Power Systems

Secure boot in PowerVM

Note

Before using this information and the product it supports, read the information in “Notices” on page 11 .

This edition applies to IBM® AIX® Version 7.2, to IBM AIX Version 7.1, to IBM AIX Version 6.1, to IBM i 7.4 (product number 5770-SS1), to IBM Virtual I/O Server Version 3.1.1, and to all subsequent releases and modifications until otherwise indicated in new editions. This version does not run on all reduced instruction set computer (RISC) models nor does it run on CISC models.

Contents

Secure Boot in PowerVM

IBM Power Systems servers provide a highly secure server platform. IBM POWER9™ processor-based hardware and firmware includes new PowerVM® features to provide a more secure platform for cloud deployment.

The key PowerVM features available in POWER9 processor-based servers, include:

- A secure initial program load (IPL) process or the Secure Boot feature allows only appropriately signed firmware components to run on the system processors. Each component of the firmware stack, including hostboot, the POWER Hypervisor (PHYP), and partition firmware (PFW), is signed by the platform manufacturer and verified as part of the IPL process.
- A framework to support remote attestation of the system firmware stack through a hardware trusted platform module (TPM).

Secure Boot and Trusted Boot

For this documentation, the terms *Secure Boot* and *Trusted Boot* have specific connotations. The terms are used as distinct, yet complementary concepts.

Secure Boot
The Secure Boot feature protects system integrity by using digital signatures to perform a hardware-protected verification of all firmware components. It also distinguishes between the host system trust domain and the flexible service processor (FSP) trust domain, by controlling service processor and service interface access to sensitive system memory regions.

Trusted Boot

The trusted boot feature creates cryptographically strong and protected platform measurements that prove that particular firmware components have run on the system. You can assess the measurements by using trusted protocols to determine the state of the system and use that information for security decisions.

What's new in Secure boot in PowerVM

Read about new or changed information in Secure boot in PowerVM since the previous update of this topic collection.

August 2018

- Miscellaneous updates were made to this topic collection.

Terms

Learn about the terms that are used in this documentation.

Adjunct
A child partition that uses CPU allocated to another partition. An adjunct is readily available to the system administrator and it can be used to service the main partition.

Alter/Display Unit (ADU)
A hardware resource that is used to access the main storage. An ADU is used by the hardware and firmware elements.

Code container
A verifiable code image that has a Secure Boot prefix header. The container is a structure that consists of a 4K prefix header (hardware header, prefix key header, or firmware header), followed by a

protected payload (a code image that has a hash in the prefix header), and any unprotected payload data that is unique to the server.

Code-signing authority
The authority level that is granted to individuals who have knowledge about the subject code to enable fulfillment of a role as authorized signer for signing server functions.

Core Root of Trust for Measurement (CRTM)
A priority trusted (immutable) code that is part of the platform credential. In the Static RTM Model, the CRTM code must be run first when the server or the physical hardware environment is powered on, or when the server or the physical hardware environment is reset. For the Secure Boot feature, the CRTM code is based on self boot engine/hostboot (SBE/HB). The CRTM code includes the self boot engine and sufficient hostboot code to allow a TPM device driver to initialize.

Management Console (MC)
An interface for system administrators and service representatives to view and perform tasks on the hardware, partitioning, and service aspects of a system.

Master processor
Processor in the node that is physically attached to the not-OR (NOR) flash memory.

PCR extend
An operation that is performed on the TPM platform configuration registers (PCR) to update the register value to record the history of messages that are extended to the register. Rather than performing the write operation directly on a PCR, the PCR extend operation takes the original value in the PCR, concatenates the new message to it, and takes a hash to produce an updated register value. The history of messages that are extended and the order of extents can be compared later with corresponding TPM event logs.

Platform certificate
Certificate that exists in the TPM, which certifies the TPM associated platform to be an IBM platform with a CRTM code. The certificate is not dependent on the platform model.

PNOR
Processor not-OR (PNOR), also known as flash.

Prefix header
A 4 KB structure that is prefixed to signed code images of Secure Boot code containers.

Private key for code signing
Private or secret portion of a public/private key pair that is used for public key cryptography, by using asymmetric key algorithms.

Protected registers
Registers that are read only by using scan communication (SCOM) by flexible service processor (FSP) but are read/write by using trusted code. In most cases, these registers are independent of the value that is scanned at initialization and default to a known value.

