SECURITY
INDUSTRIAL IOT

Software and Services Group
IoT Developer Relations, Intel

SECURITY IS CRITICAL

Connecting “things” to the Internet that have never been connected is valuable, but also introduces risk. - Source: McAfee Labs Q1 ‘14

46%	Increase in new malicious signed binaries
236	New threats every minute, or almost four every seconds
49%	Growth in new threats attacking the master boot record and an all-time high for a single quarter

> *“The ability to attack will outpace the ability to defend.”*
>
> *—Rand Group*

> *"It takes 20 years to build a reputation and **five minutes to ruin it**. If you think about that, you'll do things differently.“*
>
> *—Warren Buffet on Target Corp*

PROTECTING THE EXECUTION, STORAGE, AND TRANSFER OF DATA

1. **Security built into the hardware:** Hardware integrity must be enforced to ensure the device has not been altered.
2. **Secures OS and applications:** The gateway itself must have a secure operating system to ensure that data is safely stored.
3. **Secures data from chip to cloud:** Data must be transmitted securely from sensor to data center, even when one or more gateways must process it on the way.
4. **Enabling ecosystem security:** Standardized Intel solutions allow augmented security with third-party solutions.

Security and privacy are the top two inhibitors of the success of IoT deployments.
Recent survey of more than 450 IT and business leaders[1]

From the Field

- A lack of security in implanted **medical devices** opens the door for malicious activity that could put patient health at risk.
- **Industrial devices**, if tampered with, can leak sensitive operational data.
- Hackers may breach **retail devices** to gain insight into sales patterns, change prices, or hide inventory.

LOOKING AHEAD IN 2018 – USGOV IOT/CYBER SECURITY

- Protecting your own IT & OT Networks is critical for brand and security excellence
- Cyberthreats by nation states, including Russia, China, Iran & N Korea lead threat assessment
- DARPA has released several broad agency announcements (BAA/RFQ), seeking innovative IoT/Cyber solutions. 74 DARPA budget activities, totaling $856M[1] related to IOT and Cyber in 2018.
- USGov funding IoT/Cybersecurity over $5B[1] in 2018 budgets.
- Fastest BAA's ever:
  - Urgent call for securing SCADA system at international waste water giant on US side of Mexico border is due Sep 29 (only $1M).
  - Anti-phishing BAA HR001117S0050 was posted 9/11, abstract due 9/19 and bid 11/9. Bid must include best practices in bots & whitelisting, AI for zero day and for honey pots to collect attacker info .

1. Per Bloomberg Gov Analyst, at IoT/CyberSecurity Summit Sep 27.

IOT SECURITY IS ESSENTIAL TO SCALE IOT DEPLOYMENTS

HW SECURITY IS AN IOT PRIORITY

#1 Barrier to IoT Adoption* Gartner

Hackers exploiting poor device security

Mirai Botnet!

Isolation & added protections of HW security has recognized role

NEW SPECS

Pattern to secure & role of HW is defined

CUSTOMER REQUIREMENT

HW security moving from shadows to key RFP request

Security solutions Designed-in to HW are keys to accelerating adoption and scale

**Gartner 2016 IoT Backbone Survey*

**Trusted Computing Group: What Embedded and IoT Developers Think About IoT Security*

PROTECTED BOOT TYPES

ROOT OF TRUST

A set of hardware, firmware, and/or software that is inherently trusted to perform a vital security function **(NIST Definition)**

through Secure Boot/UEFI Secure Boot
BIOS security standard that prevents use of unauthorized option ROMs, and ensures the next stage of the boot is “authorized

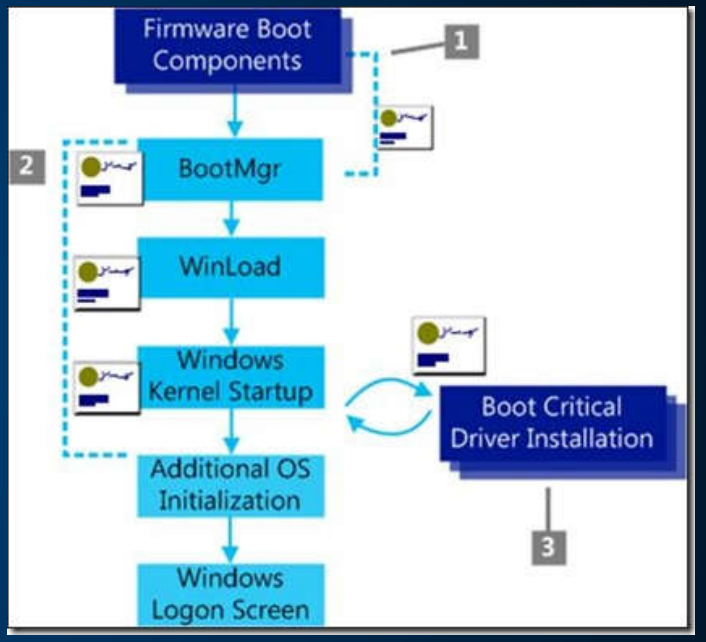
SECURE BOOT

Boot process where each stage of the boot is cryptographically verified by the previous stage; a failure in the any verification causes the boot to fail.

