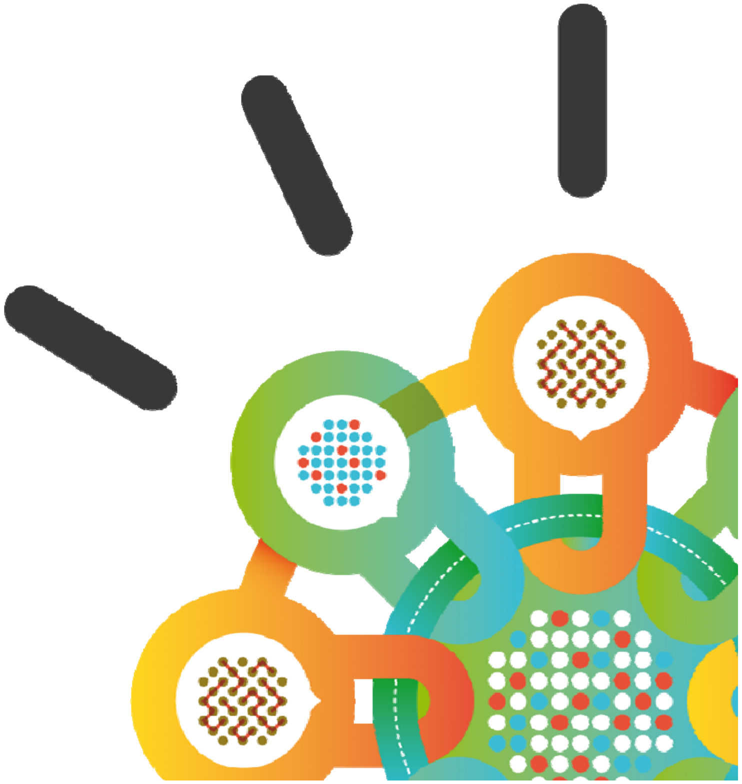
Security Intelligence.
Think Integrated.

