Introduction to Intel Transparent Supply Chain on Lenovo ThinkSystem Servers

Positioning Information

Infrastructure security has long been on top of the lists of concerns for businesses. Increasingly frequent reports of supply chain attacks add to those concerns, whether it's purported "spy chip" hardware implants, tainted firmware, interdicted shipments, or counterfeit components.

Recent publications have expressed growing concern that counterfeit electronic parts can cause safety hazards, failure of critical business applications, or that there's a risk that vulnerabilities can be introduced into the supply chain to be exploited later.

Modern manufacturing logistics and the globalization of current supply chains make it difficult to trace the origin and safety of the components inside a device. Your data center supplier must be able to provide assurance that it has tamper proof supply chains from the manufacturing facility all the way into your hands. Current supply chain practices start with trusting the source, but processes are limited to screening out counterfeit components, particularly for products containing many subsystems.

Lenovo has one of the world's best supply chains as ranked by Gartner Group, backed by extensive and mature supply chain security programs that exceed industry norms and US Government standards. Now we are the first Tier 1 manufacturer to offer Intel® Transparent Supply Chain in partnership with Intel, offering you an unprecedented degree of supply chain transparency and assurance.

What is the Intel Transparent Supply Chain?

Intel Transparent Supply Chain (Intel TSC) is a set of tools, policies, procedures and data capture. It extends from motherboard production through the manufacturing factory floor to your data center, implemented on the factory floor enabling you to verify the authenticity of components, installed firmware, and the configuration of your systems.

> Lenovo offers an unparalleled level of supply chain transparency and security with the Intel Transparent Supply Chain program

It all starts with motherboard production, where a comprehensive bill of materials detailing each electronic component – down to the smallest part – is automatically generated by the automated shop floor control systems used for printed circuit board assembly. This inventory forms the motherboard "as built" data file, with each file uniquely tied to a specific motherboard.

Next, in server manufacturing, we physically inventory all the components we assemble in a server using barcoded component identifiers scanned into our manufacturing systems. This inventory is the source of the platform "as built" data file, with each file uniquely tied to a specific server chassis.

Once server manufacturing is complete, an Intel-provided software tool is run that inventories all software readable components, installed firmware, and configuration information within the server. This information is then tied to the TPM, the Trusted Platform Module, that's on the server motherboard.

All of this data is then sent via secure connection to Intel where they digitally sign the data and post it to the Intel-hosted Lenovo ISG Transparent Supply Chain portal at https://tsc.intel.com/lenovo-dcg/. You can then retrieve the data and a companion verification tool. This way you know what's in your system, and you will have the full bill of materials and traceability report of your system along with the accountability and attestation provided by Intel's digital signature which safeguards against data tampering.

With this enhanced supply chain security capability, you will have the confidence that all components are known and genuine, and have a way to verify that the hardware you are receiving hasn't been tampered with between when it left our facility to when it arrived at yours.

This feature provides traceability back to the motherboard component level giving you the confidence of knowing exactly what's in your product. Below you will find a graphic depiction of the process.