Public key for code signing
Public or published portion of a public/private key pair that is used for public key cryptography, by using asymmetric key algorithms.

Remote attestation
Checks which software is running on a remote computer. Attestation is the process of validating the accuracy of information. Remote attestation allows authorized stakeholders to determine changes to the user's computer, by checking the status of both the TPM and the platform on which it resides.

Self Boot Engine (SBE)
Is the Power-on Reset engine that is used for initializing the processor chip to run the hostboot procedures.

Signature
Demonstrates authenticity of a message. The signature consists of the hash of the subject message that is encrypted with one half of a public/private key pair.

Static Root of Trust for Measurement (SRTM)
A system boots from an immutable portion of the firmware code that is assumed to be trusted at all times. The booting action initiates the measurement process, in which each component measures the next component in a chain.

Trusted Building Blocks (TBB)
Includes the portions of the roots of trust measurement (RTM) that do not have protected locations or protected capabilities. TBB includes the CRTM, connection of the CRTM storage to a system board, the connection of the TPM to a system board, and mechanisms for determining physical presence of the user.

Trusted code
Firmware that is authorized by predesignated IBM hardware and firmware authorities. The source of the code is authenticated and the image is checked for integrity.

Trusted Computing Group (TCG)
The Trusted Computing Group is a not-for-profit organization that is formed to develop, define, and promote open, vendor-neutral, global industry standards, supportive of a hardware-based root of trust measurement (RTM), for interoperable trusted computing platforms.

Trusted memory
Memory region that is accessible (read and write) only by trusted code. Access to trusted memory is blocked by hardware isolation mechanisms when the system boots in secure mode. A small section of memory that is outside the trusted memory region is referred to as *untrusted memory* and it can be readily accessed by service interfaces to perform read and write operations.

Trusted Platform Module (TPM)
Smartcard-like low-performance cryptographic coprocessor. A TPM can store hashes of the boot sequence in a set of Platform Configuration Registers (PCRs).

Untrusted memory
Memory region with open read and write access that includes flexible service processor (FSP) and service interfaces that exist outside the security domain of the host processors.

Validation
Verify the identity of the signer, for example, validation of a code container means to verify that the code in the contained image is digitally signed by IBM and that the image is unmodified.

Verification code
Protected code exists in the serial electrically erasable programmable read-only memory (SEEPROM) and provides the signature verification support for the Secure Boot code containers. The verification code is the key element that is used to establish the core root of trust for measurement during Secure Boot.

Secure Initial Program Load (IPL) process

The Secure Boot feature prevents unauthorized access to customer data, either through unauthorized firmware that runs on a system processor, or by access through security vulnerabilities in authorized service processor firmware, or through hardware service interfaces accessed through flexible service processor (FSP).

While the Secure Boot feature prevents unauthorized access to customer data, the Secure Boot mechanisms do not provide protection against the following threats:

- Operating system software-based attacks to gain unauthorized access to customer data.
- Rogue system administrators.
- Hardware physical attacks (for example, chip substitutions and bus traffic recording).

The Secure Boot feature implements a processor-based chain of trust in the POWER9 processor hardware that is enabled by the POWER9 firmware stack. The Secure Boot feature provides a trusted firmware base to enhance confidentiality and integrity of customer data in a virtualized environment.

The trusted boot feature of POWER9 processor-based servers allows measurement of system configuration and initial program load (IPL) path code, which can be used later as proof, through attestation of the initial IPL path configuration of the system. To create a Core Root of Trust for these Measurements (CRTM), a Secure Boot flow is used that adds cryptographic checks in each phase of the IPL process until communication with the Trusted Platform Module (TPM) is established. The Secure Boot flow ensures the integrity of all firmware that must be run on core processors, thus preventing any unauthorized or maliciously modified firmware from running. A failure to authenticate the code at any point prevents the IPL process from reaching completion.

The Secure Boot feature in POWER9 systems establishes trust through the platform boot process. Here, *trusted* means that the code that is run during the IPL process originates from the platform manufacturer, is signed by the platform manufacturer, and has not been modified.

The secure mode protection available in POWER9 processor-based servers maintains trust, by preventing read/write access to the customer data by the FSP and service interfaces, by preventing execution of untrusted code on the host processor, and by maintaining trust across all the key points in the Secure Boot process.