MEASURED BOOT

Boot process where each stage of the boot is measured, usually by a cryptographic hash, and the measurements are stored for later comparison to known good values.”.

WINDOWS SECURE VERIFIED BOOT PROCESS



http://blogs.msdn.com/b/olivnie/archive/2013/01/09/windows-8-trusted-boot-secure-boot-measured-boot.aspx

INTEL® PLATFORM TRUST TECHNOLOGY: PROTECTED STORAGE

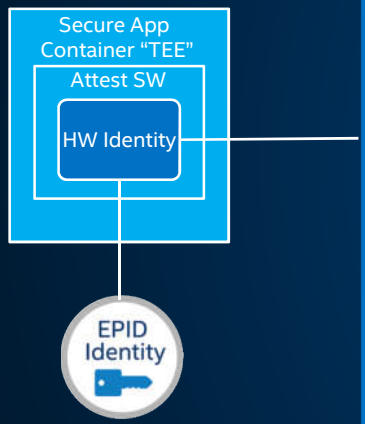
Intel® PTT is a hardware TPM 2.0 implementation for credential storage and key management across Atom, Core and Xeon. **Benefits:**

- A secure trust element to meet requirements for TPM 2.0 and Measured Boot for systems on which TPM 2.0 is required.
- Integrated solution
- Compliance with: TCG specifications, TPM Profile commands, EK cert provisioning, ECC, SHA2, Windows 10 requirements
- Protects: anti-replay, dictionary attack
- Key protection technology for distributed HW Security Module (HSM)
- Reduction in BOM cost and board savings as compared to a discrete TPM, or use with a Discrete TPM (for geo or vendor-specific)

- This is have existing installations can perform TE

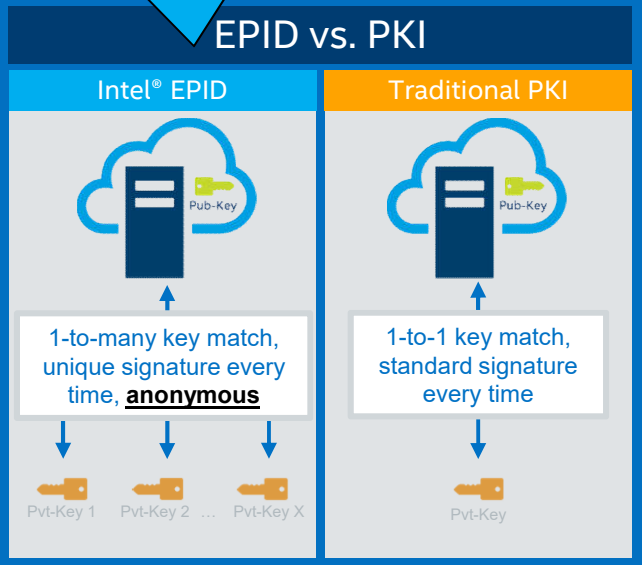
HARDWARE IDENTITY MANAGEMENT

Baseline Minimum HW Root of Trust



- Intel® Enhanced Privacy ID (Intel ® EPID)
- TCG/ISO standard with privacy preserving group authentication scheme
- Used to authenticate & open secure, authenticated channel for remote attestation
- Proven- 2.5 Billion keys fused into Intel processors since 2008. Intel® Xeon®, Intel® Core™, & Intel® Atom™
- Open source SDK
- Used by Intel solutions- SGX, DRM, IPT, Intel® Secure Device Onboard

Prevents Attack Mapping- Protects device data vs PKI that reveals data to hack device

