



# Intel<sup>®</sup> Transparent supply chain

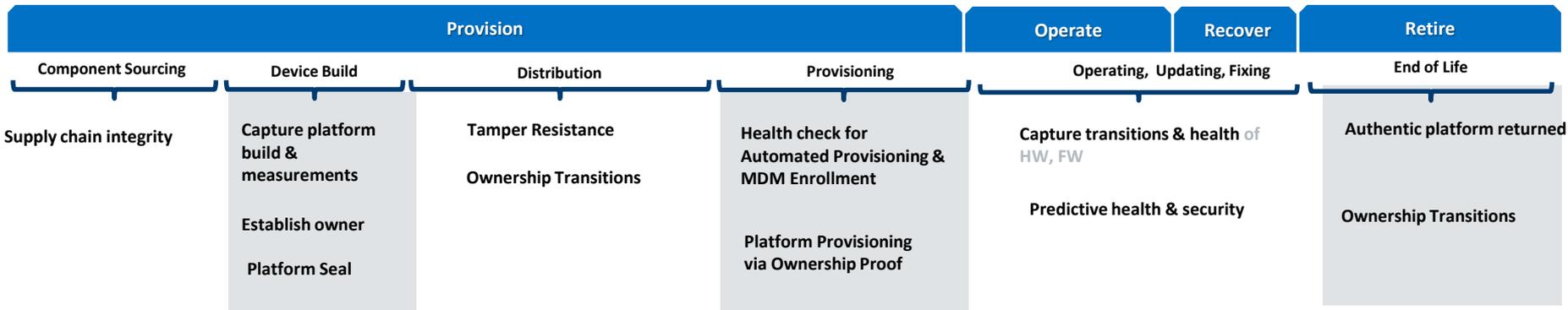
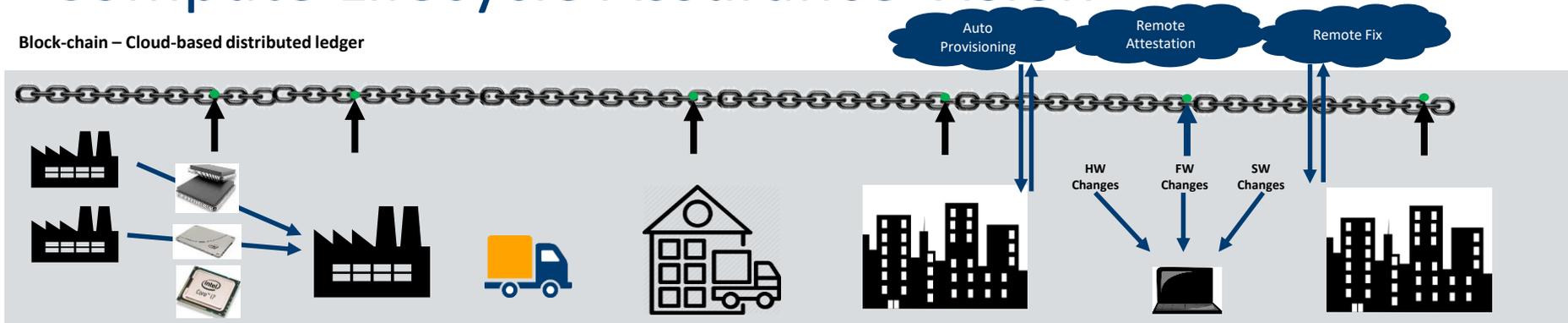
Mark Boucher – Intel Compute Lifecycle Assurance Architect

# Our Approach

- Build upon Intel's internal Supply Chain Expertise
- Scope the end-to-end supply chain(sand to EOL) and complete product lifecycle(Idea to EOL)
- Work with OEMs, Suppliers, Standards Groups and influencers to plan and to promote interoperability and standards for increased transparency
- Make this broadly available across all compute devices
- Deliver Incremental improvements that increase security with transparency of the compute lifecycle
- We are enabling the eco-system today with multiple OEM/ODMs already TSC enabled