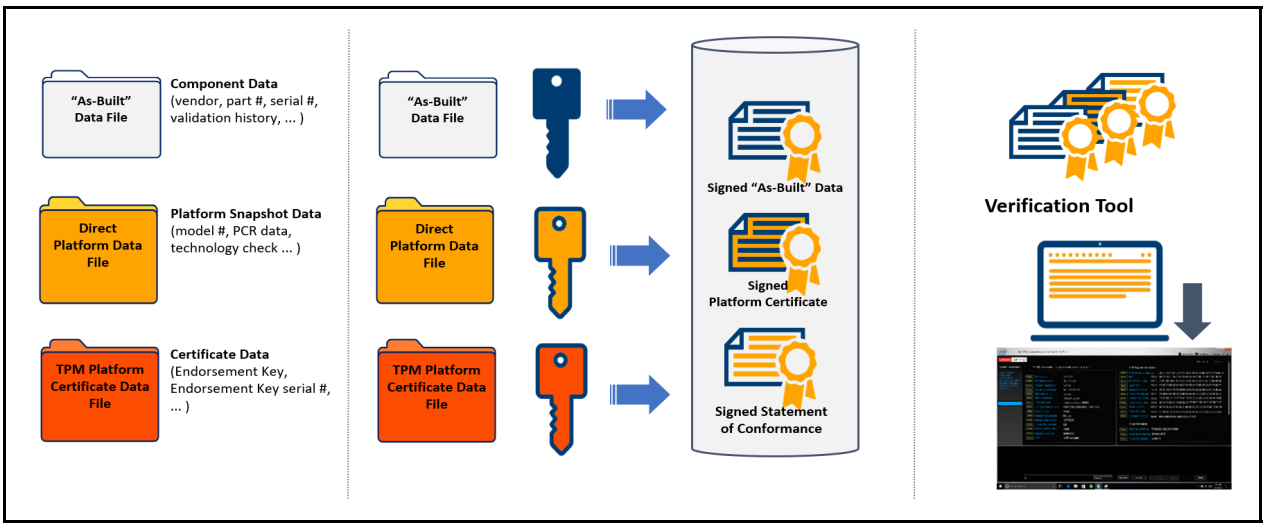
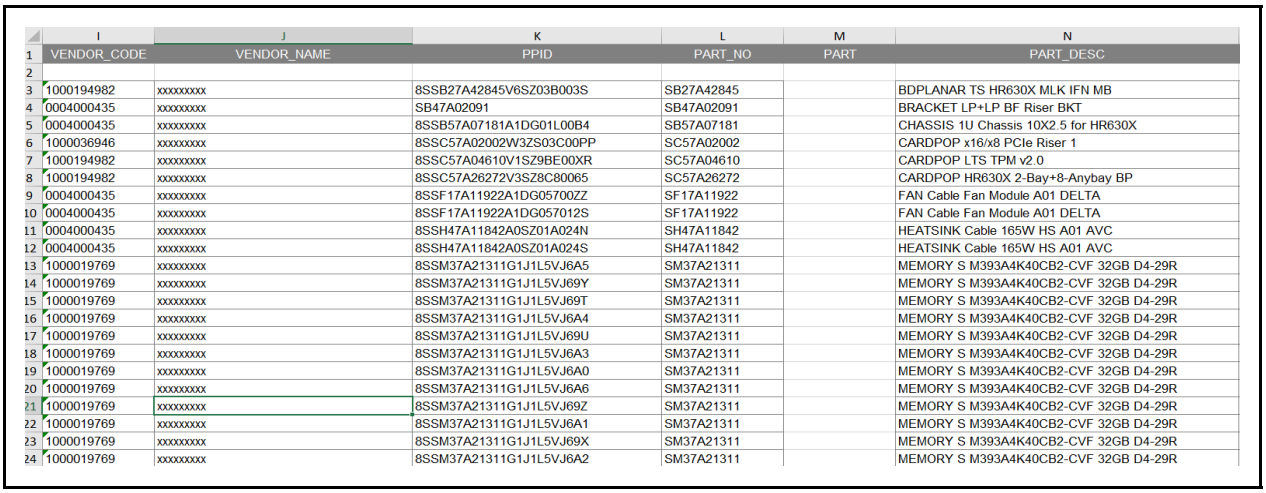


Figure 1. Intel Transparent Supply Chain workflow (click to view a larger version)

What data does the Intel Transparent Supply Chain capture?

Lenovo is the first tier 1 manufacturer to offer this capability

The motherboard "as built" data file - shown in the image below - goes to the detailed level of the motherboard: every micro circuit, chip, resistor, everything that's placed on a motherboard is inventoried along with information like where it came from, what's its part number, and if there's a serial number. Then we extend that to all the other components that are installed in the server like memory DIMMs, CPUs and hard drives. This creates a set of data which captures each of those individual pieces that make up the product.



