Intel® Transparent Supply Chain process

Tom Dodson

Supply Chain Architect, Security Solutions

Legal Disclaimers

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at www.intel.com.

All products, computer systems, dates and figures specified are preliminary based on current expectations, and are subject to change without notice.

Intel, the Intel logo, and Intel vPro are trademarks of Intel Corporation or its subsidiaries in the United States and/or other countries.

*Other names and brands may be claimed as the property of others.

INTEL® Transparent Supply Chain introduction

- Intel® Transparent Supply Chain (“ITSC”) is a set of policies and procedures that enables component level traceability for selected Intel® systems.
- ITSC was developed to provide customers with Platform Certificates signed by Intel® and a set of tools that run on the customers system to attest the system.
- Customers have access to the As Built data reports which contain information such as manufacturer, part number, batch number, distributor, on each of the system components allowing to customer to visually verify individual components.
- It addition to visual verification, the ITSC provides an end user Auto Verify tool.
- The Auto Verify tool compares the Direct Platform data allowing the customer to identify certain system changes from the time of manufacturing to the time of first boot.
- Using the As Built data report and the Auto Verify tool customers with Intel® vPro™ systems and the ITSC can have confidence in the authenticity of their systems.

Intel® Transparent Supply chain Components

- Traceability for select Intel® platforms to the customers
- Provides the following for individual systems:

Intel® TSC Component	Details
System-Level Traceability	• Supported by ***signed platform certificates*** • Linked to discrete ***Trusted Platform Module*** on motherboard
Component-Level Traceability	• Supported by ***"as-built" report*** from ODM • Intel ***ODM partnerships*** are vital to two-level traceability
Statement of Conformance	• Attests to ***authenticity of system*** • ***Signed by Intel***
Customer Web Portal	• Provides ***customer access*** to signed files • Files available for ***download***

Intel® Transparent Supply Chain Process

1

Component and Platform Data Captured at Factory

Component Data:

- For each component (processor, SSD, …)
- Capture information (part #, serial #, …)

Platform Data:

- For each platform (laptop, desktop, …)
- Capture information (model #, Intel® vPro™ technology check ODM, …)

2

Data Transmitted to Intel Key Generation Services

3

Signed Certificates Created & Stored on Intel Database

4

Signed Certificates Available for Download

System-Level Traceability

- Traceability based on a ***hardware root of trust*** for each system:
  - Root of trust provided by ***Trusted Platform Module*** (TPM) 2.0 on motherboard
  - Associates ***platform serial #*** with TPM serial # and public Endorsement Key (EK)
- Software tools deployed ***during the manufacturing flow*** at the Factory:
  - Capture ***system information***
  - Capture ***TPM serial number and public EK***
- Unique X.509 ***Platform Certificate*** for each system:
  - Generated and signed using ***Intel's Certificate Authority***
  - ***Attests*** that the purchased system is a specific system built according to the Intel® Transparent Supply Chain

Generating the Chain of Trust Based on Trusted Platform Module

Trusted Platform Module Manufacturer

- ***Creates Endorsement Key*** (EK) for each Trusted Platform Module (TPM)
- Establishes **hardware root of trust**

System Manufacturer

- Permanently ***mounts TPM*** onto motherboard
- ***Creates platform certificate*** and binds it to the EK

System Integrator

- ***Creates appliance certificate;*** binds it to the platform certificate

Capabilities & Benefits

Ability to ***trace appliance*** to credible hardware root of trust

- Establishes ***technology provider accountability***
- Creates ***transparency***

Chain of Trust Built Up by Multiple Parties in System Lifecycle

Transparent Supply Chain with Process

1 Component and Platform Data Captured at Factory

Factory

14 Components
Adapter, AC
Base Unit
Battery (Notebook)
Camera
Chassis
Hard Drive
Keyboard
LCD Panel
Memory
Motherboard
Operating System
Processor
Touchpad
Wireless Local Area Network

"As Built" Data file

24 Component data fields captured for each of the components
Ex: Vendor, S/N, Part number, validation history, etc.

Snap Shot

18 Platform Data fields captured
Ex: model #, vPro Check
24 TPM PCR Register
SSD data
CSME version

"Direct Platform Data File

TPM Platform Certificate Data file
EK, EK Serial Number

Certificate Data File"