The POWER9 Secure Boot feature implements a processor-based chain of trust. The chain starts with an implicitly trusted component, while other components are authenticated and checked for integrity before they are run on host processor cores. The verification code that is in the locked processor in the Serial Electrically Erasable Programmable ROM (SEEPROM) validates the initial firmware load. The firmware verifies cryptographic signatures of all subsequent firmware that must be trusted and that are loaded for execution on the POWER9 processor cores. On a POWER9 system, the SEEPROM security switches are set in the Self-Boot Engine (SBE) code and fixed on the manufacturing (MFG) assembly line of the system to provide the basis for hardware enforcement of secure IPL flows. Physical security mode jumpers are available on the *backplane* of a system. The jumpers can be used to override secure mode switches of the processor if the system is physically accessed by a person. The secure IPL process further enhances trusted computing Power® platform.

The following diagram illustrates the operations of a secure and trusted boot IPL process.

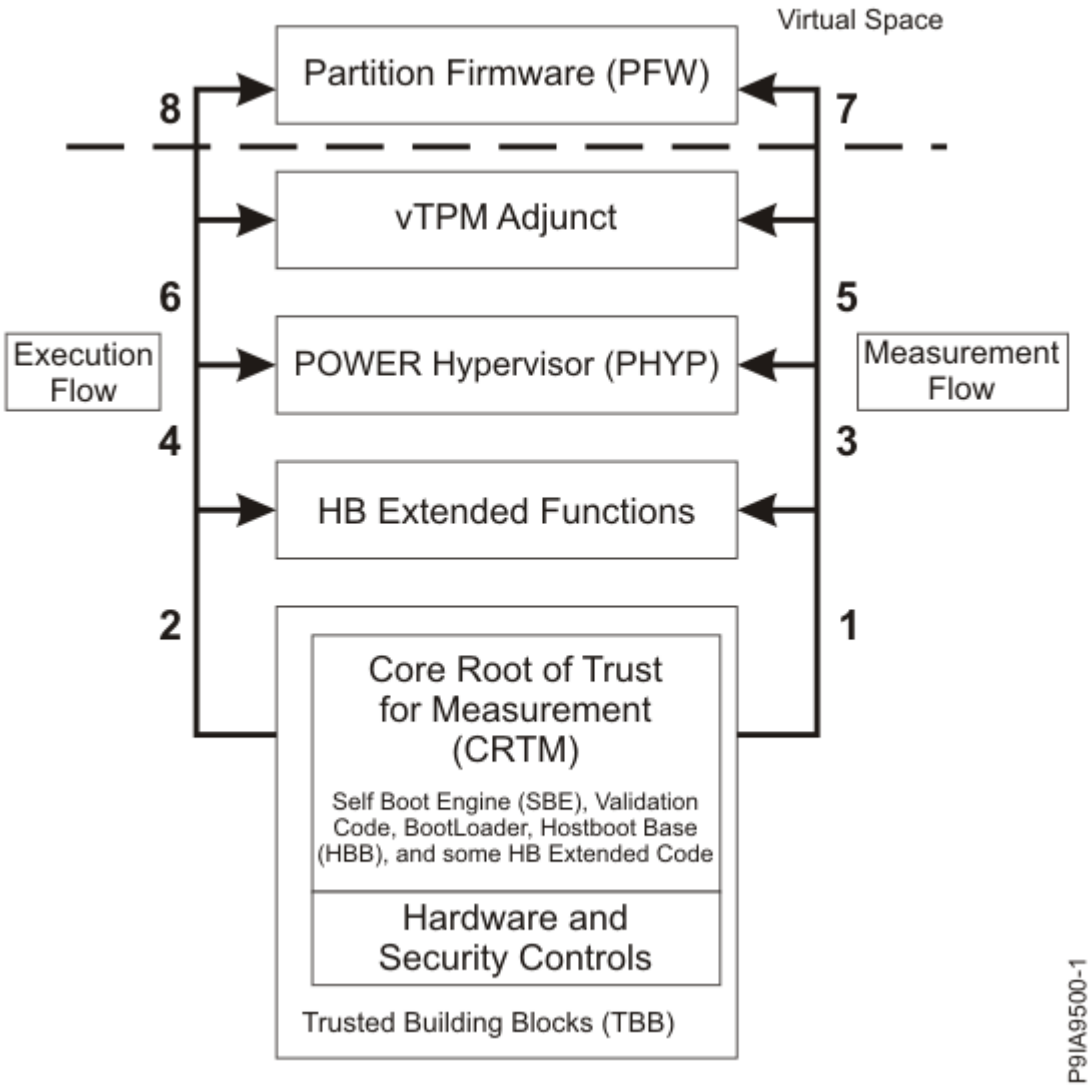

Figure 1. Secure and Trusted Boot flow

The Secure Boot feature establishes the locked SEEPROM, SBE, and host boot base code (including a small portion of host boot extended code) as the Core Root of Trust for Measurement (CRTM), with the chain of trust extended to include POWER Hypervisor (PHYP), partition firmware (PFW), selected adjunct partitions (physical trusted platform module (pTPM), virtual trusted platform module (vTPM), host boot runtime, and encryption adjuncts), and On Chip Controller (OCC – thermal management). This trust domain and the processor hardware security support ensures that the customer data is not displayed or altered through any hardware or firmware mechanisms.

The complete trusted firmware stack is authenticated by using signed images and is run in trusted memory locations. The FSP is kept out of the host server trust domain and the FSP is blocked from accessing Alter/Display Unit (ADU) registers, other protected registers, and trusted memory regions. The Self Boot Engine (SBE) enforces FSP blocking, by filtering the blacklist of processor register read/write scan communication (SCOM) facilities. The SCOM facilities are enabled by the secure access switch in the SEEPROM area of the processor chip.

The following figure shows the Secure Boot environment.