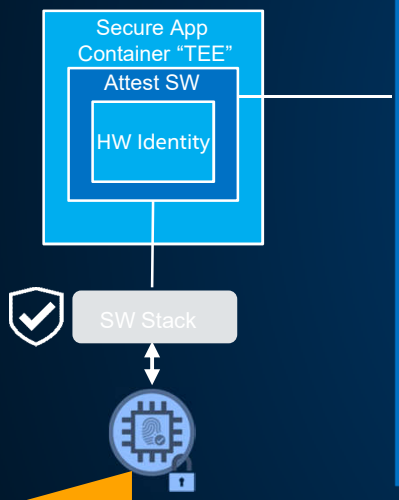


Enables Customers to deliver many use cases where privacy & attestation are key requirements

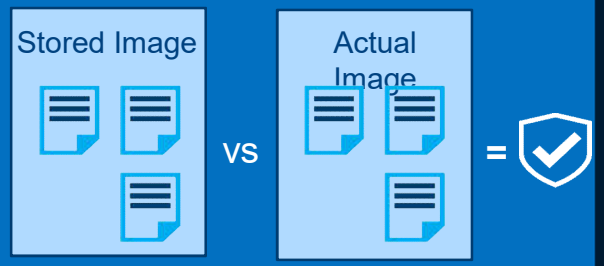
DESIGNED IN SECURITY FOUNDATION

SW IDENTIFICATION – FOR DEVICE "HEALTH" ATTESTATION

Baseline Minimum HW Root of Trust



- **Trusted Platform Module (TPM) -** on chip firmware to safely store credentials or (PCR) platform configuration registry values. Intel® Platform Trust Technology (Intel® PTT)
- **Protected Boot –** platform dependent capabilities to ensure firmware & OS are running trustworthy configuration
- **Remote Attestation -** "best." send both boot and app measurements to 3rd party that verifies device stack running is equal to predefined Trusted Configuration
- **White Listing -** "best." allowable agents/applications for that specific device- Intel helps manage ecosystem solutions

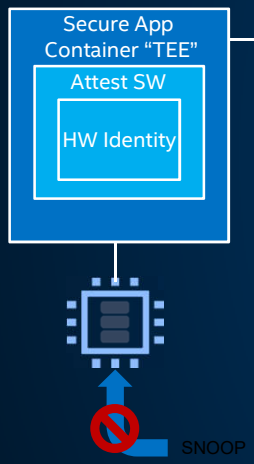


Enables Core Security capabilities available during lifetime
Utilization of "Health" Services through Device Management Platforms

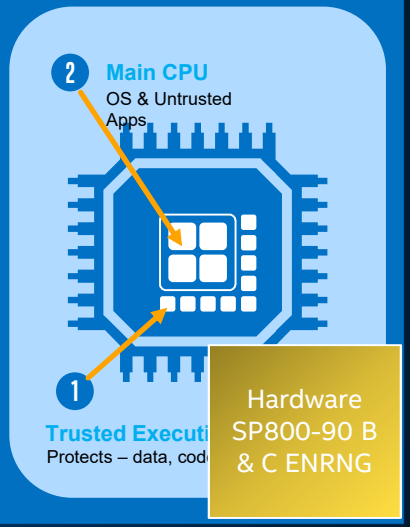
DESIGNED IN SECURITY FOUNDATION

5. TRUSTED EXECUTION TECHNOLOGY (TXT) & SECURITY ENGINES

Baseline Minimum HW Root of Trust



- **Crypto –** random # generator to create secure keys or apply message encryption - Intel® Secure Key, Intel® Advanced Encryption Standard New Instructions (Intel® AES NI)
- **Trusted Execution Environment (TEE) –** physical/logical separated processing. Only Intel signed apps run. Stored data sealed in protected memory- Intel® Software Guard Extensions (SGX), engines- Intel® Dynamic Application Loader applets
- **Usages** - secures keys for device comms, attestation, & authentication. Enables ISVs to provision & run app containers protected by hardware. Enforce code IP protection "DRM"



