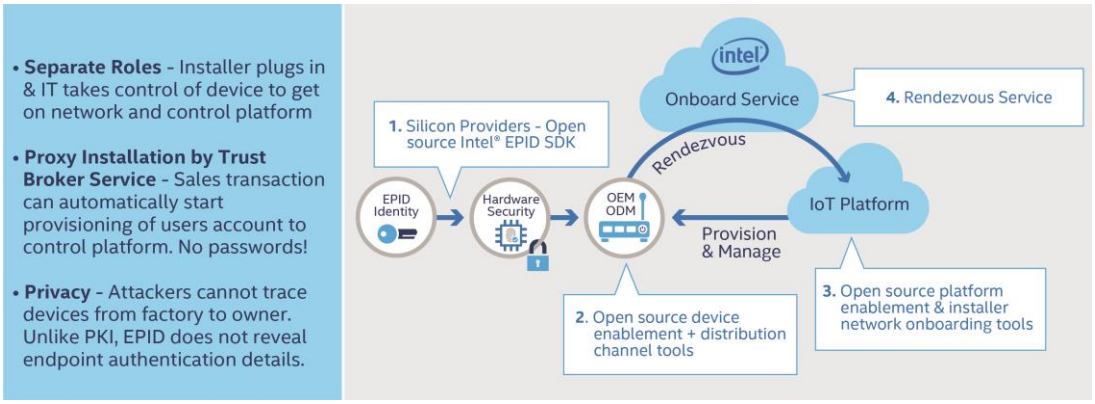
Smart Buildings and the Importance of Security

In 2013 hackers accessed personal information of millions of Target customers through network credentials stolen from the company's HVAC provider, shedding light on the vulnerability associated with bringing building appliances and equipment onto the cloud. With a heightened awareness of security after this incident, customers in this industry vertical have been acutely aware of the risks of storing proprietary data in the cloud. In addition, smart buildings often require hundreds, if not thousands, of devices to be configured, onboarded, and provisioned at once, leading to excessively long periods of time to onboard them in a secure way.

Intel® EPID and Intel®SDO provide the most secure way to onboard devices in automated buildings efficiently. With its "one to many" model, Intel® provides a solution to customers that maintains high levels of security while stripping away tedious onboarding steps.

"Everyone in our first meetings is concerned with security, but when it comes to actually onboarding devices people get impatient. They want it to be implemented quickly so they skimp on the security and they don't see the consequences of this until it's too late."

– Senior Systems Architect, Major Industrial Manufacturer



BUILT-IN STANDARDIZED SECURITY ENABLES END USERS TO FOCUS ON WHAT IS IMPORTANT TO THEM

To ensure devices are onboarded securely, customers are often faced with numerous hurdles and barriers to configure and provision their devices. Despite initial concern over—and prioritization of—security, customers often strip away security features to alleviate the burden inflicted by security hurdles. The result is easily accessible or exposed device identities and the risk of hacking.

Security must be interoperable, affordable, and easily activated to ensure customers maintain the privacy of their devices. Intel® SDO eliminates obstacles associated with security. Its seamless approach combined with Intel® EPID's security features create a solution that meets a core customer need.

"Every time you see a positive update about connected devices, it's immediately followed by a story about hacking. Security is our top priority, and it should be our end users' too."

– Senior Systems Architect, Major Industrial Manufacturer

Healthcare Regulations and the Ability to Streamline Preparation Processes

While hospitals and the healthcare industry are taking advantage of the various benefits of IoT platforms and devices, they are highly aware of the compliance requirements associated with protected health information (PHI). When implementing IoT devices and processes, customers prioritize data security and privacy in order to comply. Lack of trust, standardization, and information results in reluctant IT departments and business partners in this industry.

Intel®'s SDO solution bypasses the bureaucracy present in this industry vertical by positioning device manufacturers to offer devices that are securely onboarded and easily activated. Configuring devices to unique platforms and device integration needs should not be an added headache for device manufacturers and end users. Intel®'s SDO solution removes this step, allowing manufacturers and hospitals to focus on what's most important.

INTEL® SDO ADVANTAGE: HIGH SECURITY WITH LOW COMPLEXITY

In order for organizations to receive the benefits of utilizing IoT devices, solutions must be interoperable, secure, and deployed effectively. Currently, onboarding processes pose a barrier to easy adoption. Intel® SDO offers a solution that upholds the highest security standards and decreases the complexity associated with device configuration and onboarding. By automating the onboarding process, Intel® SDO opens up a path to reaching the 2020 vision for IoT devices.

FOR MORE INFORMATION ON INTEL® EPID, the INTEL® SECURE DEVICE ONBOARD SOLUTION visit www.intel.com/securedeviceonboard . FOR partner program questions, EMAIL **iotonboarding@intel.com**

SOURCES

[1] **How the 'Internet of Things' Will Impact Consumers, Businesses, and Governments in 2016 and Beyond.** http://www.businessinsider.com/how-the-internet-of-things-market-will-grow-2014-10**.** Accessed January 26, 2017

[2] **EPID: Enhanced Privacy ID. Intel®'s algorithm for attestation of a trusted system while preserving privacy**. For more information on Intel® EPID, please see: https://software.intel.com/en-us/node/702985

[3] **A Cost-Effective Foundation for End-to-End IoT Security.** Intel® IoT Security**.** Accessed January 26, 2017

ABOUT KAISER

Founded in 1981, Kaiser Associates is an international strategy consulting firm that serves as a key advisor to the world's leading companies. We provide our clients with the unique insights to driver critical decision making and solve their most pressing problems.

Kaiser's Technology Practice advises clients whose businesses span the whole stack from infrastructure and operating systems to gaming and analytics using a unique blend of quantitative analytics fueled by a best-in-class primary research capability. Kaiser's projects typically center on market opportunity assessments and competitive landscape understanding in hardware, software, and services, with substantial concentration in IoT and cloud topics.

ABOUT THE AUTHORS

John Wilhelm

John is a Senior Vice President in Kaiser Associates' Technology Practice based in Washington, D.C.

You may contact him by email at jwilhelm@kaiserassociates.com

Jeremy Williams

Jeremy is a Principal in Kaiser Associates' Technology Practice based in San Francisco, CA.

You may contact him by email at jwilliams@kaiserassociates.com

Sarah Macy

Sarah is a Consultant at Kaiser Associates based in Washington, D.C.

You may contact her by email at smacy@kaiserassociates.com