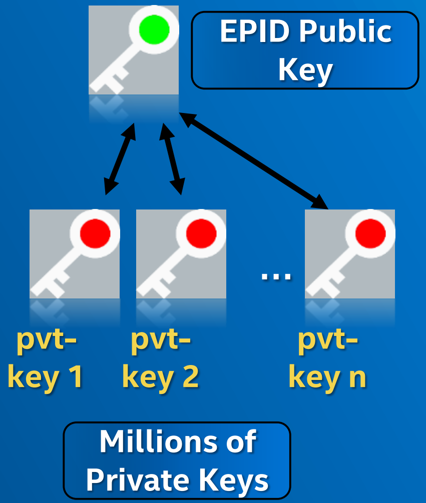
intel experience what's inside™

EPID for IoT Identity

Guy AlLee
Product Manager, IoT Security
Intel SSG, Platform Security Division

2016-Feb-08



Intel® Enhanced Privacy ID (EPID)

Enhanced Privacy ID is the leadership identity solution for IoT authentication

International Standard

- ISO/IEC 20008/20009 & TCG
- Privacy Preserving Anonymous Attestation

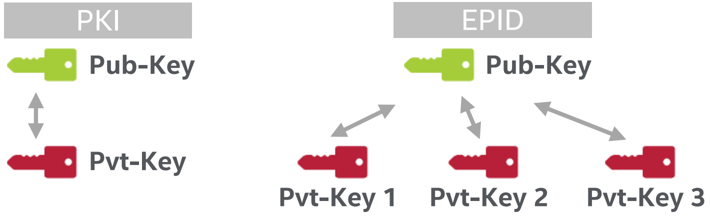
Mature Technology

- Shipping since 2008
- Xeon, Core 2011
- Atom, 2014 → sub-Atom
- 2.4B Keys since 2008

Utilization of EPID

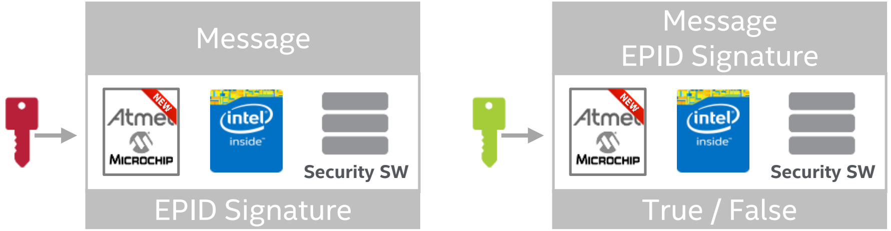
- Intel Insider (Digital Rights Management)
- Intel Trusted Execution Technology (Intel TXT)
- Intel Identity Protection Technology (Intel IPT)
- Intel Software Guard Extensions (Intel SGX)

Intel is Enabling the Industry on EPID



EPID is a digital signature scheme with special properties

- One Group public key corresponds to multiple private keys.
- Each unique private key can be used to generate a signature.
- Signature can be verified using the group public key.
- No one can tell which private key signed (privacy property).



Optimization Notice

Using EPID for IoT Identity

What is EPID

EPID is a digital signature technology that provides Direct Anonymous Attestation

- For EPID public key, many private keys (e.g., millions). The key holders form a group.
- Any key holder may sign against the one public key.
- No one can tell which private key signed the data. This is the privacy property.

