ThinkShield

Technical White Paper

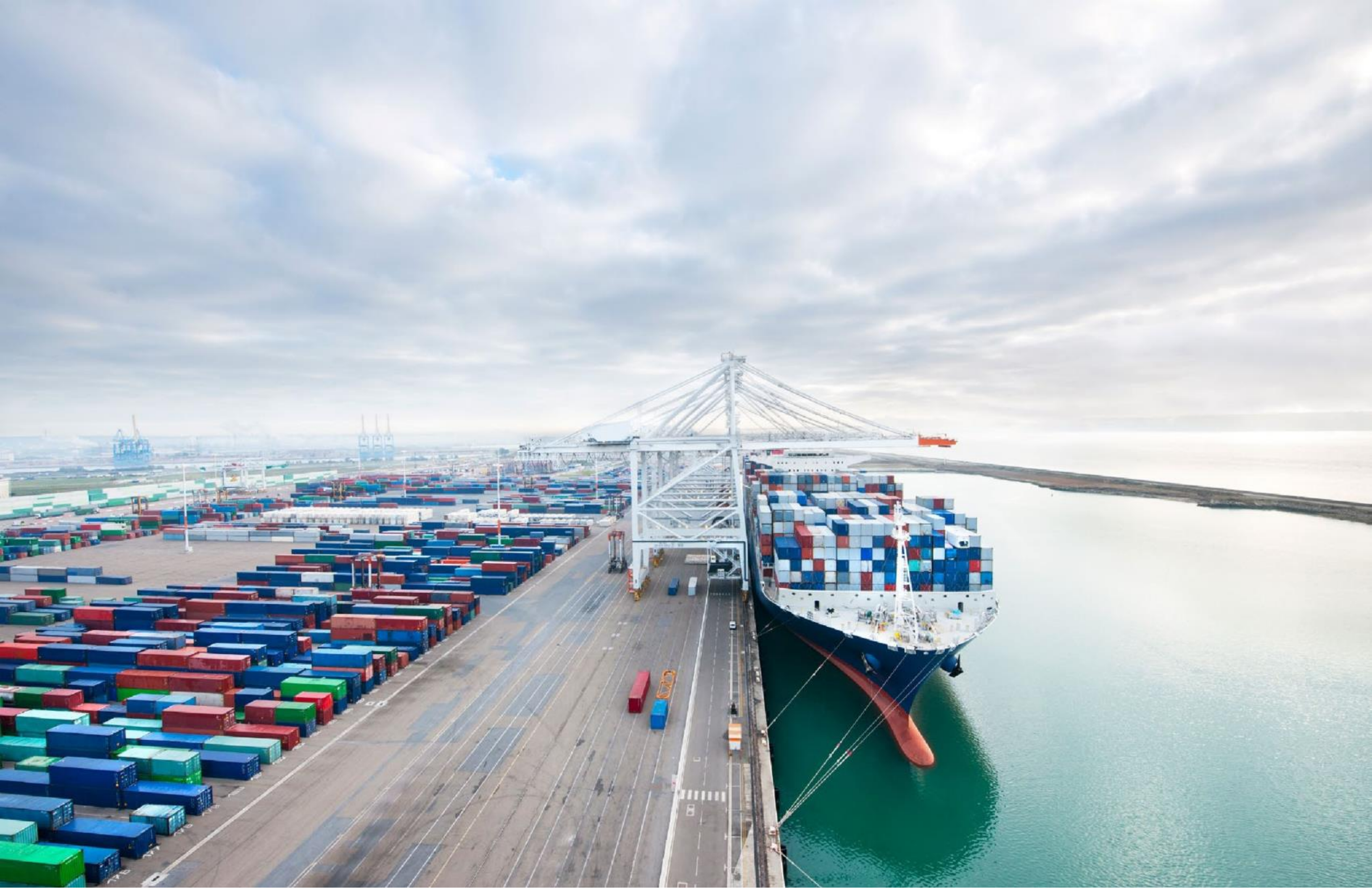
SUPPLY CHAIN SECURITY SOLUTIONS FROM INTEL AND LENOVO: ENSURING DEVICE SECURITY FROM THE FACTORY FLOOR THROUGH END OF LIFE

By **TOM DODSON**
Supply Chain Security Architect, Intel Corporation

intel vPro PLATFORM
Built for Business

Smarter
technology
for all

Lenovo



With the expansion of data centers, cloud computing, and the Internet of Things, ensuring trust in the supply chain has become more important than ever. A supply chain, based on trusted hardware and standards developed by the Trusted Computing Group, can enhance security for everything from sourcing components to distribution of the final product. This paper describes the incentives for organizations to prioritize supply chain trust and introduces the **Intel® Transparent Supply Chain** services, which Intel has developed in partnership with Lenovo. It also explains the use of a hardware root of trust to establish a trusted supply chain.