	I	J	K	L	M	N
1	VENDOR_CODE	VENDOR_NAME	PPID	PART_NO	PART	PART_DESC
2						
3	1000194982	xxxxxxxx	8SSB27A42845V6SZ03B003S	SB27A42845		BDPLANAR TS HR630X MLK IFN MB
4	0004000435	xxxxxxxx	SB47A02091	SB47A02091		BRACKET LP+LP BF Riser BKT
5	0004000435	xxxxxxxx	8SSB57A07181A1DG01L00B4	SB57A07181		CHASSIS 1U Chassis 10X2.5 for HR630X
6	1000036946	xxxxxxxx	8SSC57A02002W3ZS03C00PP	SC57A02002		CARDPOP x16/x8 PCIe Riser 1
7	1000194982	xxxxxxxx	8SSC57A04610V1SZ9BE00XR	SC57A04610		CARDPOP LTS TPM v2.0
8	1000194982	xxxxxxxx	8SSC57A26272V3SZ8C80065	SC57A26272		CARDPOP HR630X 2-Bay+8-Anybay BP
9	0004000435	xxxxxxxx	8SSF17A11922A1DG05700ZZ	SF17A11922		FAN Cable Fan Module A01 DELTA
10	0004000435	xxxxxxxx	8SSF17A11922A1DG057012S	SF17A11922		FAN Cable Fan Module A01 DELTA
11	0004000435	xxxxxxxx	8SSH47A11842A0SZ01A024N	SH47A11842		HEATSINK Cable 165W HS A01 AVC
12	0004000435	xxxxxxxx	8SSH47A11842A0SZ01A024S	SH47A11842		HEATSINK Cable 165W HS A01 AVC
13	1000019769	xxxxxxxx	8SSM37A21311G1J1L5VJ6A5	SM37A21311		MEMORY S M393A4K40CB2-CVF 32GB D4-29R
14	1000019769	xxxxxxxx	8SSM37A21311G1J1L5VJ69Y	SM37A21311		MEMORY S M393A4K40CB2-CVF 32GB D4-29R
15	1000019769	xxxxxxxx	8SSM37A21311G1J1L5VJ69T	SM37A21311		MEMORY S M393A4K40CB2-CVF 32GB D4-29R
16	1000019769	xxxxxxxx	8SSM37A21311G1J1L5VJ6A4	SM37A21311		MEMORY S M393A4K40CB2-CVF 32GB D4-29R
17	1000019769	xxxxxxxx	8SSM37A21311G1J1L5VJ69U	SM37A21311		MEMORY S M393A4K40CB2-CVF 32GB D4-29R
18	1000019769	xxxxxxxx	8SSM37A21311G1J1L5VJ6A3	SM37A21311		MEMORY S M393A4K40CB2-CVF 32GB D4-29R
19	1000019769	xxxxxxxx	8SSM37A21311G1J1L5VJ6A0	SM37A21311		MEMORY S M393A4K40CB2-CVF 32GB D4-29R
20	1000019769	xxxxxxxx	8SSM37A21311G1J1L5VJ6A6	SM37A21311		MEMORY S M393A4K40CB2-CVF 32GB D4-29R
21	1000019769	xxxxxxxx	8SSM37A21311G1J1L5VJ69Z	SM37A21311		MEMORY S M393A4K40CB2-CVF 32GB D4-29R
22	1000019769	xxxxxxxx	8SSM37A21311G1J1L5VJ6A1	SM37A21311		MEMORY S M393A4K40CB2-CVF 32GB D4-29R
23	1000019769	xxxxxxxx	8SSM37A21311G1J1L5VJ69X	SM37A21311		MEMORY S M393A4K40CB2-CVF 32GB D4-29R
24	1000019769	xxxxxxxx	8SSM37A21311G1J1L5VJ6A2	SM37A21311		MEMORY S M393A4K40CB2-CVF 32GB D4-29R

Figure 2. "As Built" data file screen capture (click to view a larger version)

The direct platform data file consists of component information that is programmatically readable from the system. A software utility runs and identifies what's installed in the server, where it will identify a hard disk if its installed, then read the model number, serial number, firmware version and other details. The utility will also read the platform configuration registers from the Trusted Platform Module (TPM) which represent system configuration values.