Intel delivers simple means to run multiple apps in our TEEs

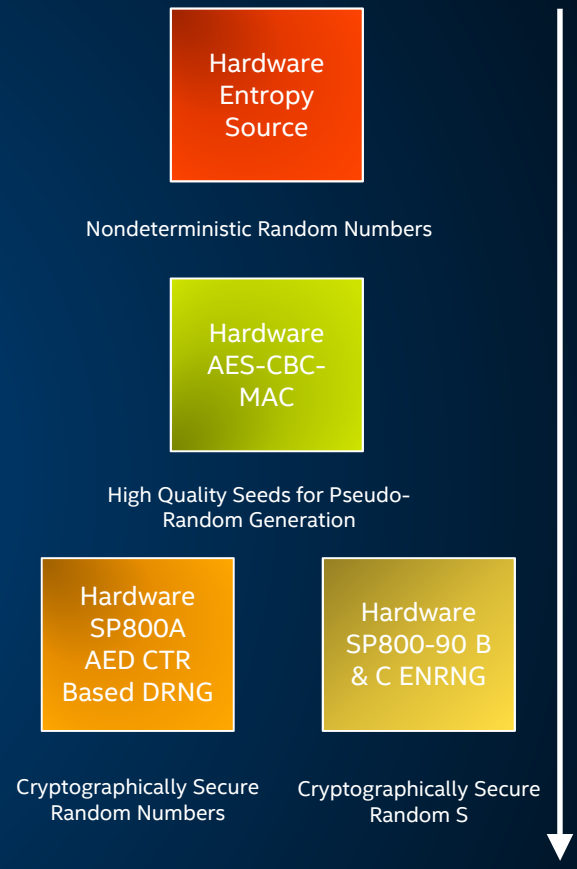
Lowers BOM costs & increases performance by using on chip vs discrete security co-processors

HW FEATURES FOR DATA PROTECTION

- AES Hardware Acceleration with AES-NI
  - Data Protection with Cryptographic Acceleration
  - AES-NI allows significant performance at a lower price point, no custom hardware.

- Hardware DRNG
  - Better Encryption Keys and Simulations with On-Board Digital Random Number Generator
  - Solves the problems of limited entropy in virtual platforms

Functions meet NIST SP800-90A, B & C: improving encryption of full disk, data at rest, in transit or transaction and app-level granularity

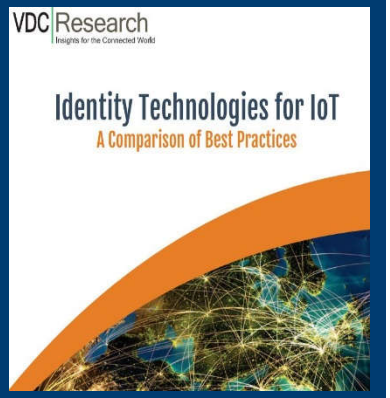


https://software.intel.com/en-us/articles/intel-digital-random-number-generator-drng-software-implementation-guide
https://csrc.nist.gov/publications/detail/sp/800-90a/archive/2012-01-23

EPID Comparison & whitepapers

	Key Strength	Provisioning	Key Distribution	Trust Model	Privacy	Scalability	Static vs. Dynamic	HWROT
X509 RSA	80-112 RSA	SW	TLS	HW + SW	○	1/Device	S	N
X509 ECDH	128-192	HW/FW	TLS (ATTEST depends on HW)	HW	○	1/Device	S	Y
E-SIM Card	Variable 80-192	FW	TLS/IKE	HW + SW	◗	1/SIM	S	Y
DICE	128-192	FW	ATTEST	HW + SW	○	1/Device	S	Y
EPID 2.0	128 ECC	HW	ATTEST	HW	●	1/Group= millions	Dyn	Y

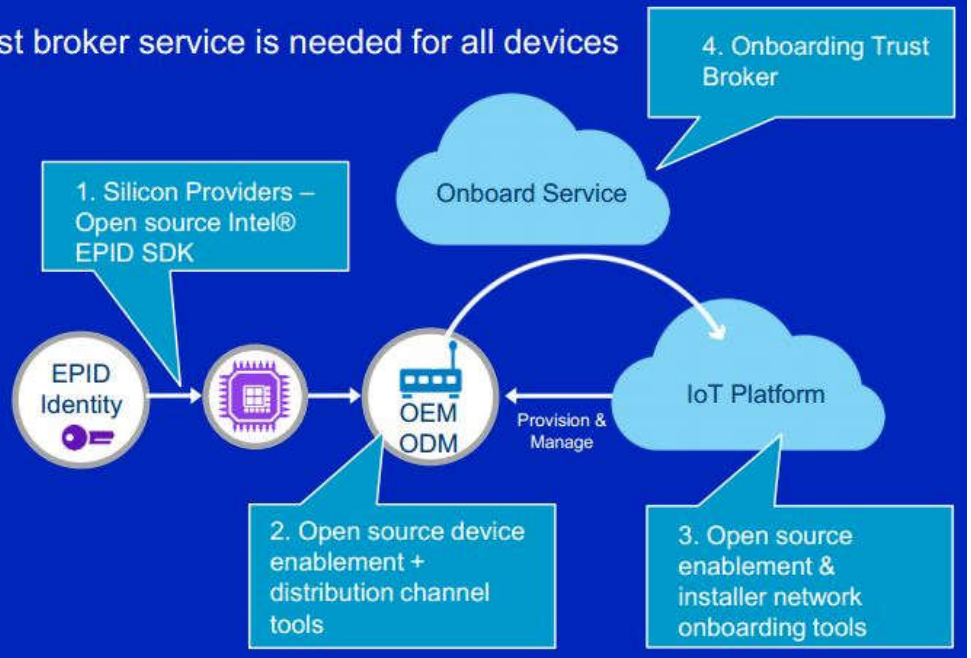
- Best practice for privacy oriented use cases like IoT device onboarding
- Post EPID authentication can swap for traditional PKI key
- Complementary to use in conjunction with other traditional PKI keys
- Post EPID authentication can swap for known identity