SUPPLY CHAIN SECURITY IS A CONCERN ACROSS THE PUBLIC AND PRIVATE SECTORS.

> Federal agencies are concerned about the risks associated with information and communications technology (ICT) products and services that may contain potentially malicious functionality, are counterfeit, or are vulnerable due to poor manufacturing and development practices within the ICT supply chain.
>
> — National Institute of Standards and Technology

INCENTIVES FOR SUPPLY CHAIN TRUST

The use of technology to compromise supply chains is not a new phenomenon; one article in *Supply Chain 24/7* provides a history of supply chain cyberattacks dating back to the Cold War.[1] Before end users even turn on their new equipment, malicious actors have numerous opportunities to disrupt and compromise the supply chain tasked with delivering new devices into end users' hands. Such attacks should concern every company regardless of their size or market focus.

The U.S. government is well aware of the significance of the problem: A paper from the National Institute of Standards and Technology (NIST) states that "Federal agencies are concerned about the risks associated with information and communications technology products and services that may contain potentially malicious functionality, are counterfeit, or are vulnerable due to poor manufacturing and development practices within the ICT supply chain."[2] In 2015, the U.S. Department of Defense published a three-page interim rule to the Defense Federal Acquisition Regulation Supplement. This interim rule gave government contractors a deadline to implement the requirements of the Special Publication 800-171,[3] which NIST published to counteract cybersecurity threats. Section 252.246-7007 of this document, Contractor Counterfeit Electronic Part Detection and Avoidance System, specifically addresses "design, operation, and maintenance of systems to detect and avoid counterfeit electronic parts and suspect counterfeit electronic parts."[4]

The Rise of Remote Work

Companies seeking to secure end-user devices are confronting a new factor in an already fraught equation: the sharp increase in the number of employees working remotely. According to Gallup, the percentage of employed Americans who said they had worked remotely doubled in the spring of 2020 alone—climbing from 31 percent in March to 62 percent in April.[5] What began as a temporary solution may well become permanent: According to Gartner, nearly three in four CFOs plan to shift some employees to remote work permanently.[6] But as the technology to serve those working from anywhere grows more sophisticated, so do the techniques to exploit it. Without the right protection, criminals can tamper with PCs, removing or replacing components—resulting in anything from malfunctioning devices to compromised systems with counterfeit parts.

Today, instances of attacks on supply chains and the use of counterfeit, substituted, or malicious components abound. In a May 2020 brief, Deloitte reported that “4 in 10 manufacturers surveyed indicated that their operations were affected by a cyber incident in the past 12 months.”[7]

> **4 in 10** manufacturers surveyed indicated that their operations were affected by a cyber incident in the past 12 months”
>
> *— Deloitte*

The diversity of today’s manufacturing, logistics, and inventory environments makes information about a device’s origin and subsequent history especially critical for organizations and end users. In particular, remote deployment and provisioning present both challenges and opportunities for supply chain security: They introduce new vulnerabilities to cyberattacks but can also decrease service costs and reduce the steps needed to physically track devices. As such, organizations stand to benefit from a trusted supply chain that enables remote deployment and provisioning of end-user devices.

Figure 1 shows vulnerable points in the supply chain and the benefits of adding trustworthy elements.

