DEMO BRIEF

IoT

Zero Touch Onboarding for IoT

"Marshal Point" - An EPID Enhanced Privacy ID POC
Enable your IoT solutions to automate, secure, and scale device registration

Secure device on-boarding requires a trust chain that spans device manufacturing, distribution, to IoT platform control. Intel is in a position to solve this for the industry.

- Security Analyst

Device Onboarding - an Unsolved Problem

Today, the onboarding process for IoT typically takes over 20 minutes per device. This involves coordination among installation techs, network admins, and IoT operations. This high cost, manual process will hold the industry back from the promise of billions of connected devices. The core challenges include: device identification, preserving ownership/data privacy across the distribution lifecycle, secure communications from edge to cloud, and configuration on the IoT platform's network/registration systems.

Marshal Point POC

Intel® is leading a Proof-of-Concept (POC) with the IoT ecosystem to craft protocols and reference code for use by silicon providers, device manufacturers (from sensor to gateways), IoT Platform providers, and industry standards organizations. Intel and other silicon providers are spearheading this initiative because baseline trust must be established using the device hardware's trusted execution environment (TEE) as a pre-cursor step before provisioning and managing the device from any IoT platform.

Core Benefits of Ecosystem Adoption

- **Automation for Scale and ROI** - Instrument IoT solutions to participate in a streamlined onboarding process> from 20 minutes to under 20 seconds.
- **Standards Based** - both EPID and Marshal Point clients are available as Open Source.
- **Security & Privacy** - Leverage the unique anonymity and group authentication properties of EPID to ensure malware cannot build threat maps of where devices are being deployed for DNS attacks.
- **Ownership Receipt** - Track the device while maintaining privacy as it changes ownership during distribution. Provide a rendezvous point in the IoT platform where the owner can claim the device.
- **Power, Place, Provision** - Address a core customer need and deliver a competitive advantage for your IoT solution with a zero touch onboarding solution.

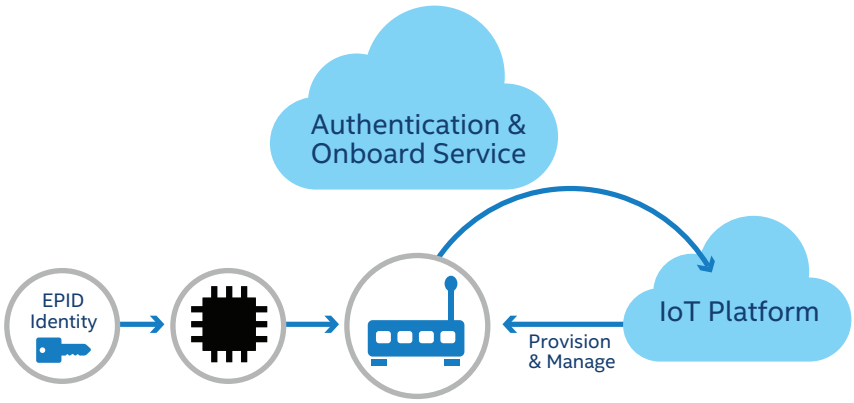


Figure 1:
Power, Place, Provision at Scale

Core On-boarding Scenario
(Elaboration of Demo Use Case - Figure 2)

1. **Silicon Provider** - Microchip embedded an EPID identity in the silicon's TEE at manufacturing utilizing the EPID 2.0 open source SDK
2. **Gateway/Device** - Dell used the Marshal Point client software in boot code to support a direct anonymous attestation communication channel to the IoT platform which passes the device GUID, rendezvous point URL, and digital ownership credential.
3. **End Owner** - After the distribution change of ownership, the final owner uploaded the box GUID and digital ownership receipt received via email to the Microsoft Azure IoT platform.
4. **IoT Platform** - Azure integrated its Platform registration system with the Marshal Point SDK/API and contacted the Marshal Point broker service with its rendezvous IP address for the device.
5. **Power Up** - Device plugged in and phones home to Marshal Point trust brokerage service to prove authenticity and received rendezvous URL where it meets new owner.
6. **IoT Trust Established** - Device and new owner mutually authenticated using EPID and the IoT platform can commence to provision normal management agents to the device and can update the secure connection with its choice of PKI credentials