* www.intel.com/content/dam/www/public/us/en/documents/white-papers/**iot-identity-comparison-white-paper-vdc-research.pdf**
www.intel.com/content/dam/www/public/us/en/documents/white-papers/**intel-epid-white-paper.pdf**

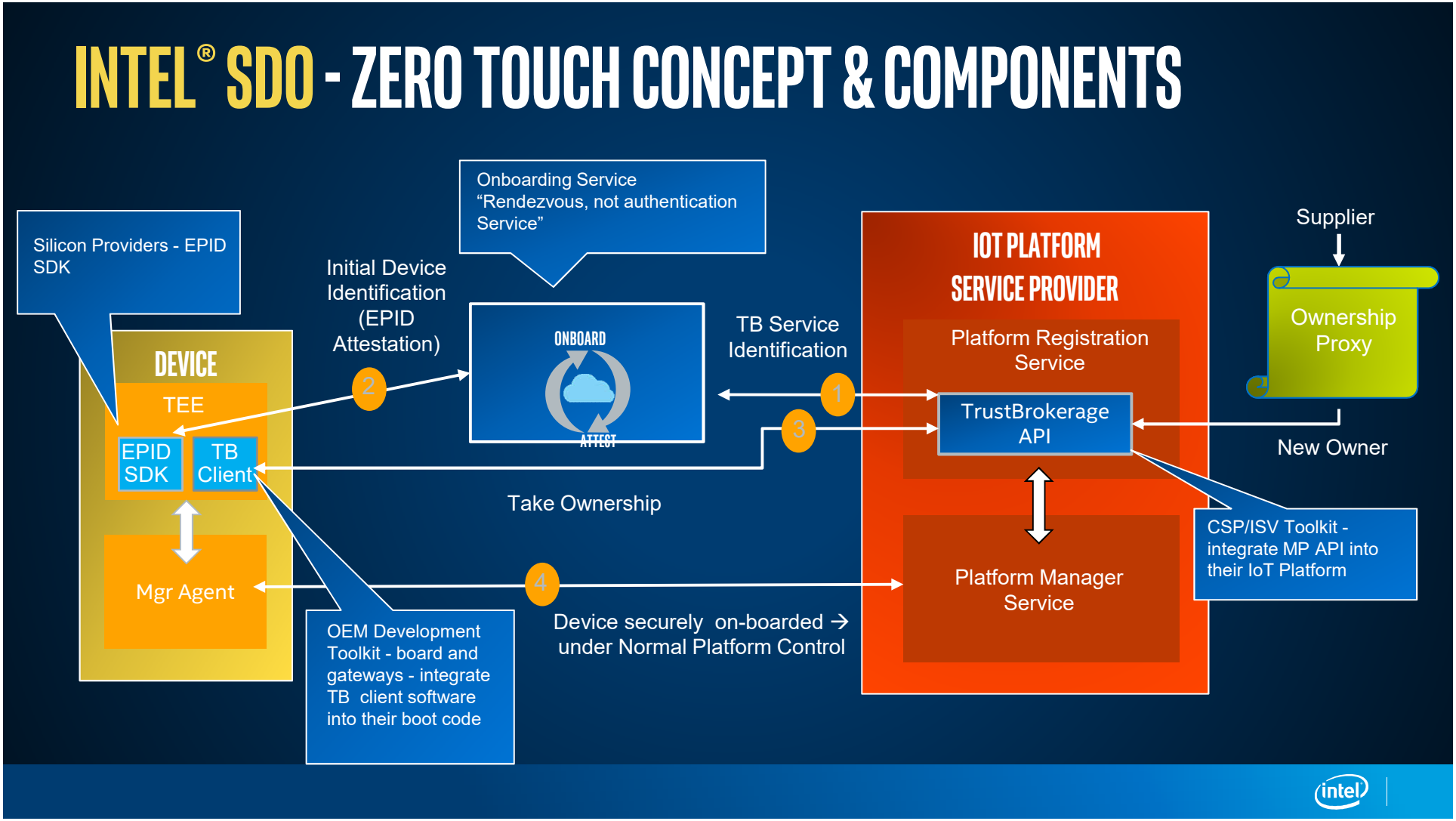
INTEL® SECURE DEVICE ONBOARD – ZERO TOUCH SERVICE