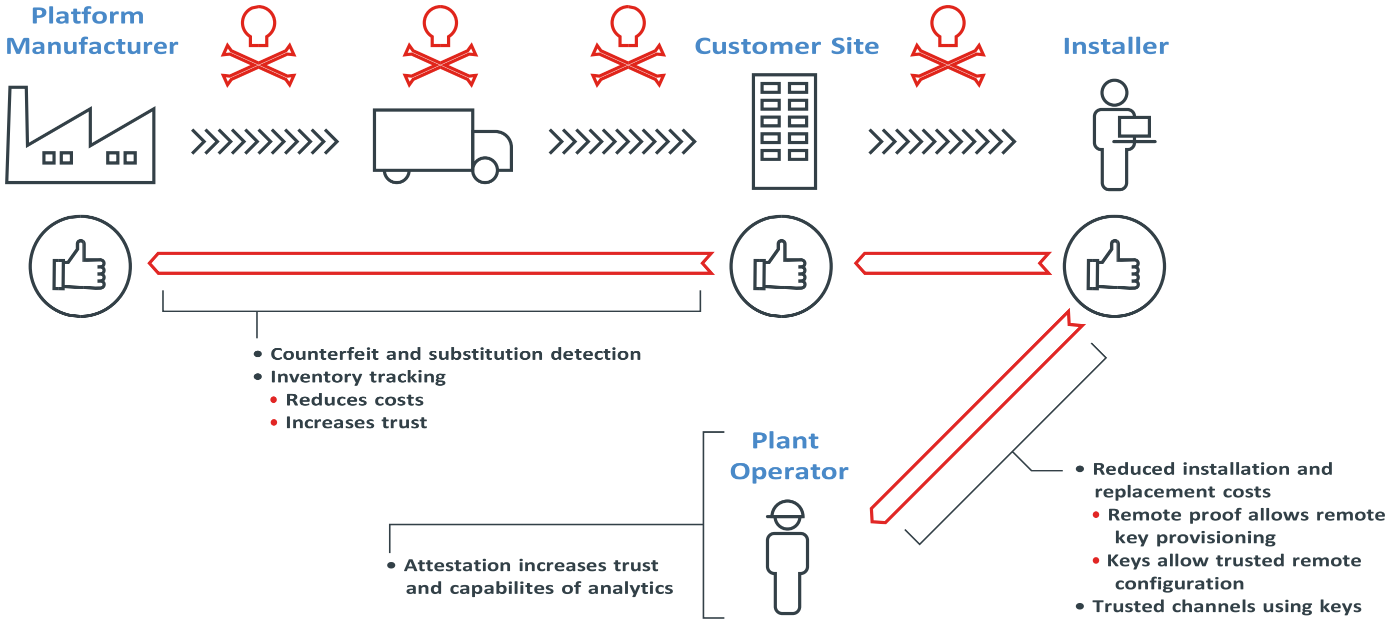

Platform Manufacturer
Customer Site
Installer
• Counterfeit and substitution detection
• Inventory tracking
• Reduces costs
• Increases trust
Plant Operator
• Attestation increases trust and capabilites of analytics
• Reduced installation and replacement costs
• Remote proof allows remote key provisioning
• Keys allow trusted remote configuration
• Trusted channels using keys
• Allows multiplexing connections •
Reduces cabling costs

Figure 1: The trusted supply chain value proposition.

How Hackers Monetize Your Data

Cybercriminals can use personal data to do anything from stealing users’ identities to selling their credit card or personal information on the black market. According to anti-malware maker Emsisoft, a “full ID package” containing a user’s name, address, phone, SSN, email, and bank account retails for between USD$30 and USD$100.[8] Consider the scale of the Equifax breach, which exposed the personal information of 147 million consumers,[9] and you begin to understand how much money is at stake. Another avenue for monetization is holding a company’s systems hostage until that company pays a ransom. In July of 2020, the GPS maker Garmin reportedly paid a multi-million-dollar ransom after a cyberattack shut down many of its crucial systems and services.[10] Although the techniques and outcomes of these attacks vary, one thing remains constant: the value of users’ data.

Assurances of a device's origin help establish the foundation for a trusted supply chain. The Trusted Computing Group's initial Trusted Platform Module (TPM) standard defined a hardware root of trust. More recently, Trusted Platform Module 2.0, now the International Organization for Standardization (ISO) standard (ISO 11889),[11] created a library specification to describe all the commands and/or features that could be implemented or needed in a variety of platforms, including embedded systems. In the Trusted Platform Module, the Endorsement Key (EK) is a permanent key (with some exceptions) that is uniquely associated with a specific Trusted Platform Module. It provides assertions about the Trusted Platform Module but no assertions about the platform. A Trusted Platform Module EK can certify other TPM and/or platform keys created by the owner or users. In addition, it also has Platform Configuration Registers, Attestation ID Keys, Signature Keys, and Encryption Keys for verifying access and protecting data.

Below, **Figure 2** shows how the Trusted Platform Module provides the hardware root of trust. Its EK certificate and a platform certificate are used to establish the documentation for the platform. The Trusted Platform Module's EK certificate is signed by the TPM vendor. Next, the Platform Manufacturer attaches the Trusted Platform Module to a platform where the Encryption Key is bound to the platform to provide a platformspecific key. The platform certificate created by the platform manufacturer attributes asset information about the platform and the Root of Trust for Measurement (RTM), binding it to the Trusted Platform Module. The value of the measurements is proportional to the trust in the RTM provided by the platform manufacturer. Finally, the supply chain obtains proof of assertions to verify platform and Encryption Key certificate signatures, as well as to verify the EK certificate bound to that platform.