EPID as Hardware Root of Trust

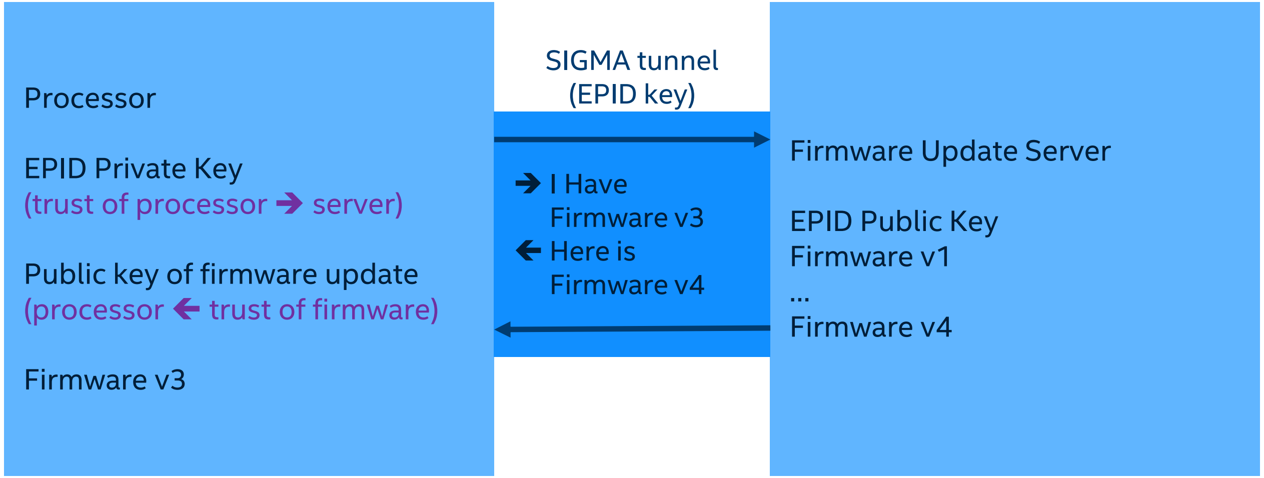
Intel provisions EPID keys in processors since 2011

Processor can open secure tunnel to provisioning server using EPID Sigma protocol. *This attests to genuine device*

Within this secure tunnel, processor can send specific information to perform device registration

Because of EPID anonymity property, devices cannot be traced using Internet monitoring

EPID for Processor Firmware (simple case)



Processor

EPID Private Key
(trust of processor ➔ server)

Public key of firmware update
(processor ➔ trust of firmware)

Firmware v3

SIGMA tunnel
(EPID key)

➔ I Have
Firmware v3
🡐 Here is
Firmware v4

Firmware Update Server

EPID Public Key
Firmware v1
…
Firmware v4

1. EPID key stored in hardware from device fabrication.

2. EPID key attests to genuine processor, but server does not know which processor (private).

3. EPID key is used to open a secure tunnel to the firmware update server (using SIGMA protocol).

4. Processor is genuine (EPID attestation), so firmware negotiation gets latest firmware.

5. Processor verifies update signature against public key stored in hardware (not EPID).

6. Processor installs firmware upgrade.

Current Uses: Intel Insider

Remote attestation to streaming service that secure Audio/Video path in PC

- EPID used to authenticate hardware has the required security to protect content
- Streaming services can rely on HW keeping content encrypted stream to display
- Higher definition content available and sooner

Send UltraViolet™ movies wirelessly to your TV,
thanks to Intel® Insider™ and Intel® Wireless Display²

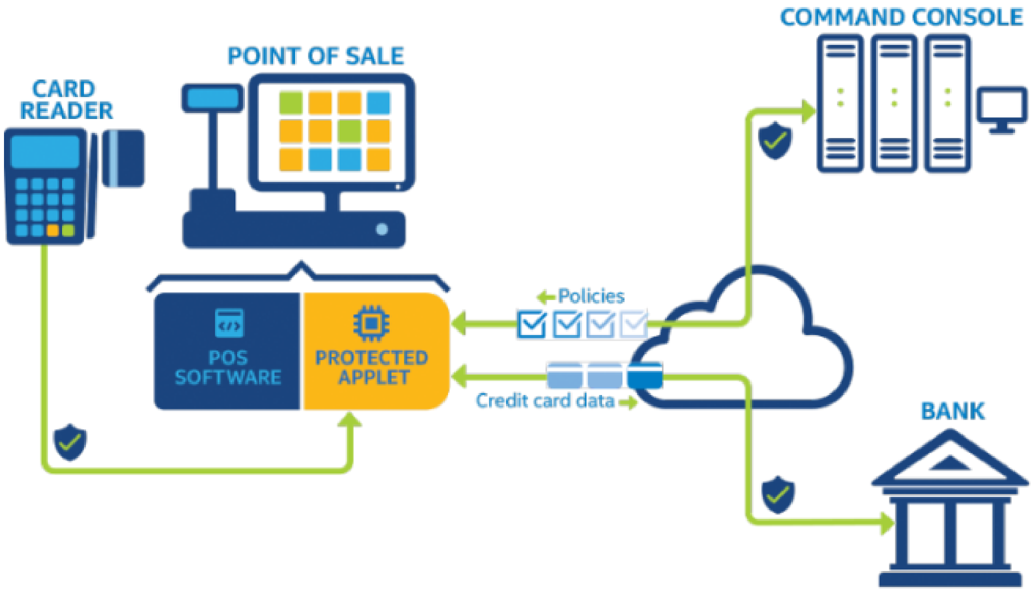
Intel® Insider™ Unlocks a World of UltraViolet* Entertainment

Unlock a world of premium UltraViolet* movies and entertainment with Intel® Insider™ to purchase, rent, and stream HD movies and entertainment wirelessly to your TV with Intel® Wireless Display.