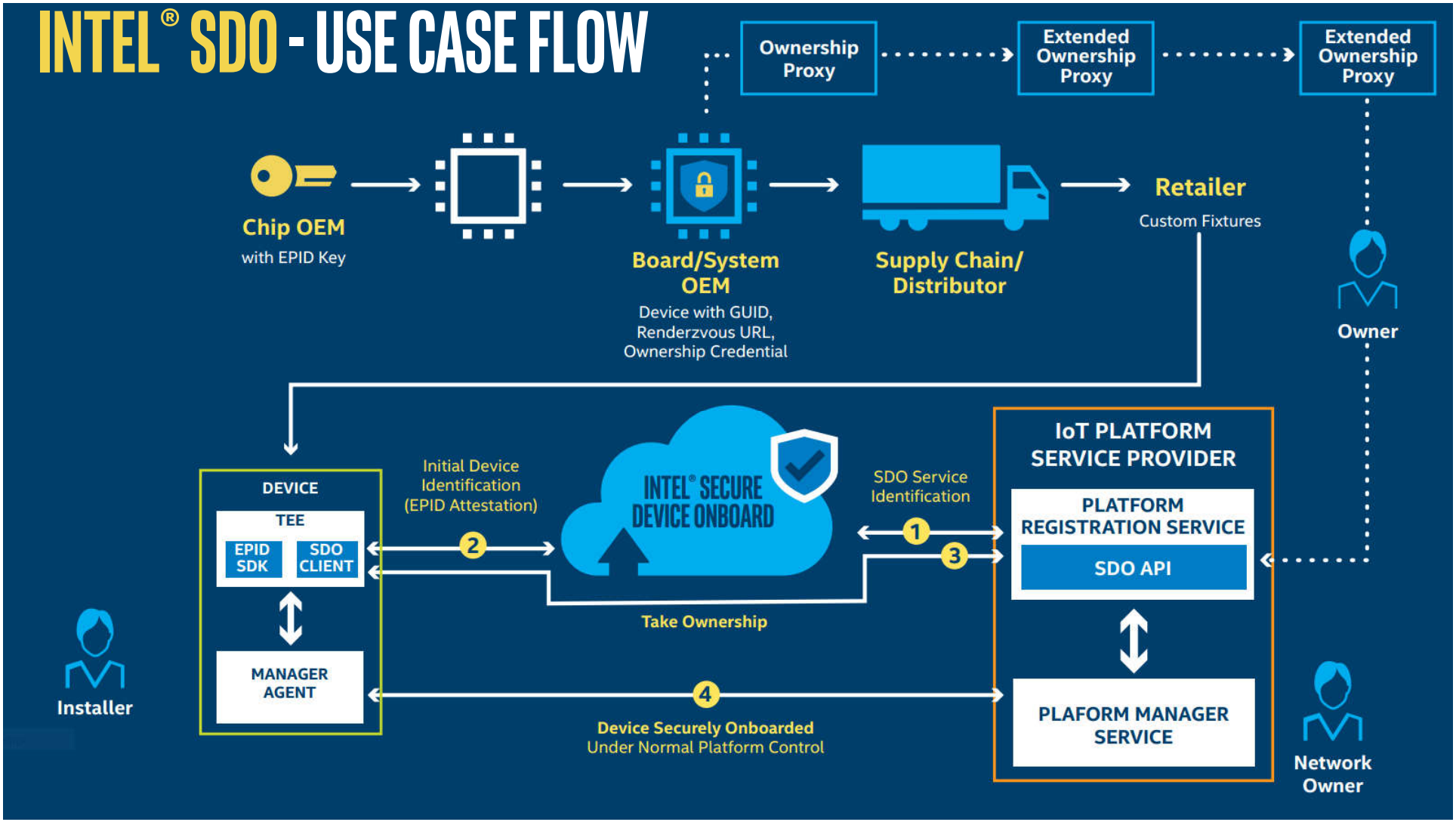
- **Separate Roles** – Installer plugs in & IT takes control of device to get on network and control platform
- **Proxy Installation by Trust Broker Service** – Sales transaction can automatically start provisioning of users account to control platform. No passwords!
- **Privacy** – Attackers cannot trace devices from factory to owner. Unlike PKI, EPID does not reveal endpoint authentication details.



