z/OS Version 2 Release 2 Security Brief

z/OS V2.2 will be designed to provide digital signatures for **SMF** records written to log streams. This function is intended to help you detect unauthorized alterations to recorded SMF data. This new function is planned to sign blocks of SMF records and chain the blocks' signatures. A planned signature verification function will be designed to help you determine whether SMF records or blocks of SMF records have been altered or removed. This is intended to provide a more trusted repository for the auditing records created by a number of z/OS system components, including RACF.

These RACF enhancements are planned for z/OS V2.2:

- The **RACF AUDITOR** attribute, when assigned to a user ID, allows a number of RACF commands to be used with options that change the events for which SMFrecords are written for auditing purposes.
  - RACF will be designed to support a new attribute, ROAUDIT.
    > This attribute, like the AUDITOR attribute, is intended to allow an auditor to list the contents of RACF profiles but not to change any RACF auditing options.
    NOTE: This is intended to help you provide a better separation of duties between RACF administrators and RACF auditors.
- RACF will be designed to provide better protection for **offline attacks** against encrypted passwords by allowing you to use stronger encryption.
  - Support is planned to allow you to accept additional special characters within passwords, define users allowed to use only password phrases, clean up a user's password history, and set an "expired" status for a user's password without changing it to a new value.
    NOTE: This support is also available in z/OS V1.13 and z/OS V2.1 with the PTF for APAR OA43999. Additionally, z/OS V2.2 RACF is planned to not set default passwords when new users are defined, to remove the need for an exit (ICHDEX01) to use password encryption, and to allow the use of a password phrase with the RACLINK DEFINE command.
- The **RACF remote sharing facility** (RRSF) will be designed to allow you to change the MAIN system in a multisystem node dynamically.
  - This new function is expected to make the overall process of changing MAIN systems much simpler.
- Also, RRSF will be designed to allow you to specify that **inbound updates** from specific systems be ignored.
  - This function is intended to allow you to have RRSF propagate updates from production systems to test systems without allowing privileged users on test systems to obtain more privileges on production systems.
- Support is planned in the **R_admin callable service** and in the **IRRXUTIL REXX language interface** for a new function designed to return RRSF configuration and operational information.
- Certificates can be used for a number of different services. z/OS V2.2 will be designed to allow you to use more granular certificate administration, supporting narrowed spans of administrative control using new profiles in the RDATALIB class.

z/OS V2.2 **SAF and RACF** are planned to provide two new functions for users of **z/OS UNIX System Services**. The first will be designed to allow a user with access to a new profile in the **UNIXPRIV class** to perform additional file system-related operations, such as listing files in a directory, without being authorized to alter files. The second will be designed to allow security administrators to protect file system directories with a **new NOEXEC attribute** intended to prevent programs from being run from files stored in those directories. These changes are both intended to help you improve z/OS UNIX security.

A number of new security health checks are planned. They will be designed to determine whether recommended controls over ICSF, z/OS UNIX System Services, and RACF remote sharing facility (RRSF) resources exist, and to determine whether recommended password controls and encryption techniques are in use. These checks will be intended to help you improve system security.

Two console security enhancements. First, the system will be designed to allow you to specify timeout values for MCS, SMCS,and HMCS consoles and to automatically log off users from those consoles when the timeout intervals are exceeded without any operator input. This can help you improve console security. Second, a new optional SAF profile will control whether the same user ID is allowed to log on to multiple consoles concurrently. This 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 only MODIFY CATALOG commands that display information about catalog processing. This is intended to provide more granular security and better operational flexibility.

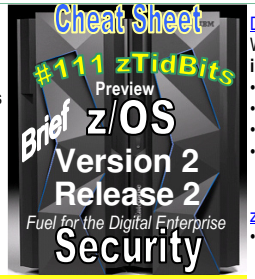
z/OS V2.2 PKI Services is planned to provide support for:

- Requiring **multiple administrators** to approve the creation of new certificates.
  - This optional multiple approver process is intended to help you prevent the creation of unauthorized certificates.
- **Online certificate status protocol** (OCSP) responses to be signed with the client specified signing algorithm as documented by RFC 6277. This is intended to improve the interoperability of PKI Services and OCSP clients.
- Using the **SHA-224 and SHA-256** with DSA encryption algorithms for signing certificates, CRLs, OCSP responses,and verify certificate requests.
- Callers running in 64-bit addressing mode.

These new ICSF functions are intended to help banking and finance sector clients meet industry standards and provide better cryptographic security with designs intended to provide support for:

- **VISA Format Preserving Encryption** (VFPE) algorithms in CCA-based callable services. This support will rely on the Crypto Express5S coprocessors on z13 processors.
- **Enhanced Random Number generation** exploiting CPACF Deterministic Random Number Generate (DRNG) instruction, intended to be compliant with NIST standard SP 800-131A.
- Allowing you to disable the **RNG Cache**.
- z/OS V2.2 **RMFTM support** is planned to help you to analyze the performance of **Crypto Express5S** co-processors operating in CCA and PKCS #11 modes.
  - This support is also planned to be available at z13 general availability on z/OS V2.1 and z/OS V1.13 with the PTF for APAR OA43493.
  - ICSF FPE and ECC/RSA digital signature activity information is planned to be included in SMF 70-2 records and in the RMF Postprocessor Crypto Activity report.

