• Using the z13 cryptographic hardware, you gain security from using the Central Processor Assist for Cryptographic Functions (CPACF) and Crypto Express5S through in-kernel cryptography APIs and, for Linux on z Systems, the libica cryptographic functions library.
The benefits of using these features are:
- File system encryption
- Communication encryption (to the applications such as IBM HTTP Server)
- System security by providing advanced cryptographic functions
• z Systems is the only commercial operating system that has achieved EAL 5+ certification.
- This certification means that although different workloads are running on the same hardware, they are protected when running in separate partitions; one logical partition (LPAR) cannot reach across boundaries into the next LPAR and compromise its security.
- The LPARs are allocated their own resources and are secure and separate environments.
• Integrated cryptographic features provide leading cryptographic performance and functions.
- Reliability, availability, and serviceability (RAS) support for the Crypto Express5S is unmatched in the industry.
- IBM is in the process of gaining FIPS 140-2 Level 4 certification for the Crypto Express5S feature.
- With FIPS 140-2 Level 4 certified cryptographic hardware, IBM provides the most secure tamper-sensing and tamper-resistant security module that is available in the market.
• Business-driven enterprise security can be encapsulated by a concept that's known as the IBM Security Framework.
- The IBM Security Framework provides a business view of the security posture of an enterprise.
- It is a high-level view, but it incorporates all that is necessary for consideration.
The IBM Security Framework has the following features:
- Enables innovation through security-rich, end-to-end infrastructures and platforms.
- Reduces the number and complexity of required security controls.
- Reduces redundant security expenses.
- Improves organizational and operational agility and resiliency.
- Leverages industry expertise to help unify policy management.
- Delivers needed visibility, control, and automation.

The PCI DSS was created jointly in 2004 by four major credit card companies: Visa, MasterCard, Discover, and American Express. The z13 solution can help secure data and IT infrastructure end to end and help you to exceed your PCI DSS goals.

Solution overview

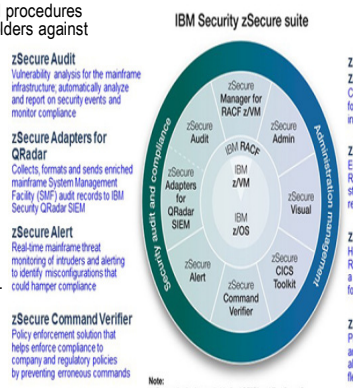
• To effectively detect and prevent security breaches, security intelligence and powerful analytics must be implemented.
• The solution to this is the IBM z13 with new Common Cryptographic Architecture (CCA) enhancements that were recently announced include:
- VISA format preserving encryption (VFPE): The z13 offers VFPE for payment card account numbers.
Note: The z13 can help provide additional security by enabling legacy databases and applications to contain encrypted data of sensitive fields without having to undertake a restructuring of the database or applications. FPE is a valuable tool for payment card applications that helps maintain the character length between input clear text and resulting cipher text.
- Greater than 16 domain support: Greater than 16 domain support allows a cryptographic coprocessor to be shared across more than 16 domains, up to the maximum number of LPARs on the system.
Note: This support relies on enhanced firmware that is available with a minimum microcode level for the Crypto Express5S coprocessor. With the adjunct processor (AP) extended addressing (APXA) facility installed, the z Systems crypto architecture can support greater than 16 domains in an AP.
- Customers have the flexibility of mapping individual LPARs to unique crypto domains or continuing to share crypto domains across LPARs.
• These enhancements use the following IBM z Systems features, which also are redesigned to provide even more security and performance:
- Cryptographic Functions (CPACF) and Crypto Express5S CPACF is designed to improve performance for cryptographic functions.
Note: The optional Cryptographic Coprocessor adapter (Crypto Express5S) provides new virtualization capabilities and performance increases.
- SIMD allows construction of richer, complex analytics models that use SIMD to provide better accuracy of insight:
o Allows analytics workloads to be ported from IBM Power and x86 with ease, and can accelerate analytics to provide speedy business insight.
o Increases programmer productivity of ISV and customer analytics workload development leading to rapid business insight generation for competitive advantage.
- SMT: Process more workloads (throughput for IFLs).
• The Payment Card Industry Data Security Standard (PCI DSS) is a widely accepted set of policies and procedures that is intended to optimize the security of credit, debit, and cash card transactions and protect cardholders against misuse of their personal information.
Note: It applies to all entities, including merchants and service providers that store, process, or transmit cardholder data, such as Personal Account Number (PAN) data.
• Additionally, the following z Systems security software supports PCI-DSS compliance:
- IBM Resource Access Control Facility (IBM RACF®): The premier External Security Manager (ESM) for IBM z/OS® and IBM z/VM® environments.
- Integrated Cryptographic Service Facility (ICSF): The component of z/OS that provides cryptographic services interfaces (APIs).
- IBM Security Identity Manager: The IBM solution for Enterprise Identity Management
- Encryption Facility for z/OS: Encrypts (and optionally compresses) data at rest for media whose contents must be securely transported, that is, physically moved, for example, shipped in a truck, or electronically sent over non-secure links.
- IBM Security zSecure™ Suite: A comprehensive suite of products that enhance the management, auditing, reporting, and compliance of security in RACF, CA-ACF2, and CA-Top Secret environments.
This suite includes the following products:
o Security zSecure Admin
o Security zSecure Audit
o Security zSecure Alert
o Security zSecure Command Verifier
- IBM InfoSphere® Guardium® Database Security: Provides the simplest, most robust solution for real-time database security, ensuring the privacy and integrity of trusted information in your data center.