z/OS 2.1 Security Updates

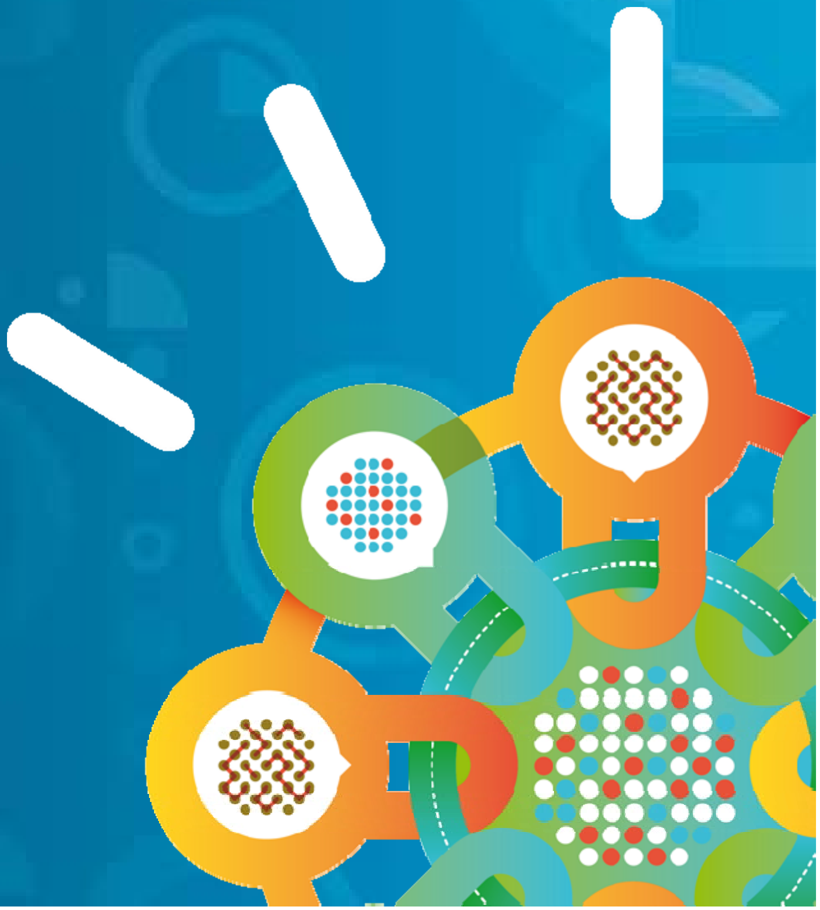
September 2013

Julie Bergh
jbergh@us.ibm.com



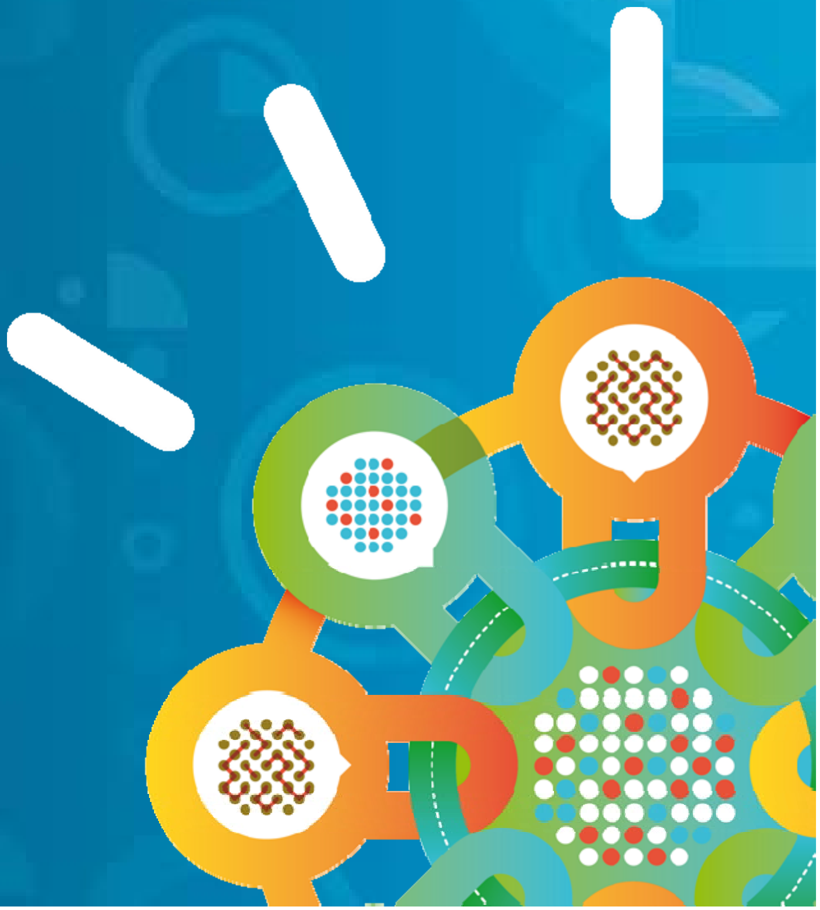
Agenda

- Overview of Security Changes
- z/OS Communication Server
- RACF
- ICSF PKI Services
- z/OS ITDS
- zSecure



Agenda

- Overview of Security Changes
- z/OS Communication Server
- RACF
- ICSF PKI Services
- z/OS ITDS
- zSecure



Overview of z/OS Security Changes

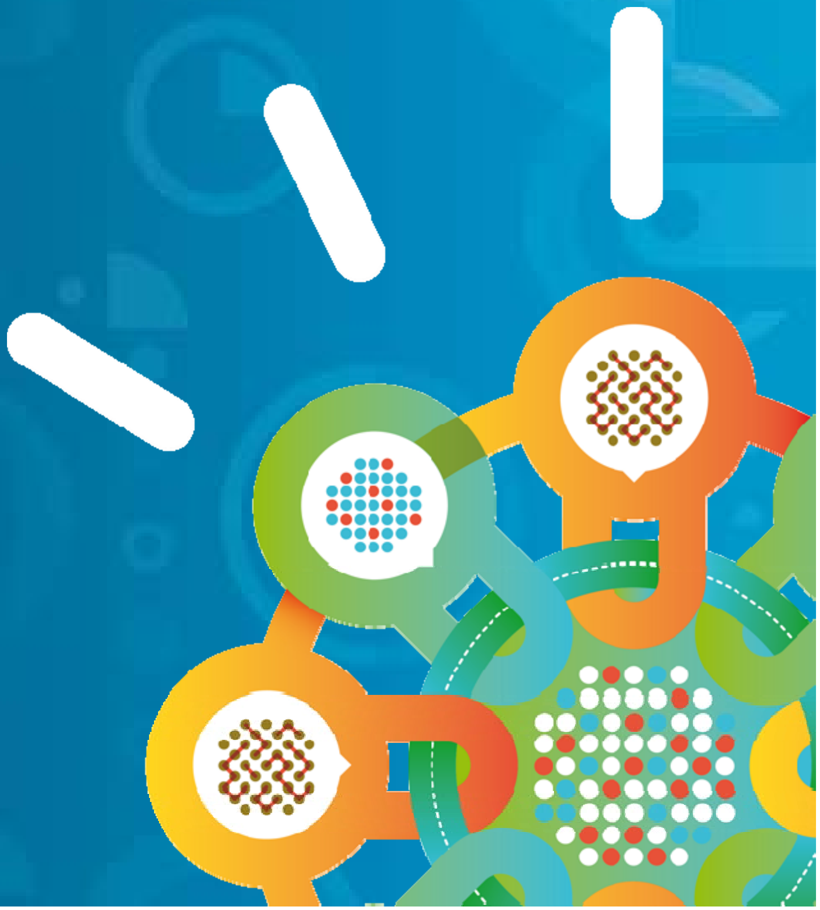
- In z/OS V2.1, IBM TDS (LDAP) is designed to allow applications, such as those running on Linux clients, to send data to z/OS to be processed by ICSF, leveraging the CryptoExpress4S cards available on zEnterprise servers. This support is designed to allow applications to request secure key cryptographic services from z/OS without exposing the keys in memory. Exploitation of these services is planned to be made available for Linux clients.
- New ICSF functions are designed to help banking and finance sector clients provide improved security, such as those functions that support emerging standards.
- New Communications Server capabilities to support security exits for z/OS FTP clients you can use to help secure file transfers.