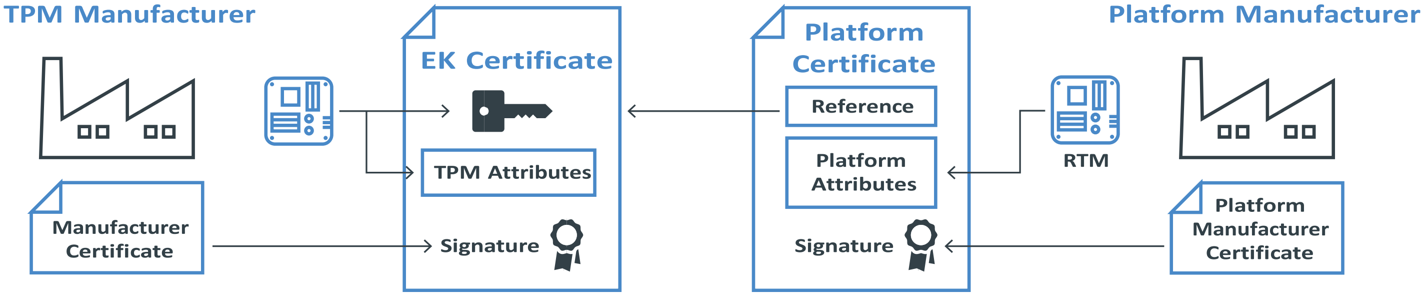


Figure 2: The TPM general architecture transfers keys and certificates to build trust.

IMPLEMENTING A TRUSTED SUPPLY CHAIN

Building on the Trusted Platform Module general architecture, **Figure 3** shows the steps for the documentation for the root of trust, which continues through the supply chain until it gets to the final owner, where an IT expert uses open-source tools to verify platform signatures and EK certificates, as well as conduct other trustconfirming tasks.

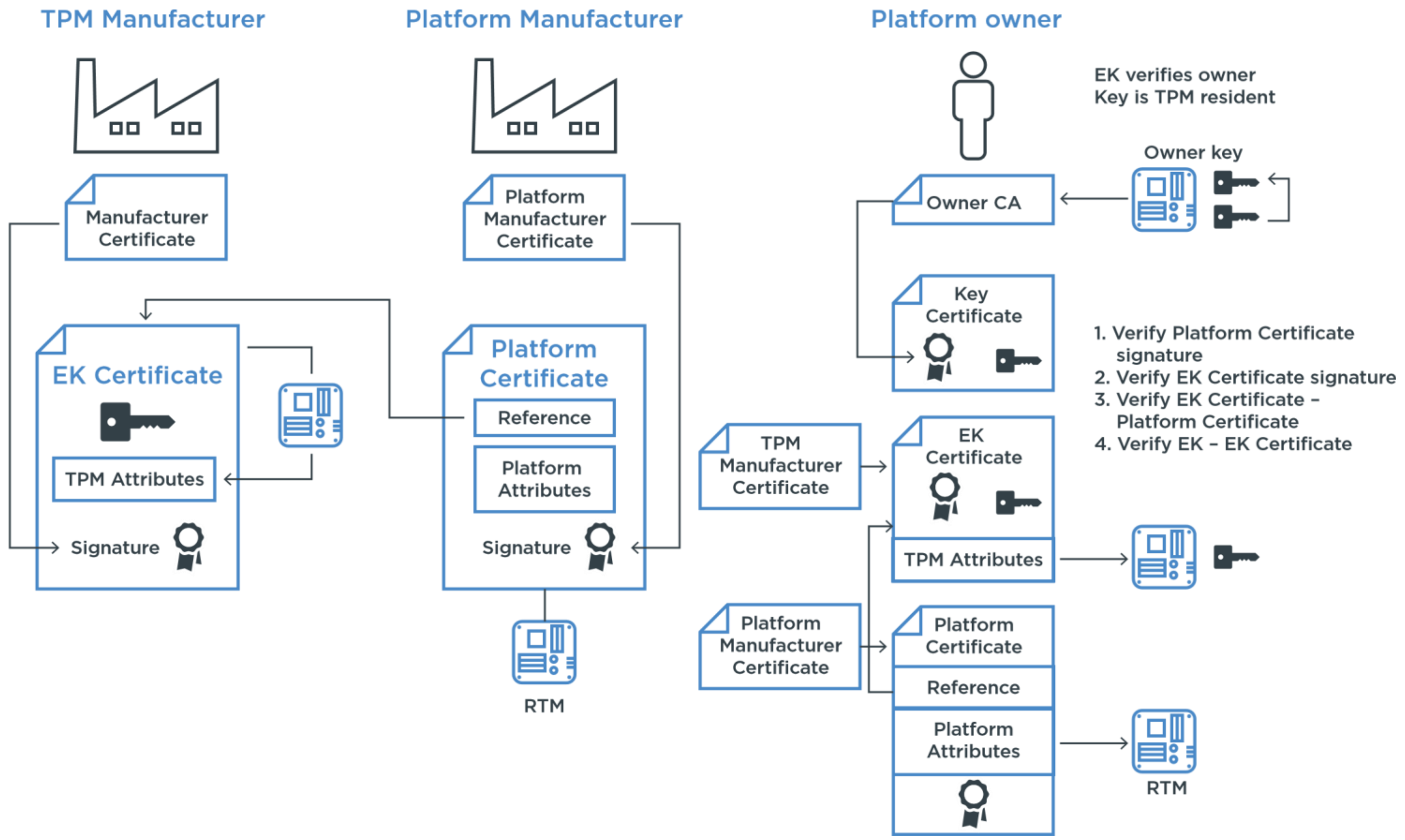


Figure 3: Trusted Supply Chain traceability extends to the platform owner and users.