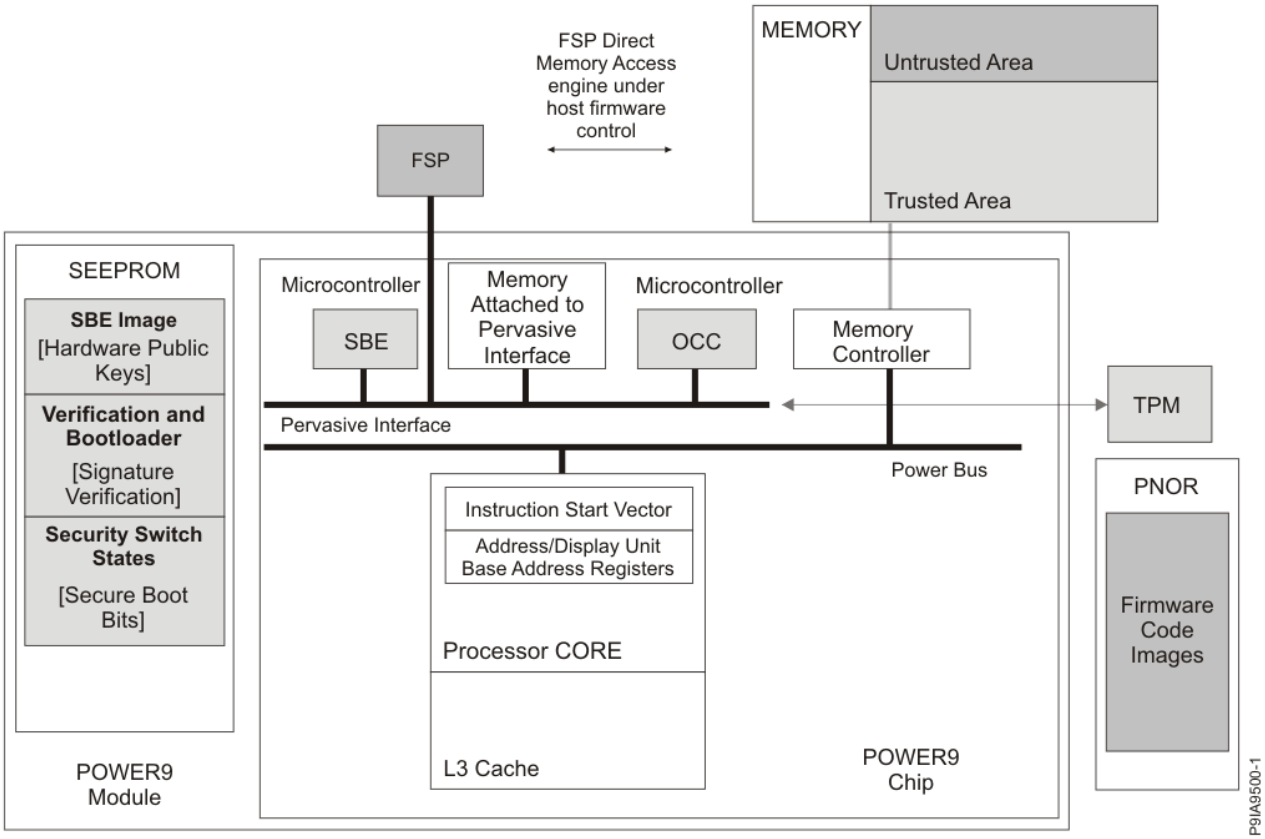

Figure 2. The Secure Boot environment

When the Secure Boot process starts, the FSP element sends a boot request and details about the boot-type to processor chips in the system. Internally, the state of the Secure Boot logic is cleared of previously set values to start from an appropriate, known state. The state is also cleared of any tempering requests that were run previously. Hardware protection mechanisms are implemented to prevent a malicious attacker from skipping this initial step. The access from the FSP to internal chip resources is locked and the Secure Boot engine starts fetching initialization code from memory that is on-module, secure, nonvolatile, and locked. This code performs basic chip initialization and resets the TPM.

After the initial step in the booting process is completed, the Self Boot Engine (SBE) loads the host boot loader and validation code from SEEPROM into the internal L3 cache of the processor chip. A processor core is then started and the boot loader fetches the initial Host Boot Base (HBB) code from Processor NOR (PNOR) flash chip and loads it into the L3 cache. In secure mode, the validation code from the L3 cache is used to verify the HBB image that is now available in the trusted cache. After the initial flash code is verified, the processor core continues to run the validated code from the trusted memory space, and loads and validates HB extended functions (HBI). After the HBI is measured and the signature is verified and copied, its measurement (image hash), indicating valid authentication, is recorded in the TPM, as indicated by **Step 1** in Figure Secure and Trusted Boot flow. At this point, all code that is run is fully contained in the PNOR flash chip and the system has not been accessed by any other mechanisms. This is referred to as the boundary of the trusted boot. In case the verification fails, the system is immediately stopped and is protected by hardware protection mechanisms to prevent execution of untrusted or rogue code.

