Understanding and Implementing Intel® Transparent Supply Chain

A whitepaper describing Intel® Transparent Supply Chain

Rev 1.1

December 2015

Intel® Server Board and Systems

<Blank Page>

Document Revision History

Revision Number	Date Published	Description of changes
1.0	November 2015	Initial Release
1.1	December 2015	Update naming with legal naming

Document Disclaimer Statements

Intel technologies features and benefits depend on system configuration and may require enabled hardware, software or service activation. Learn more at Intel.com, or from the OEM or retailer.

You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Intel products described herein. You agree to grant Intel a non-exclusive, royalty-free license to any patent claim thereafter drafted which includes subject matter disclosed herein.

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

The products described may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

Intel, the Intel logo, Xeon, and Xeon Phi are trademarks of Intel Corporation in the U.S. and/or other countries.

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

Table of Content

1. Introduction

Since the mid-2000's, there are growing concerns that a counterfeit electronic part might cause the failure of a business critical application. Many of the concerns are described in the October 13, 2008 BusinessWeek cover story "Dangerous Fakes". A recent survey by Enterprise Strategy Group reports that 16% of companies in the study had purchased some form of counterfeit IT equipment between 2006 and 2008.[1] With no common methods to verify equipment authenticity, it seems likely there are more companies that are unaware of counterfeit IT equipment infiltrating their recent purchases.

In 2011, US Congress passed and President Obama signed into law new legislation requiring purchases controlled by Cost Accounting Standards (CAS) to "Detect and Avoid Counterfeit Electronic Parts".

In 2015, the Defense Federal Acquisition Regulation Supplement (DFARS) extend these requirements beyond "CAS" contracts to include the small businesses set-asides. Smaller contractors must now follow these new regulations.

When it comes to counterfeiting, we don't know what we don't know, so a good first step is to start looking at ideas and methods that protect us even when we are unaware of any specific threat. For several years, Intel has been researching methods to cost effectively mitigate risk. Intel shares most of this research openly through industry consortiums like the Semiconductor Industry Association (SIA), and standards development organizations like SEMI Standards International, ANSI, JEDEC, SAE, and ISO.

Many standards development actions at the industry, national, and international level were initiated to mitigate risks caused by counterfeiting. Continuing with these efforts to lead the charge in fighting counterfeit components, Intel is implementing a "transparent supply chain" which means that we enable visibility of individual component sourcing so that we enable end users to track these parts back to the original component manufacturer. This paper describes how Intel is putting transparency in the supply chain and what a system integrator needs to do in order to take advantage of it.

2. Overview of Transparent Supply Chain

When buying from authorized supply the risk of counterfeit components is dramatically reduced. Intel's goal is to buy from authorized supply. The benefit of the Transparent Supply Chain it that it allows the system integrator and all the way to the end user the ability to audit and validate the authorized supply chain. This is a capability that is not generally available in the market.

Transparency begins by collecting and storing data about each server board as it is being manufactured. From this data, Intel generates a "build report". As each server board is being assembled, the data detailing batch numbers and serial numbers are readily available. If this data is not collected during the board assembly process, it becomes very difficult to determine later.

The build report, also known as the "As-Built" report, contains the sourcing details for the components that have been used to build the product. Currently, this capability is only in place for the Intel server boards. The components included in the report consists of the bare PCB, passive components such as capacitors and resistors, and active components such as transistors, FETs and ICs. The report also includes the image source file name and the checksums of the programmable devices.

[1] http://www.esg-global.com/research-reports/cyber-supply-chain-security-revisited/

Component traceability is achieved by listing the sourcing information for each individual component. This sourcing information identifies where Intel procured the given component from. This report can be audited to check that Intel is procuring parts directly from the component manufacturer or from an authorized distributor of that manufacturer. Procuring parts directly from the component manufacturer or from an authorized distributor of that manufacturer is a new requirement of DeFARS section 246.870-2.

Procurement data that are captured before manufacturing includes: receiving the shipment invoice identifier, the storage container identifier, the part manufacturer, the part batch code or part date code, and the part model number. During the manufacturing process, procurement data are moved into the shop floor control system and recorded for each individual component inserted into each server board. By capturing these real time events as they happen on the manufacturing floor it becomes possible to generate a built report for each board. A typical built report lists the component's manufacturer, date code/batch code, and component's supplier/distributor. Each report file is accessed using each server board's individual serial number.