Ref: Software Announcement 215-006



Capturing the mobile enterprise: 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 available on zEC12, zBC12, and z13 processors for z/OS V2.1 and z/OS V1.13 are available in the Cryptographic Support for z/OS V1R13 - z/OS V2R1 web deliverable;you can download at http://ibm.com/systems/z/os/zos/downloads

Further support planned for V2.2 ICSF has been introduced in PTFs:

- z/OS V2.1 ICSF, z/OS V1.13 ICSF, and the Cryptographic Support for z/OS V1R10 - z/OS V1R12 web deliverable with the PTFs for APAR OA45548 ICSF are designed to support exploitation of counter (CTR) mode for the AES-based encryption on z196 and later processors.
- z/OS V2.1 ICSF and the Cryptographic Support for z/OS V1R11 - z/OS V1R13 web deliverable and later, with the PTFs for APAR OA43816 ICSF are designed to support enhanced PKA key translation without the need to use a User Defined Extension (UDX). This support requires minimum MCLs for Crypto Express3 and Crypto Express4S coprocessors on z196 and later processors.
- z/OS V2.1 ICSF and the Cryptographic Support for z/OS V1R12 - z/OS V1R13 web deliverable and later with the PTFs for APAR OA44444 are designed to provide Common Cryptographic Architecture (CCA) support for new German Banking Industry-defined PIN processing functions. This support requires minimum MCLs for Crypto Express3 and Crypto Express4S coprocessors on z196 and later processors.

z/OS V2.2 ICSF and the Enhanced Cryptographic Support for **z/OS V1R13- z/OS V2R1 web deliverable** are planned to include enhancements designed to allow for you to query reference date information for key tokens and key objects in a **key data store (KDS);** to mark records in a KDS as "archived," rendering them ineligible for use; to retrieve labels from a KDS that satisfy certain search criteria; to mark records in a KDS with start and end dates; and finally to provide methods to manage metadata and start and end dates associated with a KDS record, including the abilities to archive and recall keys.

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**, serves as 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
- A **new RACF read-only auditor capability** for stronger separation of duties between security auditors and security administrat
- Increased protection against attacks with variety of **strengthened security capabilities** in RACF and other system component
- **Faster data encryption** to handle increased transaction volume with the **new Crypto Express5S** cryptographic adapter and improved *performance* for on-chip cryptographic coprocessors; also, improved virtualization of the cryptographic adapter across up to 85 domains for improved economics.

z/OS V2.2 System SSL is planned to provide:

- Support for the **online 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 CRL support is intended to allow you to specify that System SSL should retrieve CRL information using HTTP as described by RFC 3280 and 5280. These functions are intended to supplement the existing LDAP CRL processing and help you ensure that valid certificates are used to complete SSL and TLS secure connections.
    NOTE: **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 for secure connections within an SSL environment. 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 also **available for z/OS V1.13 and z/OS V2.1** with the PTF for APAR OA45216.
- Support to take advantage of the secure key support available with Crypto Express4S (CEX4) and features available for zEnterprise EC12 (zEC12) when configured in EP11 mode, by supporting the use 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.
  - Communications Server is planned to provide FTP support to allow new data connections to reuse associated SSL sessions 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.509 certificates for Kerberos-based authentication** as described by RFC 4556. This is intended to help make it unnecessary for end users to manage strong passwords for some applications.

z/OS V2.2 **BCPii** will be designed to write **new SMF Type 106 records** for HWISET 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.

These ICSF functions, planned for z/OS V2.2 ICSF, *are already available* in the Cryptographic Support for z/OS V1R13 – z/OS V2R1 web deliverable. They are intended to help banking and finance sector clients meet standards and provide better 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 for key management, generation, transport, and derivation.
  NOTE: This support requires minimum MCLs for Crypto Express3 and Crypto Express4S coprocessors.
- 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 Express4S coprocessors.
- 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 XCBC-MAC processing.
- Support for a number of frequently used **User Defined Extensions (UDX) callable services** to CCA firmware, expected to hel you reduce costs associated with UDX maintenance. This support, which requires minimum MCLs for Crypto Express3 and Crypto Express4S coprocessors (zEC12), is designed to provide these new services:
  – Recover **PIN From Offset**, which can be used to calculate the encrypted customer-entered PIN from a PIN generating key, account information, and an IBM-PIN0 Offset.
  – **Symmetric Key Export with Data**, which can be used to generate an authentication parameter (AP) and return it encrypted using a supplied key.
  – **Authentication Parameter Generate**, which can be used to export a symmetric key, along with application-supplied data,

These enhancements require min. levels of EP11 firmware and mc level for the Crypto Express4S (zEC12).

***More* ICSF enhancements** planned for z/OS V2.2 ICSF, and also available in the **Cryptographic Support** for **z/OS V1R13 – z/OS V2R1** web deliverable, are designed to provide new functions for public sector customers, including industry standard APIs for IBM z Systems, and are intended to provide better interoperability with other platforms and help improve application portability and simplify system setup:

- **Enhanced Enterprise PKCS #11 mode support** designed to add secure key support for the Diffie-Hellman, Elliptic Curve Diffie-Hellman, RSA-PSS algorithms, and Secure DSA Domain Parameter Generation.
- Support for **Enterprise PKCS #11 applications** intended to allow them to change a key's compliance mode using the Set Attribute Value function.
- Support for **ECC keys** generated using **Brainpool curves** while executing in **FIPS mode encrypted** using an **RSA key**.