The HB code then manages any pending updates of the secure nonvolatile memory by using a new trusted image. To protect the Core Root of Trust (CRTM), the HB code locks the secure memory, thereby preventing any further write access to that memory (this action means that if the system is rebooted, it returns to this trusted state). The HB code then initializes the on-chip memory controller and the attached memory dual inline memory modules (DIMMs). The HB code also initializes other chips that are directly attached to the processor on which it is running before it establishes the memory coherent interface to the other chips in the system. These other chips are also verified to ensure that they are in a secure and trusted state.

Higher firmware stack components are then loaded, verified, run, and their measurements are recorded in the TPM. This action completes **Step 2**, which is indicated in Figure Secure and Trusted Boot flow. In **Step 3** of the figure Secure and Trusted Boot flow, the POWER Hypervisor (PHYP) payload is loaded into main memory. Then, the code is cryptographically authenticated and after successful authentication, the PHYP starts to run. The authentication measurement of the PHYP code is recorded in the TPM. Similarly, **Steps 4 through 8**, which are indicated in Figure Secure and Trusted Boot flow are performed to load the code from unlocked flash memory to trusted memory, the code is cryptographically authenticated, and then various adjuncts and partition firmware (PFW) are run.

Physical TPM support in Secure Boot

The trusted platform module (TPM) enables remote attestation of the code stack on a running system. The chain of trust firmware records the hash of the loaded firmware and stores the records in the network of processor TPMs. The network can consist of one physical TPM per master processor on low-to-mid range platforms, or redundant TPMs through master or alternate-master processors on multi-node enterprise platforms. The chain of trust firmware also records all events appropriately in TPM event logs.

The attestation supports Trusted Computing Group (TCG) 2.0 compliant trusted boot. The TPM infrastructure supports a reference remote attestation implementation that is open-sourced by IBM.