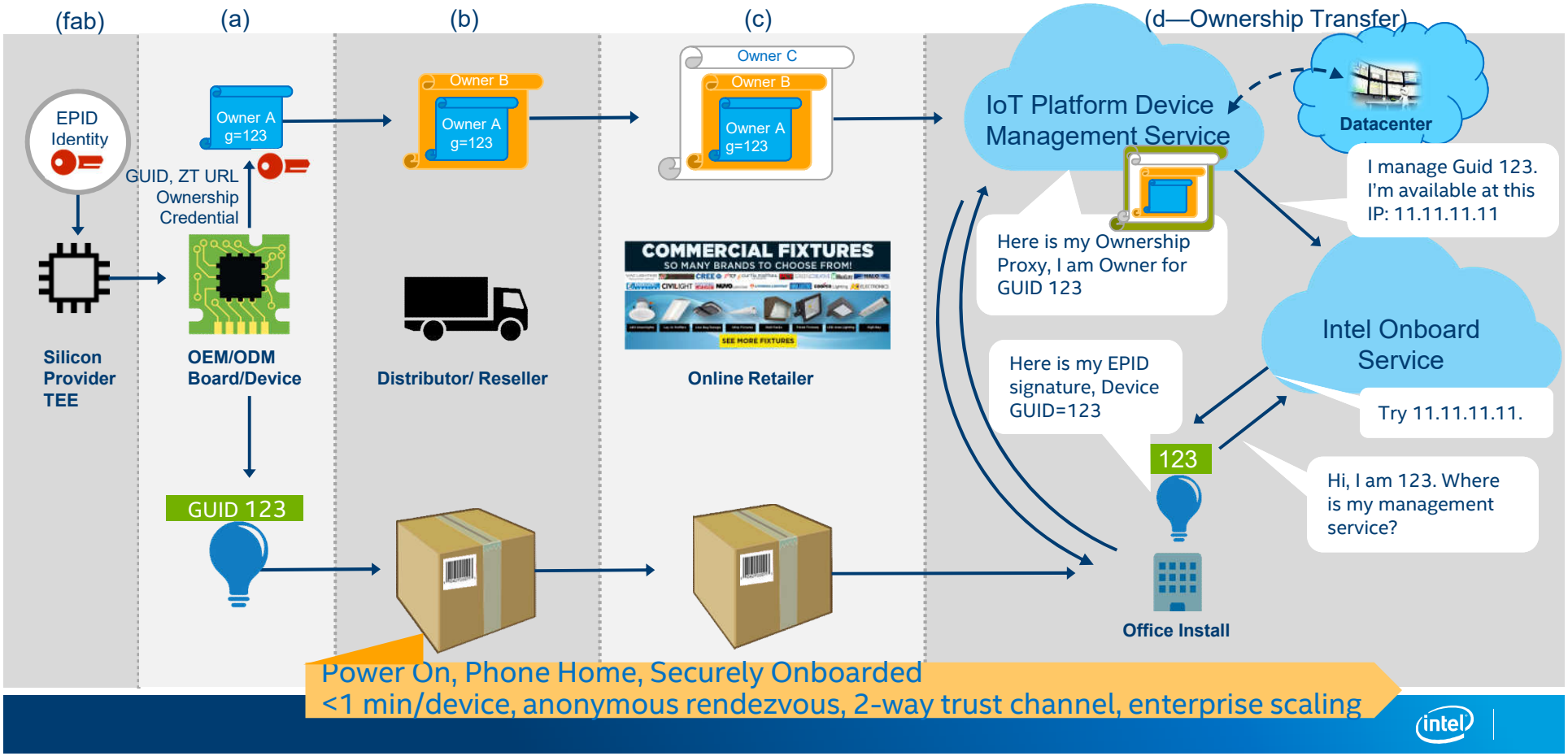
- Solves major pain point in securely deploying IoT “things”
- Manual deployment, staging, & OEM pre-loads are not optimal and causing deployment delays
- Hardware root of trust EPID based service for “0” touch device onboarding
- Tremendous ROI for customers & ecosystem
- Scale’s POCs to production. Increases number of devices in use