# Compute Lifecycle Assurance Vision

Block-chain – Cloud-based distributed ledger



# Intel® Transparent Supply chain

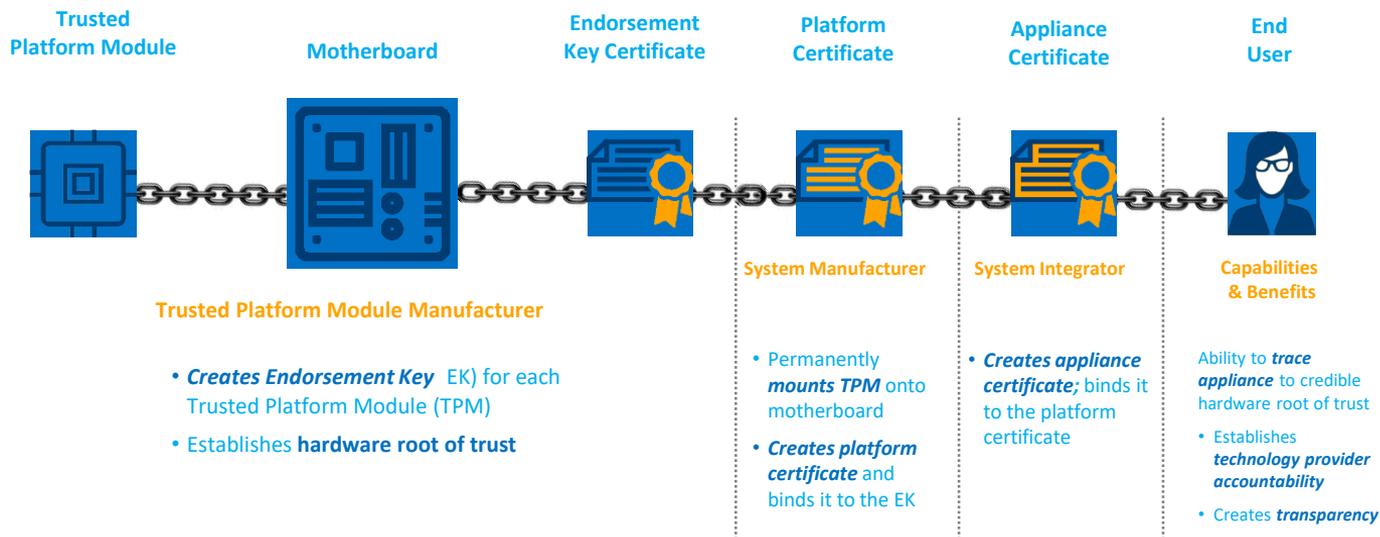
Traceability for select Intel® platforms to customers

## Components

Provides the following for individual systems:

INTEL® TSC COMPONENT	DETAILS
System-Level Traceability	<ul style="list-style-type: none"><li>• Supported by <b>signed platform certificates</b></li><li>• Linked to discrete <b>Trusted Platform Module</b> on motherboard</li></ul>
Component-Level Traceability	<ul style="list-style-type: none"><li>• Supported by <b>“as-built” report</b> from ODM</li><li>• Intel <b>ODM partnerships</b> are vital to two-level traceability</li></ul>
Platform Component Traceability	<ul style="list-style-type: none"><li>• Snapshot of the Platform Components</li><li>• Allows for End-User Verification using Auto Verify Tool</li></ul>
Statement of Conformance	<ul style="list-style-type: none"><li>• Attests to <b>authenticity of system</b></li><li>• <b>Signed by Intel</b></li></ul>
Customer Web Portal	<ul style="list-style-type: none"><li>• Provides <b>customer access</b> to signed files</li><li>• Files available for <b>download</b></li></ul>