The host processor TPM is prepared for remote attestation in the manufacturing (MFG) industry and includes a provisioning phase and an initialization phase. *TPM Provisioning* is a one-time process and is performed on the field-replaceable unit (FRU) of the TPM module before assembling the system. *TPM Provisioning* prepares the TPM to provide the necessary security services to its full-stack users. *TPM Provisioning* includes setting TPM preconfiguration values, authorization values and policies, provisioning hierarchies, and installing relevant certificates and keys in the TPM nonvolatile (NV) space, to bind the certificates to the specified TPM. This process includes establishing an endorsement key and platform certificate for single-node systems, and a node certificate for multi-node systems. At this stage of processing, the system requires a certification from an IBM certificate authority.

TPM Initialization is performed by firmware once per initial program load (IPL). The TPM then transitions from a power off state (reset asserted or TPM power not applied) to an initialized state. *TPM Initialization* includes resetting of the Roots of Trust for Measurement, validation of TPM firmware, and preparation for accepting commands on the TPM interface. The TPM self-test (extent as defined by platform startup policy) is completed before the TPM enters a fully operational mode.

Provisioning TPM 2.0

Learn about the Trusted Platform Module (TPM) provisioning process.

The *TPM Provisioning* process in the manufacturing (MFG) industry has the following requirements:

- TPMs must be available on pluggable cards for all POWER9 platforms. This requirement provides for a single point of control for *TPM Provisioning*. *TPM Provisioning* is designed based on the POWER7®/ POWER8® Vital Product Data (VPD)/Anchor Card process.
- *TPM Provisioning* must be performed through an offline subassembly process (not the MFG box assembly-line process).
- After *TPM Provisioning*, the TPM card is still considered a generic card that does not have system or order-specific information.
- After the TPM card is provisioned, it becomes an Asset Protection Classification number 3 (APC3) part (as defined in secure supply chain tracking).
- *TPM Provisioning* requires connectivity to an IBM certificate authority while provisioning the TPM card.
- *TPM Provisioning* requires a process to restore the TPM card to a shippable state for canceled fulfillments.

TPM event logs

When a Trusted Platform Module (TPM) Platform Configuration Register (PCR) Extend operation is performed, an event log entry is recorded in a TPM Event log file. This log file is used by external entities

that depend on remote attestation and by host firmware during multi-node synchronization. The log files are used to reconstruct and validate the PCR values against known values. The event log files are not maintained by the TPM. Thus, the firmware must provide storage for the log files and provide interfaces to update the log files on PCR Extends and access the log files for attestation purposes.

Because the initial *PCR Extend* operations are performed by the Host Boot (HB) code, when POWER Hypervisor (PHYP) is started, the event log information that is associated with the initial program load (IPL) time Extend operations are saved in the HB code. The HB code also communicates the relevant event log entries to PHYP through the host data area (HDAT) structure.

The PHYP maintains the TPM event log information in the physical TPM (pTPM) adjunct state. A maximum of 64 MB of storage area is allotted for each TPM log file. Preference is given to log entries that are created for concurrent firmware updates (also known as, unbounded log entries). Low and mid-range platforms have a single pTPM per node. Multinode enterprise platforms have another (redundant) pTPM per node.

If a TPM log buffer is full, additional *PCR Extend* operations to the TPM are allowed. The truncation of the log file is recorded and the attestation interfaces receive a flag that indicates that the delivered log files have been truncated.

At the time of initial program load (IPL), *PCR Extend* operations that have appropriate event log information are created. *PCR Extend* operations are also created for concurrent firmware updates. The log files include code measurements and configuration and platform history.

Current estimates on a first (cold) IPL are 50 event records per node on a single node system, and 200 event records per node on a four node system (at 128 B per event record, this rate is 25 KB per node per IPL).

The TPM event log information can be obtained through a resource dump. The event log files are NOT migrated with logical partitions because the log files are associated with the physical platform. Thus, the TPM history of the physical TPMs (pTPMs) might not be the same as the TPM history of the logical partitions.

TPM configuration settings that do not require a node TPM during a first (cold) or subsequent (warm) IPL do not require event log files. However, if the **TPM Required** option is set, *PCR Extend* operations and associated event log files must be maintained.

Signatures and keys in Secure Boot

The security design uses asymmetric keys and the hash of the hardware public keys is stored in the Serial Electrically Erasable Programmable ROM (SEEPROM). The verification code from SEEPROM, along with the hardware public keys and additional software public keys, is used to validate the signatures of the firmware code images in the code containers. Each firmware image that must be run on the core processors is loaded into the system memory as a code container, comprising a prefix header with the necessary security information and the code image. The container validation process ensures code integrity (that is, the code remains unmodified) and code authentication (that is, signed by proper authority).

