They will be designed to determine whether recommended public key infrastructure services, serves as your secured data vault, helps meet regulatory requirements, and reduces operational risk:

- **SMF record signing**
- **New RACF read-only auditor capability**
- **New Crypto Express5S Version 2** for on-chip cryptographic coprocessors; also, improved virtualization of the cryptographic adapter attribute, when assigned to a user ID, allows a number of RACF commands to be used with options that change the events for which SMF records are written for auditing purposes.
- **RACF** will be designed to support a new attribute, **ROAUDIT**.
- **System SSL’s new OCSP support** is designed to help reduce risk and improve the security of mobile and other transactions by checking certificate revocation status over a network.
- **Additional advances in cryptography** are planned to support these functions for application-transparent transport and later processors.
- **Remote Key Export callable service** is planned to be used by the system to determine whether a specific user is authorized to change the MAIN system in a multiple node system.
- **Additional information** is provided in **z/OS V1.13 and z/OS V2.1** with the PTF for APAR AA43999.
- **z/OS V2.2 SAF and RACF** are planned to be supported for new users of z/OS UNIX System Services.
- **Two console security enhancements** are planned to be used by the system to determine whether a specific user is authorized to issue MODIFY CATALOG commands that alter the behavior of the system or to issue any MODIFY CATALOG command to alter the information about catalog processing. This is intended to provide more granular security and better operational flexibility.

**z/OS V2.2 PKI Services** is planned to provide support for:
- **New PKCS #12 key store (KDS) as "archived," rendering them ineligible for use; to retrieve labels from a KDS that satisfy certain search criteria; ... and finally to provide methods to manage meta-data and start and end dates associated with a KDS record, including**
  - **Reference key data**
  - **Account information**, and an IBM-PIN Offset.
- **Multiple enhancements** may be used to improve the cryptographic security with designs intended to provide:
  - **Support for emerging standards for American Express, JCB, MasterCard, and Visa payment systems (EMVCo)** in CCA-based callable services.
  - **Support for AES MAC enhancements to the Symmetric MAC Generate and Symmetric MAC Verify callable services, allowing** for key lengths greater than 128 bits for XCB-CMAC processing.
  - **Support for a number of frequently used User Defined Extensions (UDX) callable services to CCA firmware, expected to help you reduce costs associated with UDX maintenance. This support, which requires minimum MCLs for Crypto Express3 and Crypto Express4 coprocessors on z196 and later processors.**
  - **Using the new PIN Format Preserving Encryption (VFPE) algorithms in CCA-based callable services. This support will**

**z/OS V2.2 RMTM support in z/OS V2.2** is planned to help you analyze the performance of CryptoExpress3 coprocessors on specificmode, including TIPA and PKCS #11 modes. This is intended to improve the interoperability of PKCS #11 mode and provide better cryptographic security with designs intended to provide support for:
- **VISA Format Preserving Encryption (FPE) algorithms in CCA-based callable services. This support will rely on the CryptoExpress3 coprocessors on x3 processors.**
- **Enhanced Random Number generation exploiting CPACF Deterministic Random Number Generator (RNG) instruction, intended to improve the interoperability of PKCS #11 mode and provide better cryptographic security with designs intended to provide support for:**
- **Enhanced KDS support that allows you to disable the RMI Cache.**
- **z/OS V2.2 RMTM support in z/OS V2.1.13 with the PTF for APAR AA43993.**
- **ICSF FPE and ECC/RSA digital signature activity information is planned to be included in SMF 70-2 records and in the RMI Postprocessor Crypto Activity report.**