Based on the previous chain established in the lifecycle of the system, **Figure 4** shows how appliance certificates are generated. Generating the chain of trust starts with the Trusted Platform Module, creating the Encryption Key for each TPM and establishing the hardware root of trust. Next, the platform manufacturer permanently mounts the TPM onto the platform, creates the platform certificate, and binds it to the Encryption Key. A Signing Service provides a platform certificate that cryptographically binds the platform to the EK. Finally, the System Integrator creates an appliance certificate and binds it to the platform certificate. At the end of the process, the end user benefits from the ability to trace the appliance to credible hardware root of trust, establishing technology provider accountability as well as transparency.

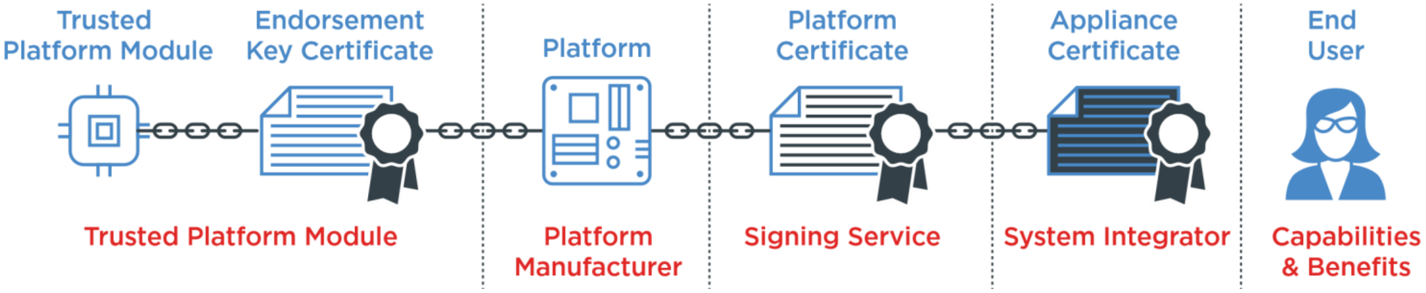


Figure 4: Generating the chain of trust in a typical system touches each stage.

The chain of trust process is essential to provide total traceability and an hardware root of trust based on the Trusted Platform Certificate. It enables component-level traceability for platforms and systems to mitigate the risk of counterfeit electronic parts, while conforming to DFARS Supplement 246.870-2. The fact that chain of trust satisfies government regulations for security, which are often more stringent than even large enterprise protocols, reinforces the efficacy of the service. The trusted supply chain also provides an end-user Auto Verify tool that identifies certain system changes from the time of manufacturing to the time of first boot. The "AsBuilt" data report and Auto Verify tool offers customers confidence in the authenticity of their systems.

Traceability in the supply chain includes platform certificates with component level traceability (supported by an "As-Built" report generated from the factories), a statement of conformance attesting to the authenticity of the system, and a customer web portal that downloads the files with a link to access details to the files and certificates. **Figure 5** shows how the various trust items flow through the Transparent Supply Chain process, from initial generation to the Auto Verify tool.

The Auto Verify tool collects data on all the components in the system, not just the TPM, providing Platform Certificate Validation as well as Direct Platform Components Validation. The components could include a laptop with some drives, memory, processors, and more. The first time the customer powers up their device, the tool checks for any changes in the hardware, comparing what the customer received to what the original design manufacturer (ODM) shipped.

