• 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

• 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 security.

• The LPARs are allocated their own resources and are secure and separate environments.

• Integrated cryptographic features provide leading cryptographic performance and functions.

  - Reduced latency, delay, and serviceability (RAS) support for the Crypto Express5S is enhanced in the industry.

  - IBM is in the process of gaining FIPS 140-2 Level 4 certification for the CryptoExpressSS feature.

  - With FIPS 140-2 Level 4 certified cryptographic hardware, IBM provides the most secure tampering- 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 any environment, and incorporates all that is necessary for consideration.

  - The IBM Security Framework has the following features:

    - Enables innovation through secure-key, end-to-end infrastructure and platforms.

    - Ensures the speed 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.

• 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 of the card data even if the output is cleartext and requiring ciphertext.

  - Greater than 16 domain support: Greater than 16 domain support allows a cryptographic coprocessor to be shared among up to 16 domains, up to the maximum number of LPARs in an AP.

  - This support relies on enhanced firmware that is available with a minimum microcode level for the CryptoExpressSS coprocessor. With the adjacent processor (AP) extended addressing (APXA) facility in effect, systems crypto architecture support can greater than 16 domain support an AP.

  - Requires the flexibility of mapping individual LPARs to unique crypto domains or continuing to share crypto domains across LPARs.

• These enhancements are the following IBM z Systems features, which also are redesigned to provide even more security and performance:

  - CPACF - Crypto Express5S and Crypto ExpressSS CPACF is designed to improve performance for cryptographic functions.

  - Note: The optional Cryptographic Coprocessor adapter (CryptoExpressSS) provides new virtualization capabilities and performance increases.

  - SIMD allows construction of rich, complex analytics models that use SIMD to provide additional speed.

  - API enhancements applied to existing IBM Power and x86 environments.

  - SMI: 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: The solution 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 2 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 service for PCI/VISA (and other applications) data at rest and data in transit. The content must be secure and transported, that is, physically moved, for example, shipped in a truck, or electronically sent over non-secure links.

• IBM Security S2Secure™ Suite: A comprehensive suite of products that enhance the management, auditing, reporting, and compliance of security in RAFC, CA-AF2C, and CA-Top Secret environments.

• This suite includes the following products:

  - SecurezSecure Admin

  - Security zSecure Audit

  - Security zSecure Alert

  - 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. To defend against these threats, IBM has invested in the z13 security breach ($5.8 million US dollars USD)!

  - Analytics, machine learning, and cloud computing are all one thing in common: They need a platform that has a deeply integrated security stack.

  - There is a physical layer that 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 PCI Express adapter is configured as an accelerator, it is optimized for Secure Sockets Layer (SSL) acceleration and key key RSA operations, which allows savings of processing time by offloading processor-intensive cryptographic algorithms.

The US government uses ECC to protect internal communications.

It is the mechanism that is used to prove ownership of bitcodes.

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 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:
  - The Generate a set of master key part wizard-like feature allows you to create a key pair for each of the different types of master keys.
  - 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.
- 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.
- 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:
  - TKE 8.0 has limited print support. The Configure Printers utility allows the administrator to add printers to the TKE.
  - The GUTENPRINT and HLP/PRINTER device driver packages. You cannot load your own device drivers.
- New features in the Crypto Node Management (CMM): The TKE Workstation Setup utility allows you to load and save user roles and profiles.
- The CMM utility now has a stand-alone launch points for these two tasks in the Access Control drop-down menus.
- 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: 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.
- 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.

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, find 5000 logs followed by a successful login, to identify suspicious security incidents. Event correlation is an important tool, but it is not enough.

There are two problems:
- Considering the 10,000:1 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 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 count on that they 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
- Support for the audit and Log Management task, audit reports can be generated, viewed, saved, and offloaded. The Customized Scheduled Operations task allows you to schedule audit report generation, saving, and offloading.

The Monitor System Events task allows Security Logs to send email notifications 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 process 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 generated 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 stored 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 transport key in transport key in which the flash encryption key authentication key is wrapped. This transport key is used while in transit from the SE 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 connects 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. The modem on installed HMC FC 0091 hardware do not work with HMC Version 2.15.0, which is required to support the z13.

Security characteristics
The following security characteristics are in effect:
- Security: The retention of all security data on the HMC is required for 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 connection:
- If the HMC and SE are at Driver 2, the driver uses a new remote interface 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 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 RSF.

Note: If you are using a proxy for RSF, the proxy must provide the DNS.