2 Data Transmitted to Intel Key Generation Services

ABD

DPD

PCD

Intel Key Generation Services

PI.D

ABD

DPD

EK#

3 Signed Certificates Created & Stored on Intel Database

Intel Database

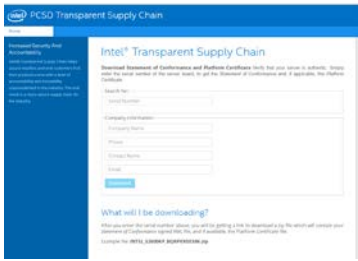
Signed As Built Data

Signed Platform Certificate

Signed Statement of Conformance

4 Signed Certificates Available for download, view, and data analytics

Customer



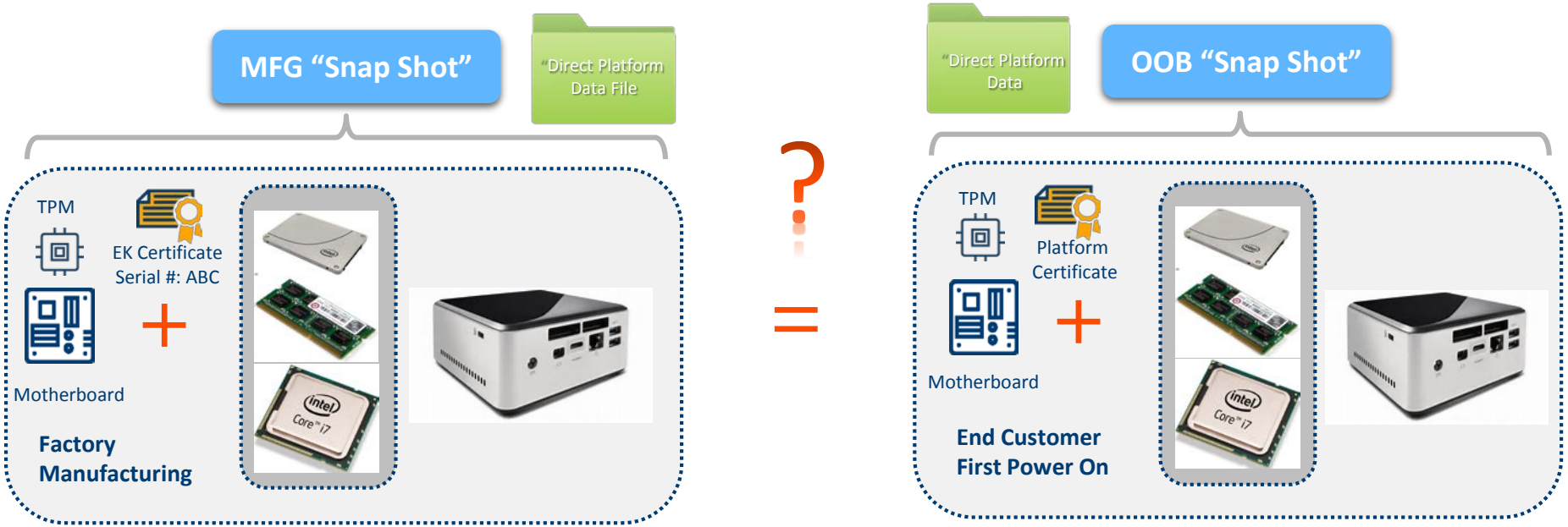
5 Auto Verify Tool Web Download

TRANSPARENT SUPPLY CHAIN – AUTO VERIFY TOOL

- For the Customers who have purchased Intel® vPro™ platform with Intel® Transparent Supply Chain Intel provides the ***Auto Verify tool***
- First is the ***Platform Certificate Validation***
  - The Platform Certificate Validation is used verify that the platform TPM module matches the Cryptographically signed Intel Platform Certificate downloaded from the Customer Web Portal
  - Platform Attestation is confirmed by challenging the TPM module's Endorsement Key and comparing this key with the Endorsement Key stored in the Platform Certificate
- Second is the ***Direct Platform Components Validate***
  - The Auto Verify tool compares the "Snapshot" of the platform component data taken during manufacturing with a "Snapshot" of the platform components taken at first boot
  - Any changes in system will be flagged and reported out to the customer in the tool

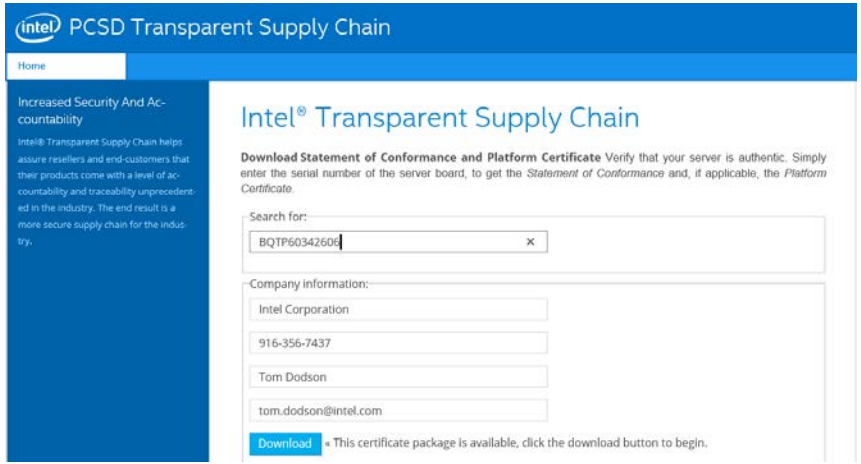
Transparent Supply chain direct platform data snapshots

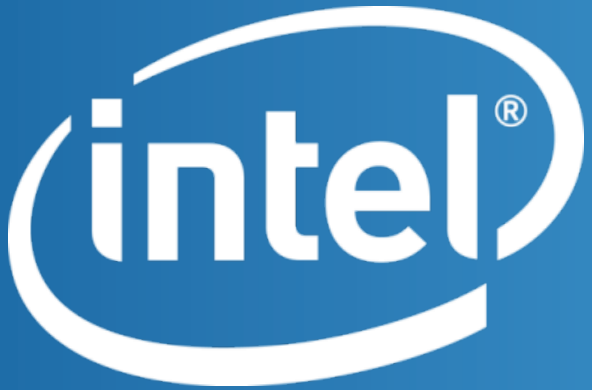
- Is the platform that arrived at the customer that same platform that shipped out of the Factory?
- The Auto Verify tool uses "Snap Shots" to compare the contents of the Direct Platform Data
- Any changes in the Direct Platform Data from the Factory to the Customer will be flagged!



Customer Web Portal (www.intelserveredge.com/tsc)

- Available to customers who have purchased ***Intel® platforms manufactured using Intel® Transparent Supply Chain***
- Customers must be ***validated by email domain***:
  - Pre-approved email domains: ***immediate access***
  - Non-approved email domains: ***additional validation*** required
- Download ***system-specific collateral:***
  - Signed ***platform certificate***
  - Signed ***"as-built" report***
  - Signed ***statement of conformance***
  - Signed ***"Direct Platform Data"*** Intel® vPro™




intel®