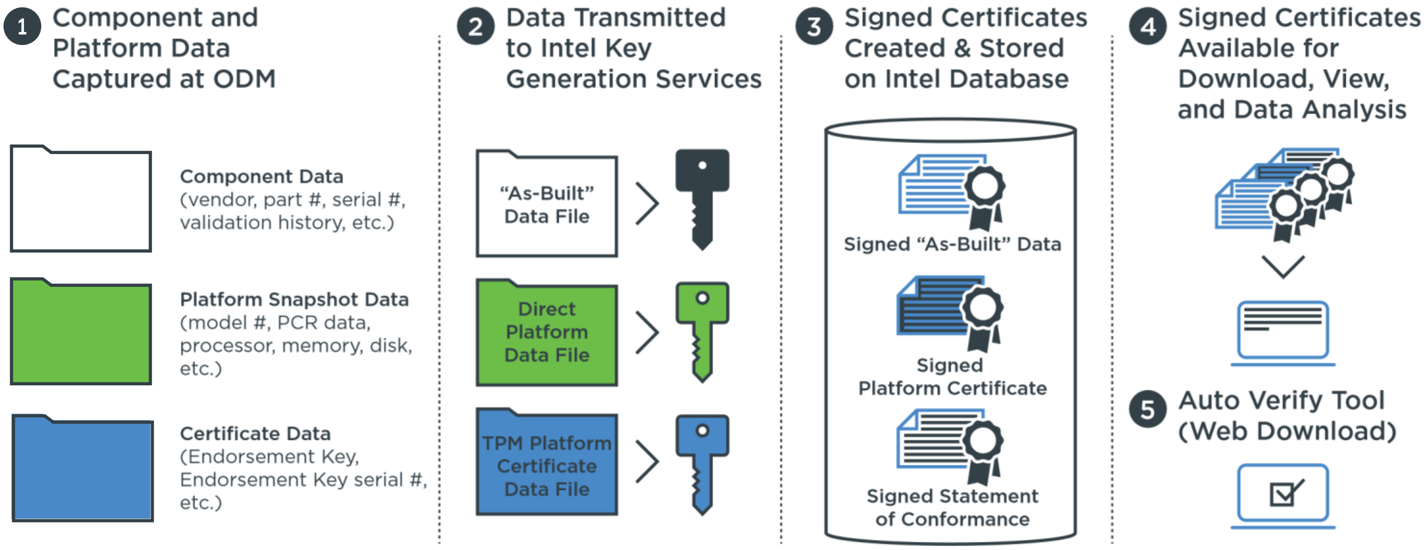
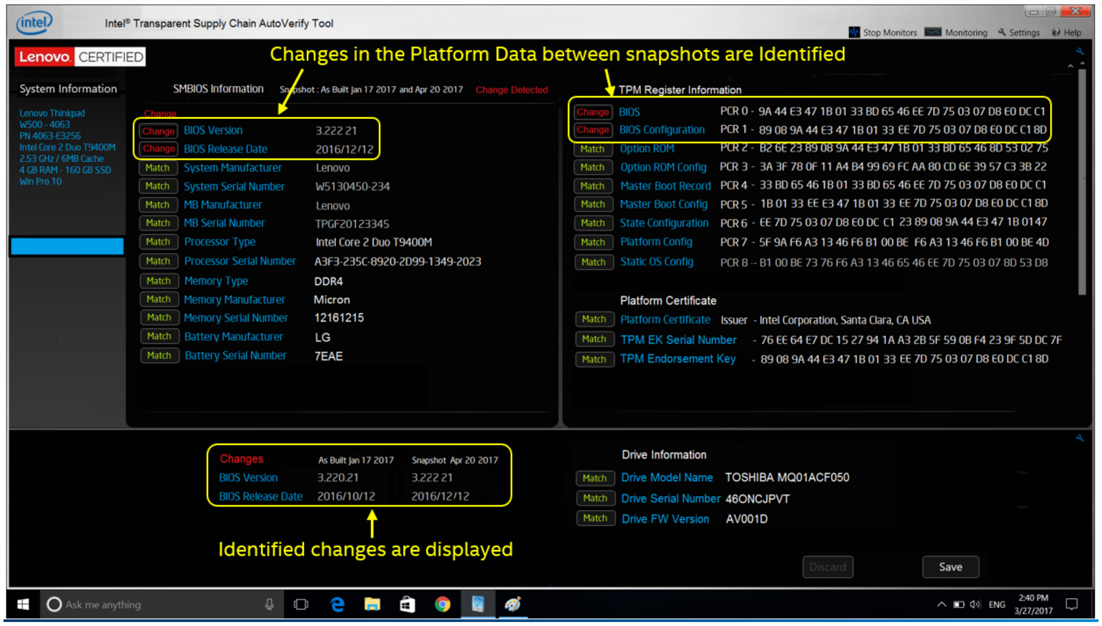

1 Component and Platform Data Captured at ODM
Component Data (vendor, part #, serial #, validation history, etc.)
Platform Snapshot Data (model #, PCR data, processor, memory, disk, etc.)
Certificate Data (Endorsement Key, Endorsement Key serial #, etc.)
2 Data Transmitted to Intel Key Generation Services
"As-Built" Data File
Direct Platform Data File
TPM Platform Certificate Data File
3 Signed Certificates Created & Stored on Intel Database
Signed "As-Built" Data
Signed Platform Certificate
Signed Statement of Conformance
4 Signed Certificates Available for Download, View, and Data Analysis
5 Auto Verify Tool (Web Download)

Figure 5: The Trusted Supply Chain process uses the HRoT in the TPM, platform certificates, and other data confirmed by the Auto Verify tool.

System-level traceability is based on a hardware root of trust (HRoT) for each system and starts with the HRoT provided by the Trusted Platform Module on the motherboard. In addition, software tools deployed during manufacturing capture system information and the Trusted Platform Module certificate (including the public EK). A unique X.509 platform certificate for each system is generated and signed using Platform Manufacturer Certificate Authority. This attests that the purchased system is the specific system built by the manufacturer.