INTEL® SDO - ZERO TOUCH CONCEPT & COMPONENTS

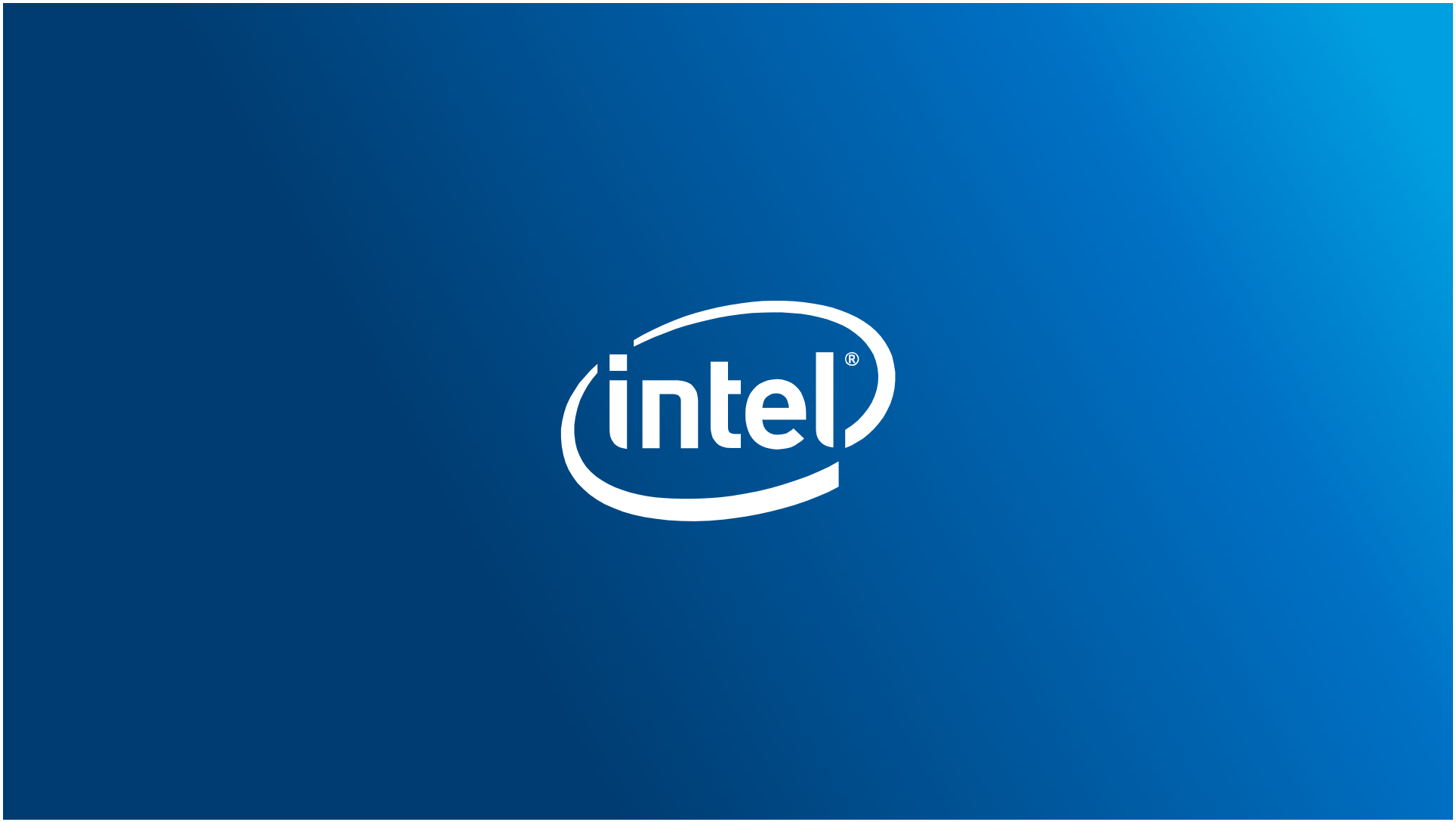



INTEL® SDO - USE CASE FLOW
Ownership Proxy
Extended Ownership Proxy
Extended Ownership Proxy
Chip OEM
with EPID Key
Board/System OEM
Device with GUID, Renderzvous URL, Ownership Credential
Supply Chain/ Distributor
Retailer
Custom Fixtures
Owner
DEVICE
TEE
EPID SDK
SDO CLIENT
MANAGER AGENT
Initial Device Identification (EPID Attestation)
2
INTEL® SECURE DEVICE ONBOARD
SDO Service Identification
1
3
Take Ownership
IoT PLATFORM SERVICE PROVIDER
PLATFORM REGISTRATION SERVICE
SDO API
PLAFORM MANAGER SERVICE
4
Device Securely Onboarded
Under Normal Platform Control
Installer
Network Owner

INTEL® SDO - ZERO TOUCH USE CASE FLOW



Lab


intel