**Deliver a trusted and resilient system of record**

With its legendary security and support for the most highly regulated industries, z/OS V2.2 helps you build public key infrastructure services, as served your secured data vault, helps meet regulatory requirements, and reduces operational risk:
- **SMF record signing intended to make your SMF-based auditing data a highly trusted repository**
- **New audit controls for better separation of duties between security auditors and security administrators**
- **Increased protection against attacks with variety of strengthened security capabilities in RACF and other system components**
- **Faster data encryption to handle increased transaction volume with the new Crypto ExpressSS cryptographic adapter and improved performance for on-chip cryptographic coprocessors; also, improved virtualization of the cryptographic adapter across all 85 SSL/TLS world-wide economies.**
- **z/OS V2.2 System SSL is planned to provide:**
  - **Support for the open certificate status protocol (OCSP) to retrieve certificate revocation status and certificate revocation lists (CRLs) over HTTP.**
  - **The OCSP support is planned to retrieve revocation status information for x.509 certificates as described by RFC 2560, and HTTP URL support is intended to allow you to specify that System SSL should retrieve CRL information using HTTP as described by RFC 3290 and 5280. These functions are intended to supplement the existing LDAP CRL processing and help improve the auditability and security of your business processes.**
- **z/OS V2.2 Communications Server is planned to support these functions for application-transparent transport layer security (AT-TLS), to enable their use for applications and middleware.**
- **Support for PKCS #12 certificate files.** This support is designed to allow applications to specify a PKCS #12 file to be used. PKCS #12 certificate key store files can contain multiple certificate authority (CA) and end entity certificates, and more than one certificate chain. This is intended to provide better interoperation for applications that create PKCS #12 key store files, such as Java-based applications.
- **This support is available for z/OS V1.13 and z/OS V2.1 with the PTF for APAR AA45216.**
- **Support to take advantage of the secure key support available with CryptoExpress4 (CEX4) and features available for zEnterprise ED12 (zEC12) when configured in EP11 mode, by using the support of secure DSA keys for signing data and for fixed Elliptic Curve Diffie-Hellman (ECDH) key exchanges.**
- **Support allowing SSL sessions to be reused across different TCP ports.**
- **Support for AES MAC enhancements to the Symmetric MAC Generate and Symmetric MAC Verify callable services, allowing** for better compatibility and performance with certain FTP servers and clients. This enhancement, available for System SSL users and for both AT-TLS and native SSL users of FTP, is intended to provide both improved security and performance. The z/OS V2.2 network authentication service (NAS) is planned to support the use of X.597 certificates for Kerberos-based authentication.**
- **This support is also available for z/OS V1.13 and z/OS V2.1 with the PTF for APAR AA45216.**
- **NOTE:** This support is intended to help improve usability. A new optional OPERCMDS profile is planned to be used by the system to determine whether a specific user is authorized to issue MODIFY CATALOG commands that alter the behavior of the system or to issue any MODIFY CATALOG command to alter the information about catalog processing. This is intended to help improve usability.
- **Enhanced support in the Remote Key Export callable service to allow you to specify the desired key-wrapping method to be used for key generation and transport.**

**NOTE:** This support requires minimum MCLs for Crypto Express3 and Crypto Express4 coprocessors.

**More ICCS functions** planned for z/OS V2.1.13 include:
- **Support for SMF Type 106 records for HWINSET and HWICMD events. This enhancement is intended to allow you to audit operations such as updates to attribute values for CPC processor weights, image profiles, and activation profiles; and, for operations affecting a CPC or image such as image activations.**
- **Support for emerging standards for American Express, JCB, MasterCard, and Visa payment systems (EMVCo) in CCA-based callable services for key management, generation, transport, and derivation.**
- **Enhanced support for PKCS #11 to provide support for X.509 certificates for Kerberos-based authentication.**
- **Support for AES MAC enhancements to the Symmetric MAC Generate and Symmetric MAC Verify callable services, allowing** for key lengths greater than 128 bits for XCB-CMAC processing.
- **Support for a number of frequently used User Defined Extensions (UDX) callable services to CCA firmware, expected to help you reduce costs associated with UDX maintenance. This support, which requires minimum MCLs for Crypto Express3 and Crypto Express4 coprocessors on z196 and later processors.**
- **Using the new PIN Format Preserving Encryption (VFPE) algorithms in CCA-based callable services. This support will**
- **Account information, and an IBM-PIN Offset.**
- **Symmetric Key Export with Data, which can be used to generate an authentication parameter (AP) and then retrieve encrypted using a supplied key.**
- **Authorization Token Generator, which can be used to export a symmetric key, along with application-supplied data.**
- **More ICCS enhancements planned for z/OS V2.2 include:**
- **Support for PKCS #11 applications intended to allow them to change a key’s compliance mode using the Set Attribute Value function.**
- **Support for ECG keys generated using Brainpool curves while executing in FIPS mode encrypted using an RSA key.**

**Ref: Software Announcement 215-006**