Current Uses: DPT for Transactions

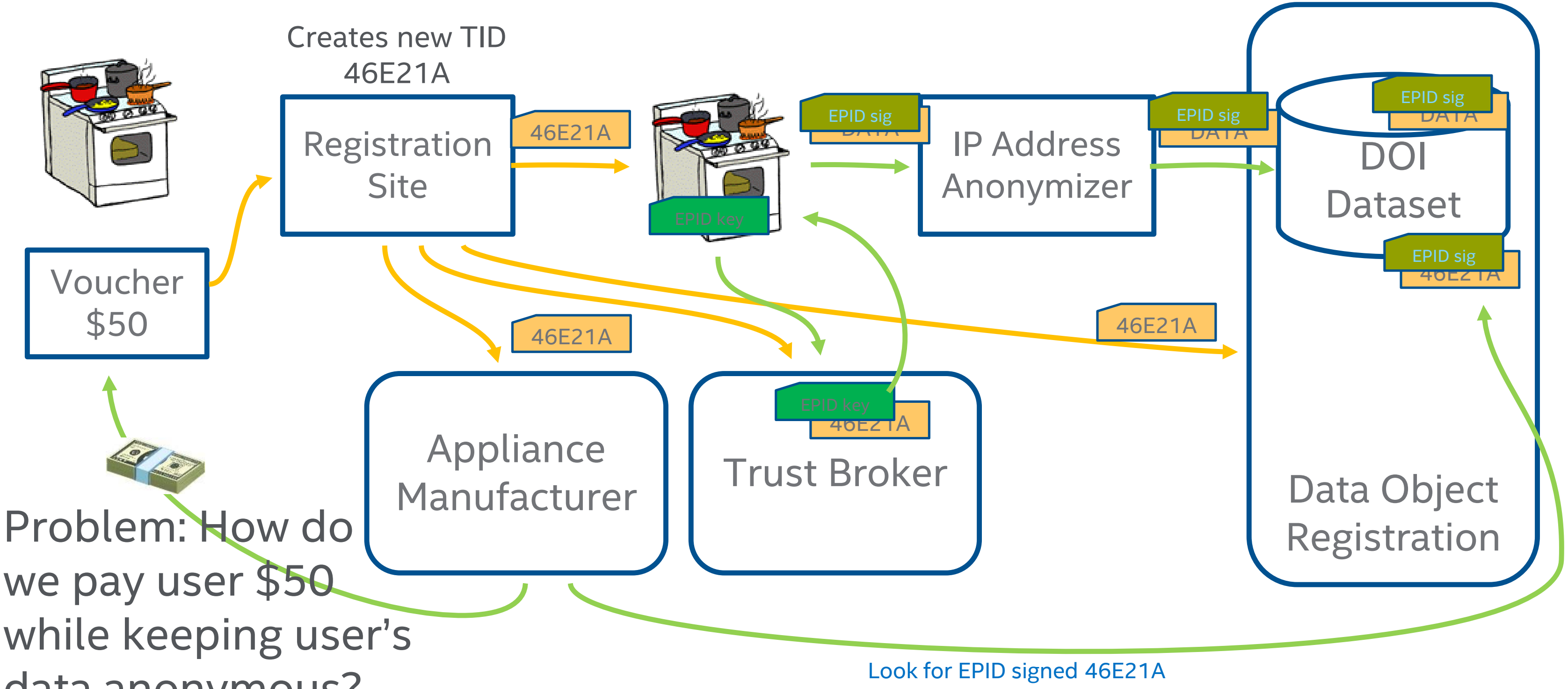
End-to-End security for credit card and personal data

- EPID used to authenticate Point of Sale (POS) terminal
- Banking Security Credentials provisioned to POS over secure tunnel
- Credit card and personal data encrypted from card reader to bank