The world is becoming more digitized and interconnected, which open the door to emerging threats, leaks and attacks. The average cost of a security breach is $5.8 million US dollars (USD)! Analytics, mobile, social, and cloud computing all have one thing in common: They need a platform that has a deeply integrated security stack.

There is a physical layer of protection that is included with the z13 crypto cards. *For example*, if someone attempts to pull the cards out of the machine to access the keys, the cards automatically zeroize. They also zeroize if the temperature changes drastically, such as the case where someone attempted to freeze the cards and extract the crypto keys with a $7 USD can of compressed air! These products have physical protection built-in.

The Payment Card Industry Data Security Standard (PCI DSS) is a widely accepted set of policies and procedures that is intended to optimize the security of credit, debit, and cash card transactions, and protect cardholders against misuse of their personal information. It applies to all entities, Including merchants and service providers that store, process, or transmit cardholder data, such as Personal Account Number (PAN) data.

When the PCIe adapter is configured as an accelerator, it is optimized for Secure Sockets Layer (SSL) acceleration and clear key RSA operations, which allows savings of processing time by offloading processor-intensive cryptographic algorithms.



zSecure Audit
Vulnerability analysis for the mainframe infrastructure; automatically analyze and report on security events and monitor compliance

zSecure Adapters for QRadar
Collects, formats and sends enriched mainframe System Management Facility (SMF) audit records to IBM Security QRadar SIEM

zSecure Alert
Real-time mainframe threat monitoring of intruders and alerting to identify misconfigurations that could hamper compliance

zSecure Command Verifier
Policy enforcement solution that helps enforce compliance to company and regulatory policies by preventing erroneous commands

zSecure Manager for RACF z/VM
Combined audit and administration for RACF in the VM environment including auditing Linux on System z

zSecure Admin
Enables more efficient and effective RACF administration, tracking and statistics using significantly fewer resources

zSecure Visual
Helps reduce the need for scarce, RACF-trained expertise through a Microsoft Windows-based GUI for RACF administration

zSecure CICS Toolkit
Provides access RACF command and APIs from a CICS environment, allowing additional administrative flexibility

Note:
• zSecure Audit also available for ACF2™ and Top Secret®
• zSecure Adapters for QRadar SIEM is a capability of zSecure Audit and is also available for ACF2™ and Top Secret®
• zSecure Alert also available for ACF2™

Solution architecture

• To enable security intelligence and powerful analytics, a combination of z13 hardware and software products should be employed.
- Common Cryptographic Architecture (CCA) enhancements have been announced that use the z13 enhancements and include CPACF and the Crypto Express5S.