Firmware verification is performed during functional testing of the server board at the end of the manufacturing process. The functional test software reads the programmable device checksums and verify that it matches with the current firmware revisions of that motherboard. The checksum is the total of all the firmware so that when added up gives a unique value which can only be attributed to the correct software image.

Provisioning of the Trusted Platform Module (TPM) is the last step in the process. The TPM module is programmed at the end of the functional test once all of the firmware checksums have been read and verified. Intel completes the process by generating and signing an industry standardized Platform Certificate for each individual motherboard.

Customer documentation is the last step in the Transparent Supply Chain (TSC). With each and every server board supported by the TSC; a "Statement of Conformance" shall be produced. The statement of conformance (SoC) is a PDF file that is produced and digitally signed with Intel's private key from the Intel secure database. The SoC contains basic product information like the part number of the server and a list of the critical components purchased for that particular motherboard. The SoC is not digitally linked to the motherboard. For documentation that is digitally tied to a particular mother board Intel is offering a "Platform Certificate". In order to receive a Platform Certificate the motherboard must contain a TPM (trusted platform module). The TPM has public key which is placed in the Platform Certificate and digitally signed by Intel. In this way a platform certificate can be verified by a third party providing proof of purchase through Intel's Transparent Supply Chain.

3. Customer Responsibilities

3.1 Receiving Platform Certificates from Intel

Once the signed Platform Certificate is generated by Intel, it is ready to be transmitted to the system integrator. Methods of transmission can be established by mutual agreement between the system integrator and Intel. Examples include e-mail, FTP, or private web site. While it is true the integrity of the data in a Platform Certificates is protected by the digital signature, Platform Certificates contains data specific to each server board that should remain confidential. Some form of encryption should be used to transfer Platform Certificates from suppliers to customers.

3.2 Reading and Verifying the Platform Certificates

Platform Certificates delivered by Intel conform to the ITU Telecommunication Standardization Sector (**ITU-T**) X.509 version 3 standard. Following industry standards for the Platform Certificates enables access and support from a variety of existing industry tools that display and verify the content of a Platform Certificate.

3.3 Integrator Platform Certificates

The Platform Certificate from Intel provides assurance to the end customer that the platform was manufactured through the Intel®Transparent Supply Chain process. In addition to the Platform Certificate, the system integrator has the option of creating and providing an Appliance Certificate to the end customer. The purpose of an Appliance Certificate is to allow the integrator to make security claims about what they have added to the platform. The Appliance Certificate will assert that there were additional capabilities added to the bare platform by the integrator.

An integrator can create an amended (Appliance) Certificate to inform software about proprietary features added by the integrator. First, the integrator must procure a PKI key-pair from Certification Authority that will be used to sign the new Certificate. As with any key-pair, the integrate needs to protect the private key of this pair. The integrator incorporates the Intel server board into their product and adds their features. After checking the Platform Certificate (using the three step process from above) the integrator copies the TPM public key contained in the Platform Certificate signed by Intel into the new amended Certificate and then the integrator uses their private key to sign the amended Certificate.

4. How An End User Challenges a Platform Certificate

4.1 Certificates use “Keys”:

Platform Certificates use a digital and secure identity management scheme called “Public Key Infrastructure” also known as “PKI”. In this scheme, everyone who uses PKI agrees to trust a “Certification Authority” (also known as “CA”) to issue “Keys”. In other words, you agree to trust any “Key” issued by the “CA”. This also means you need to “black list” any CA that you don’t trust to prevent tools from using keys issued by the CA you don’t trust. Trust concerns and issues about any specific CA’s should be disclosed and negotiated long before manufacturing begins.

So let’s just assume you agree to trust the company that Intel uses for PKI keys. For example, one of the Certification Authorities Intel might use is USERTrust. While you might not know of USERTrust, it is likely security folk in you IT department know of them. In this example, Intel is going to create a chain of keys as follows: USERTrust -> Intel -> Platform Certificate.

4.2 What is a “Key”?

In the PKI scheme, keys are created and issued in pairs. Each key is more correctly called a key-pair. Each key in the pair is just a long and random binary number. One of these long random numbers is called the “public key” and the other is called the “private key”. It is critically important to protect the private key and never ever tell anyone the details of the private key. The details of the private key must be kept secret. The specific detail that must be kept secret is the long random binary number known as the private key. These random numbers are used in a complex mathematical equation to encrypt and decrypt information.

Remember: Keep your private key secret.

The public key is also a long binary number that is not the same as the private key, and you must tell other people all the details of the public key. Public Key Infrastructure (PKI) is the convenient method Intel uses to inform the world about the details of the public keys used with Platform Certificates. Every platform certificate contains a public key that is unique and specific to that platform.