The code signing private keys are stored in a secure hardware (for example, IBM 4767 Cryptographic Coprocessor) behind a firewall with restricted access and full audit controls.

Remote attestation of system software

The Trusted Platform Module (TPM) enables remote attestation of the code stack on a running system. The chain of trust firmware records the hash of the firmware that is loaded and stores the records in the network of Secure Boot TPMs. The network can have one physical TPM per master processor on POWER9 processor-based platforms. The attestation supports Trusted Computing Group (TCG) 2.0 compliant trusted boot. The identified TPM infrastructure supports future attestation stacks.

Physical attestation interfaces allow a trusted third-party client to retrieve information about the trusted boot state of the target PowerVM system. This process uses the physical TPMs of the system that are TCG 2.0 compliant devices. These TPMs are used by the system firmware to extend measurements during the boot process.

Notices

This information was developed for products and services offered in the US.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

INTERNATIONAL BUSINESS MACHINES CORPORATION 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. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work must include a copyright notice as follows:

© (your company name) (year).
Portions of this code are derived from IBM Corp. Sample Programs.
© Copyright IBM Corp. _enter the year or years_.

If you are viewing this information in softcopy, the photographs and color illustrations may not appear.

Accessibility features for IBM Power Systems servers

Accessibility features assist users who have a disability, such as restricted mobility or limited vision, to use information technology content successfully.

Overview

The IBM Power Systems servers include the following major accessibility features:

- Keyboard-only operation
- Operations that use a screen reader

The IBM Power Systems servers use the latest W3C Standard, WAI-ARIA 1.0 (www.w3.org/TR/wai-aria/), to ensure compliance with US Section 508 (www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards) and Web Content

Accessibility Guidelines (WCAG) 2.0 (www.w3.org/TR/WCAG20/). To take advantage of accessibility features, use the latest release of your screen reader and the latest web browser that is supported by the IBM Power Systems servers.

The IBM Power Systems servers online product documentation in IBM Knowledge Center is enabled for accessibility. The accessibility features of IBM Knowledge Center are described in the Accessibility section of the IBM Knowledge Center help (www.ibm.com/support/knowledgecenter/doc/kc_help.html#accessibility).

Keyboard navigation

This product uses standard navigation keys.

Interface information

The IBM Power Systems servers user interfaces do not have content that flashes 2 - 55 times per second.

The IBM Power Systems servers web user interface relies on cascading style sheets to render content properly and to provide a usable experience. The application provides an equivalent way for low-vision users to use system display settings, including high-contrast mode. You can control font size by using the device or web browser settings.

The IBM Power Systems servers web user interface includes WAI-ARIA navigational landmarks that you can use to quickly navigate to functional areas in the application.

Vendor software

The IBM Power Systems servers include certain vendor software that is not covered under the IBM license agreement. IBM makes no representation about the accessibility features of these products. Contact the vendor for accessibility information about its products.

Related accessibility information

In addition to standard IBM help desk and support websites, IBM has a TTY telephone service for use by deaf or hard of hearing customers to access sales and support services:

TTY service
800-IBM-3383 (800-426-3383)
(within North America)

For more information about the commitment that IBM has to accessibility, see IBM Accessibility (www.ibm.com/able).

Privacy policy considerations

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user, or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as the customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM's Privacy Policy at http://www.ibm.com/privacy and IBM's Online Privacy Statement at http://www.ibm.com/privacy/details the section entitled "Cookies, Web Beacons and Other Technologies" and the "IBM Software Products and Software-as-a-Service Privacy Statement" at http://www.ibm.com/software/info/product-privacy.

Programming interface information

This Secure boot in PowerVM publication documents intended Programming Interfaces that allow the customer to write programs to obtain the services of IBM AIX Version 7.2, IBM AIX Version 7.1, IBM AIX Version 6.1, IBM i 7.4, and IBM Virtual I/O Server Version 3.1.1.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at Copyright and trademark information.

Terms and conditions

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability: These terms and conditions are in addition to any terms of use for the IBM website.

Personal Use: You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative works of these publications, or any portion thereof, without the express consent of IBM.

Commercial Use: You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights: Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.