CPACF

• The CP Assist For Cryptographic Functions (CPACF) delivers high-speed on-chip cryptography.
• CPACFwas redesigned to allow handling higher volumes of transactions.
CPACF has the following features:
- It is supported by z/OS, z/VM, IBM z/VSE®, z/TPF, and Linux on z Systems.
- It has protected key support for additional security of cryptographic keys (when using Common Cryptographic Architectu (CCA) mode; Crypto Express5S is required).
- It enhances the encryption/decryption performance of clear-key operations for SSL, VPN, and data storing applications.
- It provides a set of symmetric cryptographic functions and hashing functions for the following items:
o Data privacy and confidentiality
o Data integrity
o Random Number generation
o Message Authentication.
Many users of the CPACF benefit from it, such as the following ones:
- IBM InfoSphere Guardium Data Encryption for DB2® and IBM IMS™ databases
- IBM DB2 built-in encryption
- z/OS Communication Server: IPsec/IKE/AT-TLS
- z/OS System SSL
- z/OS Network Authentication Service (Kerberos)
- IBM Encryption Facility for z/OS DFSMSdss encryption feature
- IBM Encryption Facility for z/OS
- z/OS Java SDK
- Linux on z Systems: Kernel, openSSL, openCryptoki, and GSKIT.
Note: CPACF must be explicitly enabled by using a no-charge enablement feature (#3863). SHA algorithms are enabled with each server.

Crypto Express5S

• The Crypto Express5S is hardware-protected, secure-key cryptography providing the following features:
- High speed advanced cryptography, that is, intelligent encryption of sensitive data that runs off the processor, which saves on costs.
- PIN transactions, EMV transactions for integrated circuit-based credit cards (chip and pin), and general-purpos cryptographic applications that use symmetric key, hashing, and public key algorithms, and simplification of cryptographic key management to meet the needs of current banking, retail, and other applications.
- Designed for FIPS 140-2 Level 4 certification to meet regulations and compliance for PCI standards.
- Concurrent Segment 3 updates to meet the highest levels of availability.

New features

• Hardware-based logic upgrades for Elliptic Curve Cryptography (ECC) for Elliptic Curve Digital Signature Algorith (ECDSA) and Elliptic curve Diffie-Hellman (ECDH) key agreement protocols
• A new prime number generator
• Firmware support for VFPE.

Crypto Express5S PCIe adapter: A coprocessor or an accelerator

• The PCIe adapter contains a tamper-resistant hardware security module and can be configured in one of three ways by using the Hardware Management Console (HMC) panels:
1. IBM Common Cryptographic Architecture (CCA) coprocessor
2. IBM Enterprise PKCS #11 (EP11) coprocessor
3. Accelerator
• When the PCIe adapter is configured as a CCA coprocessor, it supports the following features:
- Secure key transactions to protect your most sensitive information.
- It meets the requirements of national security applications with Federal Information Processing Standard (FIPS) 140-2 Security Level 4 certification.
- User-defined extension (UDX) services to implement custom cryptographic functions and algorithms.
• When the PCIe adapter is configured as an IBM Enterprise PKCS #11 (EP11) coprocessor, it supports the following features:
- Provides open, industry-standard cryptographic services that follow the PKCS #11 specification v2.20.
- Simplifies porting PKCS#11 applications to z Systems.
• The z13 extends enhanced key public support for constrained digital environments that use Elliptic Curve Cryptography (ECC) by providing hardware-based ECC support through the CryptoExpress5S to ensure improve performance.
Here are some examples of the use of ECC:
- The US government uses ECC to protect internal communications
- It is the mechanism that is used to prove ownership of bitcoins
- It provides signatures in Apple's iMessage service
- It is used to encrypt DNS information with DNSCurve
- It is the preferred method for authentication for secure web browsing over SSL/TLS.
Note: Chrome and Firefox use it to establish secure connections

• IBM provides the Trusted Key Entry Workstation (TKE) as a means for ensuring secure creation and management of key material and for managing the crypto adapters on the host.
- Recent versions of the TKE have enhanced the management of those crypto adapters, including the ability to capture information from the current adapters, and then push that configuration to new adapters.