The software also talks to the TPM that's on the server motherboard to read the platform configuration registers representing system configuration values, and to read unique characteristics built into each TPM from the TPM manufacturer such as serial number, and cryptographic endorsement key, certificate. Since the TPM is soldered down to the motherboard it provides a unique representation that ties the collected data to a specific motherboard with specific components in a specific system.

How do I add Intel Transparent Supply Chain to my order?

To add Intel Transparent Supply Chain to your order simply add the following feature code in the DCSC configurator, under the **Security** tab.

Table 1. Feature code for Intel Transparent Supply Chain

Feature code	Description
BB0P	Intel Transparent Supply Chain

What are the benefits of adding this feature to my order?

The benefits of adding Intel Transparent Supply Chain can be summarized in four features, as follows:

 **Traceability**	 **Accountability**	 **Assurance**	 **Security**
Full component traceability linked to TPM	Detailed bill of materials and platform certificate digitally signed by Intel + access to the companion verification tool that provides digital proof of product origin.	Receive a higher level of information and proof compared to the current industry standard	Increased integrity and authenticity of the supply chain

Additionally, servers manufactured under the Intel Transparent Supply Chain program conform to the US Department of Defense Federal Acquisition Regulation (DFAR) 246.870-2/252.246-7007: Contractor Counterfeit Electronic Part Detection requirements.

What systems are currently supported on this program?

These are the Lenovo systems where you can currently add this enhanced security feature, with more to be added in the coming months, check back to this article for any updates.

Edge systems:

- ThinkSystem SE350

Mainstream rack systems:

- ThinkSystem SR150
- ThinkSystem SR250
- ThinkSystem SR530
- ThinkSystem SR550
- ThinkSystem SR570
- ThinkSystem SR590
- ThinkSystem SR630
- ThinkSystem SR630 V2
- ThinkSystem SR650
- ThinkSystem SR650 V2
- ThinkSystem SR670
- ThinkSystem SR670 V2

Cloud Service Provider/Hyperscale systems:

- ThinkSystem HR610X
- ThinkSystem HR630X

- ThinkSystem HR630X V2
- ThinkSystem HR650X
- ThinkSystem HR650X v2

Mission Critical systems:

- ThinkSystem SR850
- ThinkSystem SR850P
- ThinkSystem SR850 V2
- ThinkSystem SR860
- ThinkSystem SR860 V2
- ThinkSystem SR950

Dense/Blade systems:

- ThinkSystem SD530
- ThinkSystem SD630 V2
- ThinkSystem SD650 V2
- ThinkSystem SD650-N V2
- ThinkSystem SN550
- ThinkSystem SN550 V2
- ThinkSystem SN850

Tower Systems

- ThinkSystem ST250
- ThinkSystem ST550
- ThinkSystem ST650 V2

Software Defined Infrastructure

- ThinkAgile HX
- ThinkAgile VX
- ThinkAgile MX

Conclusion

Lenovo ISG has paired its industry leading supply chain with Intel’s innovative Transparent Supply Chain program to add a layer of protection to your data center and bring peace of mind that the server hardware you bring into it is authentic and with documented, testable, and provable origin.

Ask your Lenovo representative how this feature can be added to your purchase.

Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area. Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service. Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

Lenovo (United States), Inc.
8001 Development Drive
Morrisville, NC 27560
U.S.A.
Attention: Lenovo Director of Licensing

LENOVO PROVIDES THIS PUBLICATION ”AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary. Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk. Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

This document, LP1434, was created or updated on August 24, 2021.

Send us your comments in one of the following ways:

- Use the online Contact us review form found at:
  https://lenovopress.com/LP1434
- Send your comments in an e-mail to:
  comments@lenovopress.com

This document is available online at https://lenovopress.com/LP1434.

Trademarks

Lenovo and the Lenovo logo are trademarks or registered trademarks of Lenovo in the United States, other countries, or both. A current list of Lenovo trademarks is available on the Web at https://www.lenovo.com/us/en/legal/copytrade/.

The following terms are trademarks of Lenovo in the United States, other countries, or both:
Lenovo®
ThinkAgile
ThinkSystem

The following terms are trademarks of other companies:

Intel® is a trademark of Intel Corporation or its subsidiaries.

Other company, product, or service names may be trademarks or service marks of others.