4.3 Public Key relationship with Private Key:

PKI key-pairs are used to encrypt and decrypt files. You can choose either the public or the private key to encrypt a file. You encrypt with one key of the pair and then decrypt using the other key. If you encrypt a file using the public key, that file can only be decrypted using the private key. If you encrypt a file using the private key, that file can only be decrypted using the public key.

Let's assume I did a good job of keeping my private key secret and I am the only entity in the world that knows what it is and let's assume everyone in the world knows my public key. If I encrypt the text file containing: "this message is from me" using my private key, then only my public key can decrypt that file. Anyone can use my public key can decrypt and trust the message really is from me because I am the only person with the private key. If the message was encrypted with a different private key that is not my private key, then my public key WILL NOT decrypt the message. My public key only decrypts messages encrypted with my specific and secret private key. If you can decrypt a message with my public key, then that message was encrypted using my private key. This is the basis of digital signatures. AND, this is why it is so important to keep the private key a secret.

Now, let's say you want to send a message that only I can read. If you encrypt the message using my public key, only my private key can decrypt it. Since I have done a good job keeping my private key secret, I am the only one who can decrypt the message and read it.

Finally, if things go wrong and some malicious person finds my private key and makes a copy, I need to tell the Certification Authority to revoke the key-pair. It is important to check with the CA before using and trusting a key-pair.

4.4 Using Platform Certificates:

For server boards, Platform Certificates are used to make statements or "claims" regarding important security features and functions available on a platform. Platform Certificates require use a Trusted Platform Module (TPM). A TPM is a device that enables software running on the platform to test security features of the platform before using or exposing sensitive information. Checking before exposing reduces the risk of the sensitive information being sent to a malicious or corrupted platform.

Checking a Certificate is a three-step process. The first step is to test that the key-pair used to sign the Certificate is still valid and has not been revoked. The second step is to test that the Certificate is indeed signed using the key-pair you just tested in step one. Then the third step is to use the public key in the Platform Certificate to test that the TPM the software is using is the same TPM Intel installed in the platform. After running this three step check, the software knows it is running on a server board that was built by Intel.

Step one: Check that the key-pair is valid

> A program or app on your computer reads the Platform Certificate to discover the chain of trust that links back to the Certificate Authority (CA). Your computer sends a key-pair query to the CA and the CA responds with the status of the key-pair. (If the key-pair was revoked, something went wrong, so stop.)

Step two: Test the Certificate's signature

The Certificate was signed using an Intel private key. A program or app will use the Intel public key to decrypt a message that is part of the signature and verify the decrypted message is an exact match with a part of the signature that was not encrypted.

Think of the digital signature as two pieces. The first piece of the message is "Intel signed this". The piece of the message is "Intel signed this" encrypted with Intel's private key. After encryption, the second piece looks something like "*&4%)n(J#-+K?%j#0", a message of the same length, but complete gibberish. Only Intel's public key can decrypt the gibberish back into the legible phrase "Intel signed this". If the program succeeds in decrypting the message with Intel's public key, then we know Intel's private key was used to sign the Certificate.

Step three: Challenge the TPM

The TPM also has a key-pair that is unique to that TPM. The Platform Certificate has a copy of the public key for the TPM. Only the TPM itself knows the private key that pairs with the public key in the Platform Certificate. So to challenge the TPM, a program or app running on the platform uses the TPM public key it reads from the Platform Certificate to encrypt a random message and sends that message to the TPM with the command, decrypt this and send it back to me. The TPM uses the private key to decrypt the message and sends it back. If the message is decrypted, then the program knows it is talking to the expected TPM.

5. Frequently Asked Questions

5.1 Is a TPM required for Transparent Supply Chain?

No, a TPM is not required for Transparent Supply Chain. A TPM is required to generate a Platform Certificate. However, if the server board does not include a TPM, Intel can provide a digitally signed Statement of Conformance in lieu of a Platform Certificate.

5.2 How long is the Platform Certificate available?

The Platform Certificates will be available for 20 years.

5.3 How long is the As Built Data available?

The As Built Data will be available for 20 years.

5.4 How Do I get the the Platform Certificate available?

Intel Server Edge Website. Enter stocking ID and Serial # of the motherboard and then you can download it. For large orders we will have a different way to get them the certificates

5.5 How Do I get the As Built Data available?

This is part of the audit. You have to request it.