• Here are some of the features of TKE:
- FIPS Certified Smart Card: A FIPS certified smart card, part number 00JA710, is now included in the smart card reader and additional smart cards are optional features.
- Crypto coprocessors with more than 16 domains: In support of the z13 code's ability to allow more than 16 domains on the Crypto Express5S, TKE 8.0 allows the management of domains beyond the current limit of 16. This support is available only with the z13.
- Full-function migration wizard for EP11: The full-function migration wizard is designed to collect and apply quickly and accurately data to the Crypto Express features that are configured as EP11 coprocessors.
Note: This wizard previously supported CCA, but Crypto Module Groups are no longer supported on TKE 8.0, so the support has been removed.
- New master key management functions: TKE 8.0 allows support of three new master key management functions that are available when managing any type of master key:
o The Generate a set of master key parts wizard-like feature allows you to create a key part for each of the different types of master keys.
o The Load all new master keys wizard-like feature allows you to load a new key for each of the different types of master keys.
o For the Smart Card Readers Available indicator, TKE 8.0 displays a window title with availability information about the smart card readers.
- Configure Displayed Hash Size: TKE 8.0 supports a configuration to allow the administrator to set the display length of certain hash values that are displayed on the TKE workstation.
Note: Hash types that can be affected by this function are MDC-4, SHA-1, AES-VP, and ENC-ZERO. The Configure Display Hash Size utility is available only when you have signed on with the Privileged Mode Access user ID of ADMIN.
- ECC Authority Signature Keys: TKE 8.0 allows a user to select a key strength of 320-bit ECC key when creating an Authority Signature Key that is assigned to an Authority Index on a Crypto Express5S coprocessor.
Note: This option is available only when you are creating an Authority Signature key from inside a Crypto Module notebook of a Crypto Express5S.
- Print Capability:
o TKE 8.0 has limited print support. The Configure Printers utility allows the administrator to add printers to the TKE.
Note: The only printers that are allowed to be added are printers that have device drivers on the TKE, including the GUTENPRINT and HPLIP device driver packages. You cannot load your own device drivers.
- New features in the Crypto Node Management (CNM) Utility: The TKE Workstation Setup utility allows you to load and save user roles and profiles.
Note: The CNM utility now has stand-alone launch points for these two tasks in the Access Control drop-down menu.
- ENC-Zero Verification Pattern for 24-byte DES Operational Keys: TKE 8.0 supports an ENC-Zero verification pattern that is computed and displayed with 24-byte DES operational keys.
- Usability enhancements:
o TKE 8.0 has many usability enhancements, including the ability for users to select a check box that allows them to change their passphrase on the logon screen for a passphrase profile.
o Additionally, users can now select multiple items in the Hosts container, Crypto Module Groups container, or Domain Groups container of the main window of the TKE application.
Note: If more than one item is selected, you can delete all of the definitions or close all of the hosts or groups at once.

Usage scenarios

• Security intelligence solutions that use big data analytics can help organizations deal with a complex threat landscape.
- Industry experts recommend innovative thinking and a new approach to security.
- IBM continues to leverage and enhance the leading security capabilities that are provided by the z/OS and z/VM operating systems to build the tightest IT Security Hub, and further enhance enterprise security in the authentication, authorization, encryption, and auditing areas through the new z13 technology.
- The z13 and its latest enhancements to security, which are built into its hardware, and real-time big data analytics provide context to help detect threats faster, identify vulnerabilities, prioritize risk, and automate compliance activities.
Note: For security threat management, the key challenge is to reduce millions of logs to actionable intelligence that identify key threats. Traditional first-generation security information and event management (SIEM) products achieved this goal by leveraging correlation, for example, five failed logins followed by a successful login, to identify suspected security incidents. Event correlation is an important tool, but it is not enough.

There are two problems:

• Consider a 100,000:1 reduction ratio of events to correlated incidents. On the surface, this sounds impressive, but for companies generating 2 billion events per day (and you do not need to be a massive company to do that), that means that the company's security team has 20,000 incidents per day to investigate. Traditional SIEM correlation cannot reduce the data enough, and log managers cannot get even a 10,000:1 reduction ratio.
• Exclusive reliance on event correlation assumes that the criminals that are intent on attacking your company do not figure out ways to disable or bypass logging infrastructure, but that is practically their entire focus, and you cannot correlate logs that are not there!
Note: This limitation results in missed threats or a poor understanding of the impact of a breach.