Enable Your IoT Solutions for Scale & New Revenues

The Marshal Point initiative has been designed from the ground up to mitigate the risk of attacks to a device, to ensure privacy, and to deliver automation that dramatically reduces onboarding time to seconds. Alternative, traditional PKI based identity schemes retrofitted for IoT are destined for slow adoption that will inhibit IoT solution provider growth. By adopting, an EPID based approach, IoT solution providers gain transparency through open source, a proven security standard, and unleash a new capability that addresses customer demands for IoT security and scale. Since 2008, Intel has leveraged EPID to attest platform integrity & manage billions of embedded device identities.

Marshal Point provides the essential software components and trust brokerage services that each IoT ecosystem player will need to incorporate into their IoT portfolio. (See Figure 3).

Figure 2:
Marshal Point - EPID in use

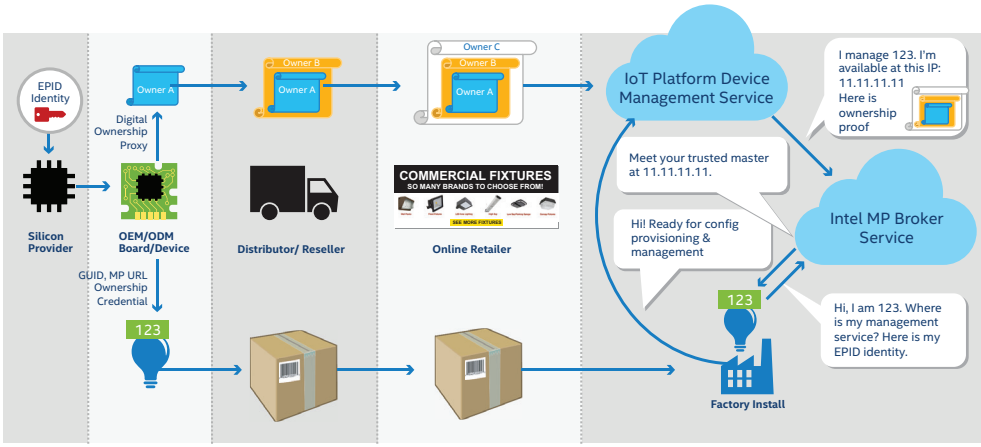
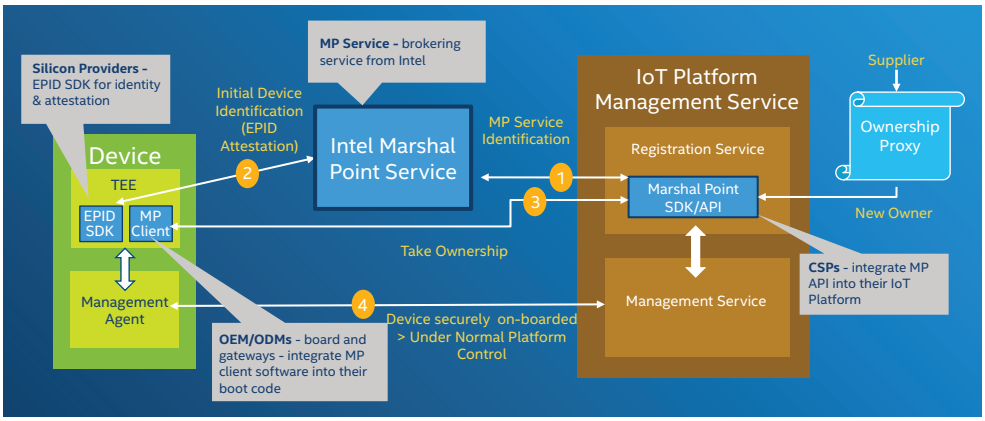


Figure 3:
Ecosystem enablement.
Blue = MP Intel software



To learn more about how to enable your IoT solution for EPID or to participate in the POC, contact iotonboarding@intel.com.

Learn more about EPID at www.intel.com/content/www/us/en/internet-of-things/iot-security.html