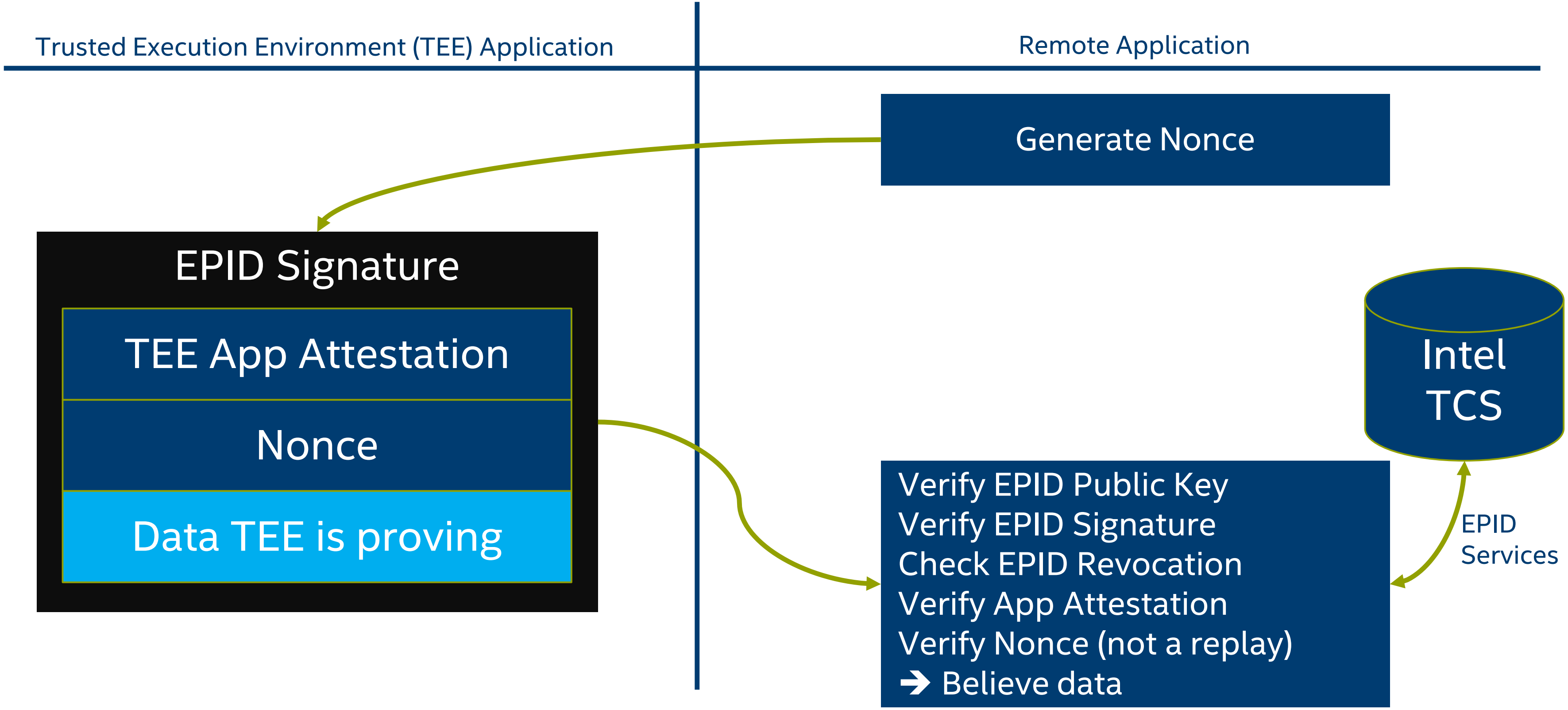
Optimization Notice

Appliance Example



Problem: How do we pay user $50 while keeping user's data anonymous?