To aid in the process, the Transparent Supply Chain AutoVerify tool is available for download on Lenovo's TSC web portal. **Figure 6** shows how data from original and as-delivered platform snapshots are identified and displayed.



Intel® Transparent Supply Chain AutoVerify Tool
Stop Monitors
Monitoring
Settings
Help
Lenovo CERTIFIED
Changes in the Platform Data between snapshots are Identified
System Information

Lenovo Thinkpad
W500 - 4063
PN 4063-E3256
Intel Core 2 Duo T9400M
2.53 GHz / 6MB Cache
4 GB RAM - 160 GB SSD
Win Pro 10

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

Change		
Change	BIOS Version	3.222 21
Change	BIOS Release Date	2016/12/12
Match	System Manufacturer	Lenovo
Match	System Serial Number	W5130450-234
Match	MB Manufacturer	Lenovo
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	Micron
Match	Memory Serial Number	12161215
Match	Battery Manufacturer	LG
Match	Battery Serial Number	7EAE

TPM Register Information

Change	BIOS	PCR 0 - 9A 44 E3 47 1B 01 33 BD 65 46 EE 7D 75 03 07 D8 E0 DC C1
Change	BIOS Configuration	PCR 1 - 89 08 9A 44 E3 47 1B 01 33 EE 7D 75 03 07 D8 E0 DC C1 8D
Match	Option ROM	PCR 2 - B2 6E 23 89 08 9A 44 E3 47 1B 01 33 BD 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 BD 65 46 EE 7D 75 03 07 D8 E0 DC C1
Match	Master Boot Config	PCR 5 - 1B 01 33 EE E3 47 1B 01 33 EE 7D 75 03 07 D8 E0 DC C1 8D
Match	State Configuration	PCR 6 - EE 7D 75 03 07 D8 E0 DC C1 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 D8

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 C1 8D

Changes	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

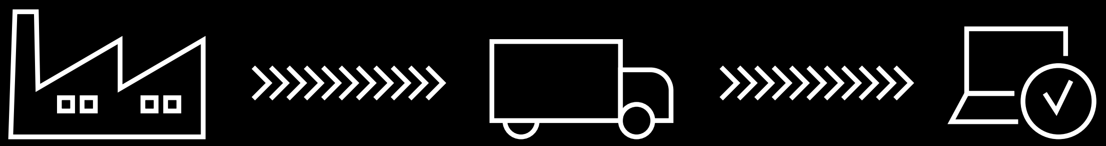
Identified changes are displayed

Drive Information

Match	Drive Model Name	TOSHIBA MQ01ACF050
Match	Drive Serial Number	46ONCJPVT
Match	Drive FW Version	AV001D

Figure 6: The Auto Verify tool communicates identified changes and other crucial data to the end-user certificates.

Protect devices...



from the point
of manufacture...

and during
transport...

until they're on-site
with the end user

Steps to Establishing Supply Chain Trust

1. **Immediately:** Evaluate your company's supply chain for its IT components.
2. **Within the next three months:**Identify IT components that have supply chain risk and determine if there is an opportunity to incorporate the TSC.
3. **Within the next six months:**Implement a secure supply chain based upon the TPM.
4. **For future purchases:** Consider platforms that incorporate Lenovo models with the Intel® Transparent Supply Chain Certification Tools for TPM 2.0 Support.

INTRODUCING INTEL® TRANSPARENT SUPPLY CHAIN

In this evolving threat landscape, Lenovo ThinkShield secures companies' critical data and business technologies with comprehensive, end-to-end protection. Taking a "security by design" approach to the entire product lifecycle, Lenovo ThinkShield offers four primary focus areas:

- **Device Protection:** Includes Transparent Supply Chain
- **Built-in Platform Security:** Includes self-healing BIOS and Trusted Supplier program
- **Security Management:** Includes integrated system management solutions for deploying, monitoring, and reporting for IT assets
- **Threat and Data Protection:** Includes endpoint protection with capabilities like Ransomware Rollback and integration with Microsoft Defender

The following section focuses on the service that falls under the Device Protection category: Transparent Supply Chain.