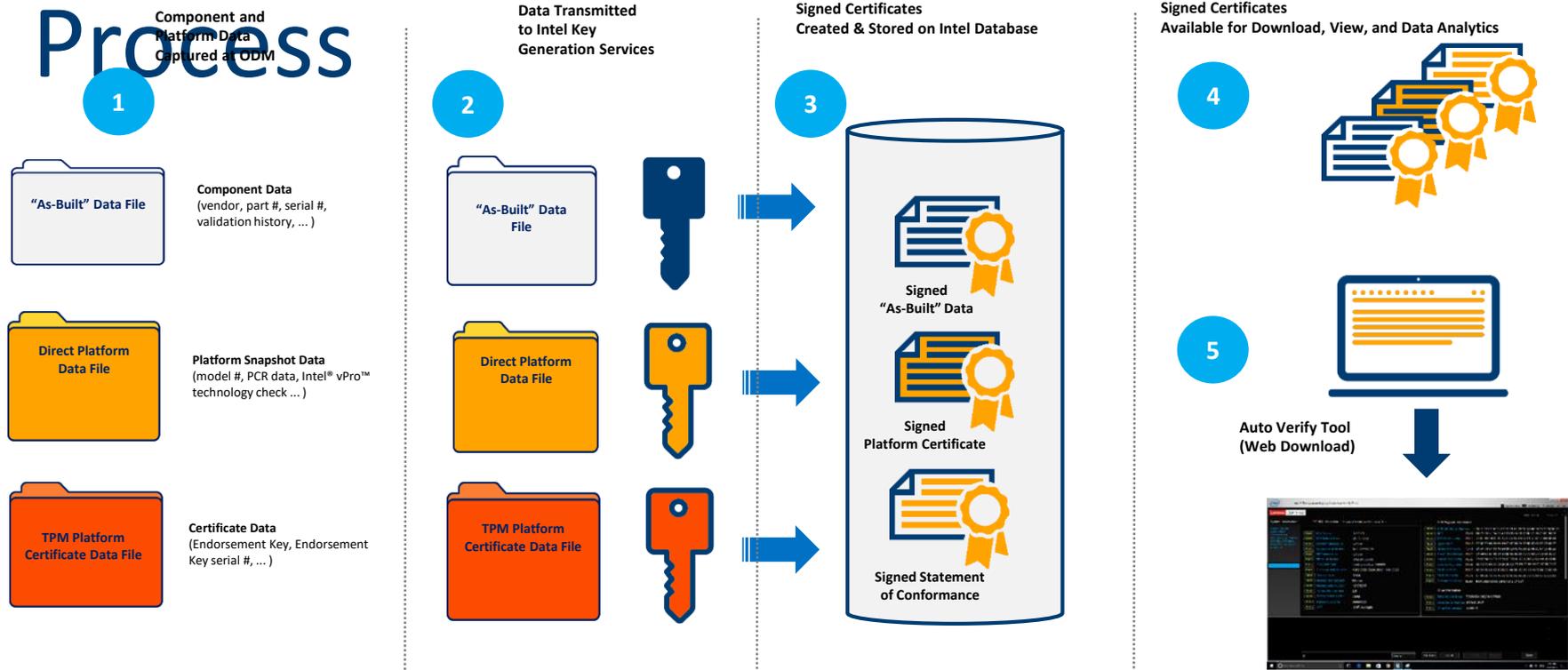
# Generating the Chain of Trust Based on Trusted Platform Module



Chain of Trust Built Up by Multiple Parties in System Lifecycle

# Intel<sup>®</sup> Transparent Supply Chain

## Process



# Transparent Supply Chain Auto Verify

Tool Chain

TPM  
Motherboard

+

OEM FACTORY



TPM  
Motherboard

+

IT CUSTOMER (FIRST BOOT)

intel® Transparent Supply Chain AutoVerify Tool

CERTIFIED

System Information

SMBIOS Information Snapshot: As Built Jan 17 2017 and Apr 20 2017 Change Detected

Changes in the Platform Data between snapshots are Identified

Change	Value
Change BIOS Version	3.222.21
Change BIOS Release Date	2016/12/12
Match System Manufacturer	W5130450-234
Match System Serial Number	W5130450-234
Match MB Manufacturer	
Match MB Serial Number	TPGF20123345
Match Processor Type	Intel Core 2 Duo T9400M
Match Processor Serial Number	A3F3-235C-8920-2D99-1349-2023
Match Memory Type	DDR4
Match Memory Manufacturer	
Match Memory Serial Number	12161215
Match Battery Manufacturer	
Match Battery Serial Number	7EAE

TPM Register Information

Change	Value
Change BIOS Configuration	PCR 1 - 89 08 9A 44 E3 47 1B 01 33 EE 7D 75 03 07 D8 E0 DC 1 8D
Match Option ROM	PCR 2 - B2 6E 23 89 08 9A 44 E3 47 1B 01 33 8D 65 46 8D 53 02 75
Match Option ROM Config	PCR 3 - 3A 3F 78 0F 11 A4 B4 99 69 FC AA 80 CD 6E 39 57 C3 3B 22
Match Master Boot Record	PCR 4 - 33 BD 65 46 1B 01 33 8D 65 46 EE 7D 75 03 07 D8 E0 DC 1
Match Master Boot Config	PCR 5 - 1B 01 33 EE E3 47 1B 01 33 EE 7D 75 03 07 D8 E0 DC 1 8D
Match State Configuration	PCR 6 - EE 7D 75 03 07 D8 E0 DC 1 23 89 08 9A 44 E3 47 1B 01 47
Match Platform Config	PCR 7 - 5F 9A F6 A3 13 46 F6 B1 00 BE F6 A3 13 46 F6 B1 00 BE 4D
Match Static OS Config	PCR 8 - B1 00 BE 73 76 F6 A3 13 46 65 46 EE 7D 75 03 07 8D 53 08