How does it work? TEE Proof Example



Trusted Execution Environment (TEE) Application

Remote Application

Generate Nonce

EPID Signature

TEE App Attestation

Nonce

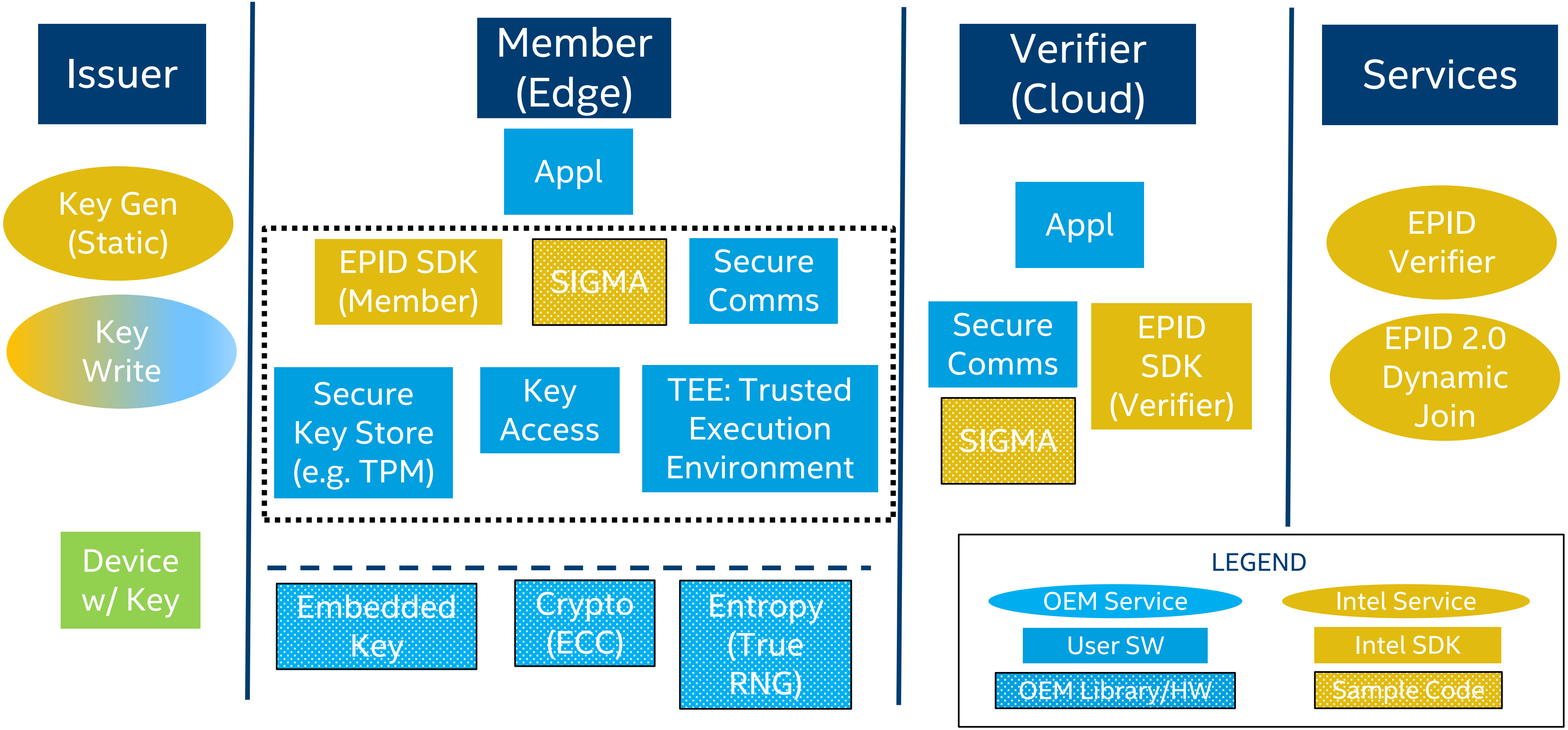
Data TEE is proving

Intel TCS

EPID Services

Verify EPID Public Key
Verify EPID Signature
Check EPID Revocation
Verify App Attestation
Verify Nonce (not a replay)
➔ Believe data

EPID/SIGMA Roles



Issuer

Key Gen (Static)

Key Write

Device w/ Key

Member (Edge)

Appl

EPID SDK (Member)

SIGMA

Secure Comms

Secure Key Store (e.g. TPM)

Key Access

TEE: Trusted Execution Environment

Embedded Key

Crypto (ECC)

Entropy (True RNG)

Verifier (Cloud)

Appl

Secure Comms

EPID SDK (Verifier)