HMC and SE security audit improvements

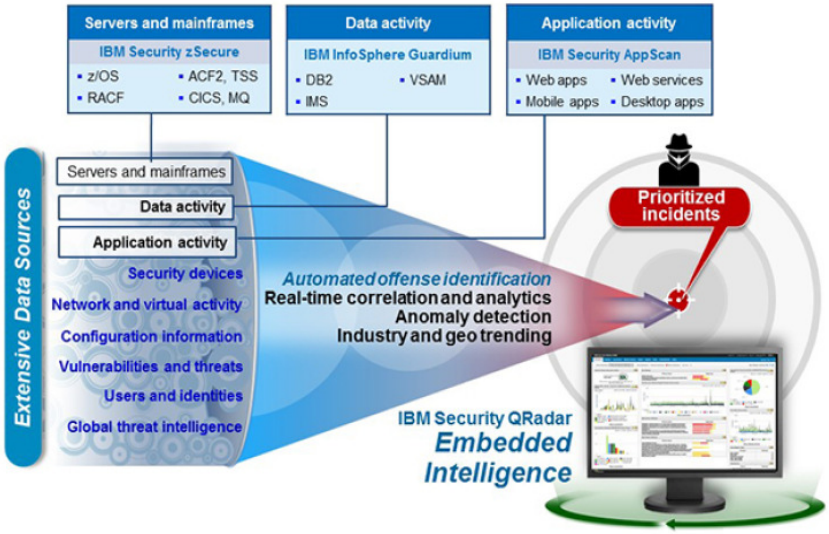
With the Audit and Log Management task, audit reports can be generated, viewed, saved, and off-loaded. The Customize Scheduled Operations task allows you to schedule audit report generation, saving, and offloading. The Monitor System Events task allows Security Logs to send email notifi-cations by using the same type of filters and rules that is used for both hardware and operating system messages.

With the z13, you can offload the following HMC and SE log files for **customer audit:**
- Console event log
- Console service history
- Tasks performed log
- Security logs
- System log

Critical issues with firmware upgrades are security and data integrity. Procedures are in place to use a proc-ess to sign digitally the firmware update files that are sent to the HMC, the SE, and the TKE. Using a hash algorithm, a message digest is gen-erated that is then encrypted with a private key to produce a digital signature.

Data that is stored on Flash Express is encrypted by a strong encryption symmetric key that is in a file on the SE hard disk. This key is also known as the *Flash encryption key/authentication key*. The firmware management of the Flash Express adapter can generate an asymmetric trans-port key in which the flash encryption key/authentication key is wrapped. This transport key is used while in transit from the Support Element to the Firmware management of the Flash Express adapter.

• IBM Security QRadar® vastly expands the capabilities of traditional SIEMs by incorporating new analytics techniques and broader intelligence.
- Unlike any other SIEM in the market today, QRadar captures all activity in the network for assets, users, and attackers before, during, and after an exploit and analyzes all suspected incidents in this context. New analytical techniques such as behavioral analysis are applied.
- QRadar notifies analysts about "offenses", which are correlated sets of incidents with all of the essential, associated network, asset, vulnerability, and identity context. By adding business and historical context to suspected incidents and applying new analytic techniques, massive data reduction is realized and threats that otherwise are missed are detected.
• The z13 combined with IBM software products' real-time correlation and anomaly detection across a distributed and scalable repository of security information enables more accurate security monitoring and better visibility for any organization, small or large. As an example of the software products that can be monitored, see figure below.



Remote Support Facility

The HMC Remote Support Facility (RSF) provides important communication to a centralized IBM support network for hardware problem reporting and service.
The following types of communication are provided:
• Problem reporting and repair data
• Microcode Change Level (MCL) delivery
• Hardware inventory data, which is also known as *vital product data* (VPD)
• On-demand enablement

Consideration: RSF through a modem *is not supported* on the z13 HMC. Broadband connectivity is needed for hardware problem reporting and service. Modems on installed HMC FC 0091 hardware do not work with HMC Version 2.13.0, which is required to support the z13.

Security characteristics

The following security characteristics are in effect:
• RSF requests always are initiated from the HMC to IBM. An inbound connection is never initiated from the IBM Service Support System.
• All data that is transferred between the HMC and the IBM Service Support System is encrypted with high-grade Secure Sockets Layer (SSL)/Transport Layer Security (TLS) encryption.
• When starting the SSL/TLS-encrypted connection, the HMC validates the trusted host with the digital signature that is issued for the IBM Service Support System.
• Data that is sent to the IBM Service Support System consists of hardware problems and configuration data.

RSF connections

• If the HMC and SE are at Driver 22, the driver uses a new remote infrastructure at IBM when the HMC connects through RSF for certain tasks.
- Check your network infrastructure settings to ensure that this new infrastructure will work.
Note: At the time of this writing, RSF still uses the "traditional" RETAIN connection. You must add access to the new Enhanced IBM Service Support System to your current RSF infrastructure (proxy, firewall, and so on).
• To have the best availability and redundancy and to be prepared for the future, the HMC must have access to the Internet to IBM through RSF in the following manner.
- Transmission to the enhanced IBM Support System requires a Domain Name Server (DNS).
- The DNS must be configured on the HMC if you are not using a proxy for RFS.
Note: If you are using a proxy for RSF, the proxy must provide the DNS.