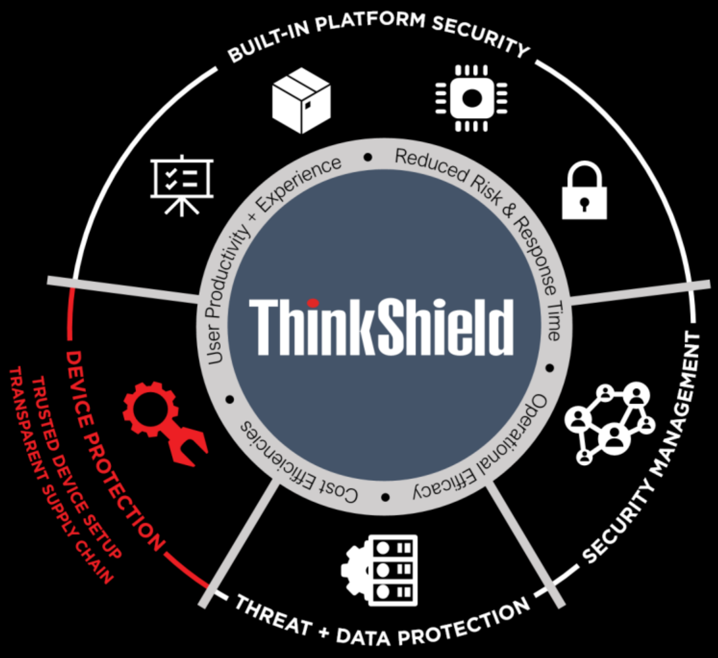
Intel® Transparent Supply Chain

Intel® Transparent Supply Chain brings Lenovo security into the transport and delivery cycle with a documented, auditable supply chain security program that enables traceability of all purchases at the component and system level. A **trusted supplier guarantee** ensures that all suppliers adhere to Lenovo's strict manufacturing standards and pass quarterly compliance and security assessments, while an **Auto Verify tool** identifies certain system changes from the time of manufacturing to the time of first boot. **The Customer Web Porta**l allows convenient access to signed files verifying integrity, such as:

- A signed **platform certificate** that links to a Trusted Platform Module (TPM) on the device's motherboard
- **"As-Built" data reports** that provide users with information on key system components (such as the manufacturer, part number, batch number, and distributor)
- **A statement of conformance**, signed by Intel, that guarantees the authenticity of the systems

CONCLUSION

Product tampering and unauthorized substitutions can occur anywhere in the supply chain. Intel and Lenovo have introduced two services to enhance end-to-end device security: Intel® Trusted Device Setup and Intel® Transparent Supply Chain. With a trusted supply chain in place, companies can reduce the risk of supply chain tampering and minimize the chance of receiving counterfeit parts—ultimately protecting valuable company data. This paper explored the mechanics underpinning these services: namely, a trusted supply chain (based on a hardware Root of Trust established by using the Trusted Computing Group's Trusted Platform Module standard) and an Auto-Verify tool (which provides traceability, accountability, assurance, and security to the user) to establish trust in the supply chain and mitigate the potential for cyberattacks due to supply chain tampering.



ABOUT THE AUTHOR

Tom Dodson has been in the Supply Chain Security field for the past 25 years working with component suppliers and system manufacturers to ensure a secure and healthy supply chain has been established. Over the last eight years, Tom has developed a set of Trusted Supply Chain Policies and Procedures, working with NIST and TCG to establish standards that can be used across the industry.

http://www.supplychain247.com/article/the_supply_chain_silent_threat_cyber_attack/security
https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-161.pdf
https://www.eventtracker.com/campaigns/nist-800-171-compliance
https://www.acq.osd.mil/dpap/dars/dfars/html/current/252246.htm#252.246-7007
https://news.gallup.com/poll/306695/workers-discovering-affinity-remote-work.aspx
https://www.gartner.com/en/newsroom/press-releases/2020-04-03-gartner-cfo-surey-reveals-74-percent-of-organizations-to-shiftsome-employees-to-remote-work-permanently2
https://www2.deloitte.com/content/dam/Deloitte/global/Documents/About-Deloitte/COVID-19/Deloitte-Global-Cyber-COVID-19Executive-Briefing-Issue-5-release-date-5.6.2020.pdf
https://blog.emsisoft.com/en/35541/how-do-hackers-make-money-from-your-stolen-data/#:~:text=In%20most%20cases%2C%20 data%20theft,marketplaces%20to%20the%20highest%20bidder
https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement
https://www.engadget.com/garmin-cyber-attack-ransomware-payment-180211805.html
https://www.iso.org/standard/66510.html

WWServices-TSC-TSC_WPa-IT-091520F-TD/RL

Products and offers subject to availability. Lenovo reserves the right to alter product offerings and specifications, at any time, without notice. Lenovo makes every effort to ensure accuracy of all information but is not liable or responsible for any editorial, photographic or typographic errors. Images are for illustration purposes only. For full Lenovo product, service and warranty specifications, visit www.lenovo.com.

Lenovo and the Lenovo logo are trademarks or registered trademarks of Lenovo. Other company, product and service names may be trademarks or service marks of others. © Lenovo 2020. All rights reserved.

Intel, the Intel logo, Intel Core, and Intel vPro are trademarks of Intel Corporation or its subsidiaries.