SIGMA

Services

EPID Verifier

EPID 2.0 Dynamic Join

LEGEND

OEM Service

Intel Service

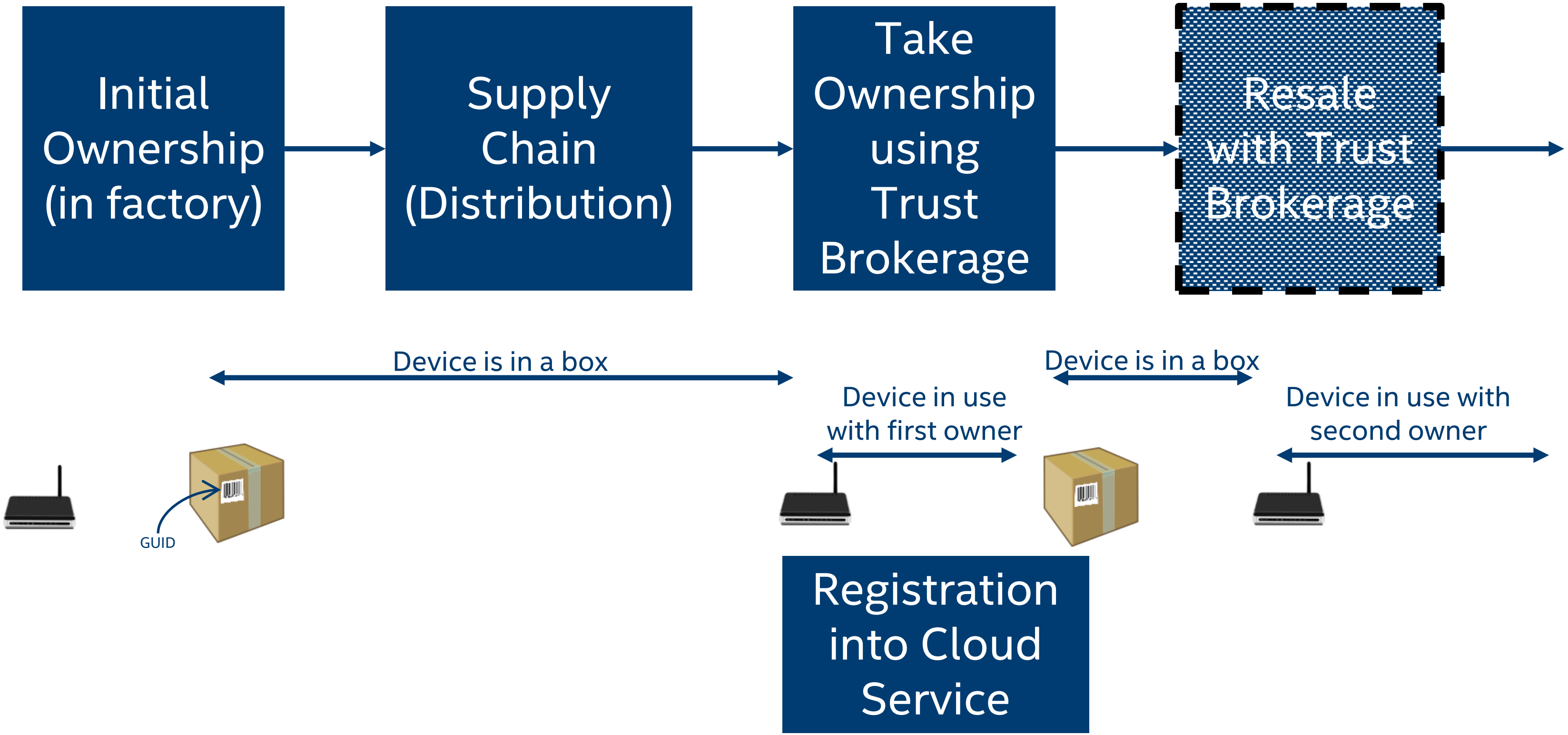
User SW

Intel SDK

OEM Library/HW

Sample Code

“Zero Touch” Device Registration & Provisioning



Initial Ownership (in factory)

Supply Chain (Distribution)

Take Ownership using Trust Brokerage

Resale with Trust Brokerage

Device is in a box

Device in use with first owner

Device is in a box

Device in use with second owner

GUID

Registration into Cloud Service

A Superior Out-of-Box IoT Customer Experience

“Zero Touch” provisioning concept

- Separate roles of installer / network controller
  - Installer: plugs in machine, verifies location
  - Network controller: takes control of device over network (NOC, cloud, etc.)
- Proxy Installation by Cloud Service
  - New device can be automatically provisioned to user’s account in a cloud service as part of the sales transaction. User doesn’t have to configure passwords, keys, GUIDs.

Privacy of Sales

- Adversary cannot trace devices from factory to owner to owner
  - Trace which products Company X owns
  - Where Manufacturer Y sells products
  - Global map of all infrastructure (e-warfare)

intel®

experience
what's inside™