Platform Certificate

Match Platform Certificate	Issuer - Intel Corporation, Santa Clara, CA USA
Match TPM EK Serial Number	- 76 EE 64 E7 DC 15 27 94 1A A3 2B 5F 59 0B F4 23 9F 5D DC 7F
Match TPM Endorsement Key	- 89 08 9A 44 E3 47 1B 01 33 EE 7D 75 03 07 D8 E0 DC 1 8D

Changes

Change	As Built Jan 17 2017	Snapshot Apr 20 2017
BIOS Version	3.220.21	3.222.21
BIOS Release Date	2016/10/12	2016/12/12

Identified changes are displayed

Drive Information

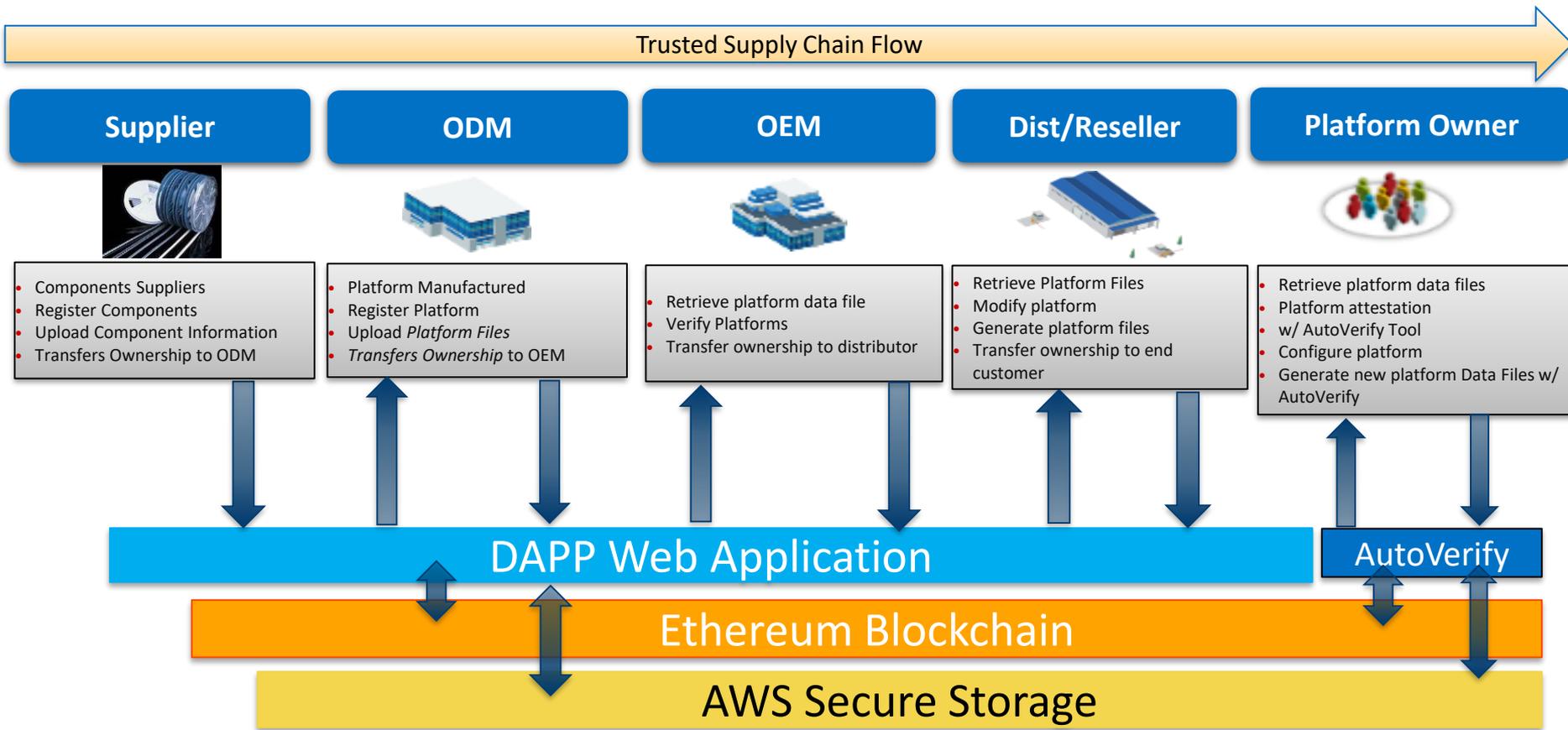
Match Drive Model Name	
Match Drive Serial Number	460NCJPVT
Match Drive FW Version	AV001D

Discard Save

Ask me anything

2:40 PM 3/27/2017

# POC - TSC on Blockchain – Supply Chain Flows



# TSC on Blockchain - POC