Overview of z/OS Security Changes

- The RACF database unload utility is designed to unload additional information about digital certificates to help you more easily perform auditing activities on certificates stored in RACF databases.
- z/OS UNIX System Services enables you to specify whether a user should be logged off after a period of inactivity.
- JES2 and JES3 support for access controls on job classes, which you can use to remove the need for exits.
- New health checks on expiration of trusted certificates, and increased resources checked in sensitive resource class

Agenda

- Overview of Security Changes
- z/OS Communication Server
- RACF
- ICSF PKI Services
- z/OS ITDS
- zSecure



z/OS Communication Server

Enhanced IDS IP fragment attack detection - The Intrusion Detection Services (IDS) IP fragment attack type is enhanced to detect fragment overlays that change the data in the packet. In addition, the IP fragment attack detection is extended to IPv6 traffic.

Improve auditing of NetAccess rules - Control over the level of caching that is used for network access control checks is introduced. You can reduce the level of caching to pass more network access control checks to the System Authorization Facility (SAF). Passing more network access control checks to SAF allows the security server product to provide more meaningful auditing of access control checks.

An additional enhancement entails including the IP address that the user is attempting to access in the log string that is provided to the security server product on each network access control check.

AT-TLS support for TLS v1.2 and related features - Application Transparent TLS (AT-TLS) currency with z/OS System SSL is supported. Support is added for the following functions that are provided by System SSL:

– Renegotiation (RFC 5746) in z/OS V1R12
– Elliptic Curve Cryptography (RFC 4492 and RFC 5480) in z/OS V1R13
– TLSv1.2 (RFC 5246) in z/OS V2R1
– AES GCM Cipher Suites (RFC 5288) in z/OS V2R1
– Suite B Profile (RFC 5430) in z/OS V2R1
– ECC and AES GCM with SHA-256/384 (RFC 5289) in z/OS V2R1

z/OS Communication Server

Improved FIPS 140 diagnostics - Enhanced diagnostics for the IKE and NSS daemons and the AT-TLS function are provided when FIPS 140 processing is required.

Integrated Cryptographic Services Facility (ICSF) is required when FIPS 140 is configured for the IKE or NSS daemons or for an AT-TLS group. Starting in V2R1, these daemons and the AT-TLS groups will fail to initialize if ICSF is not active.

Limit defensive filter logging - The existing defensive filtering function provides a mechanism to install temporary filters to either deny attack packets or log when a packet would have been denied if blocking mode was used. You can now limit the number of defensive filter messages that are written to syslogd for a blocking or simulate mode filter. You can configure a default limit to be used for all defensive filters that are added to a TCP/IP stack. You can also specify a limit when adding an individual defensive filter with the z/OS UNIX ipsec command.

z/OS Communication Server

QDIO Outbound flood prevention - CSM storage constraints are relieved when processing ICMP Timestamp requests.

Because the z/OS TCP/IP stack replies to these requests, a flood of such requests can cause problems under the right conditions. Such a flood causes the TCP/IP stack to back up because it cannot get the responses out quickly enough, which results in a constrained CSM condition.

If the constrained CSM condition is not relieved, it might cause a stack outage.
This behavior might happen with:
– Other ICMP requests that always generate a response (for example, echo requests)
– UDP requests to an application that behaves in a similar manner

QDIO outbound packets will be dropped when CSM storage is constrained and the outbound queues are congested. This support alleviates these problems.

TN3270 client-bound data queueing limit - MAXTCPSENDQ, a new parameter in the Telnet profile, is introduced to prevent large amounts of storage from being held for data that is destined for an unresponsive Telnet client.

z/OS Communication Server

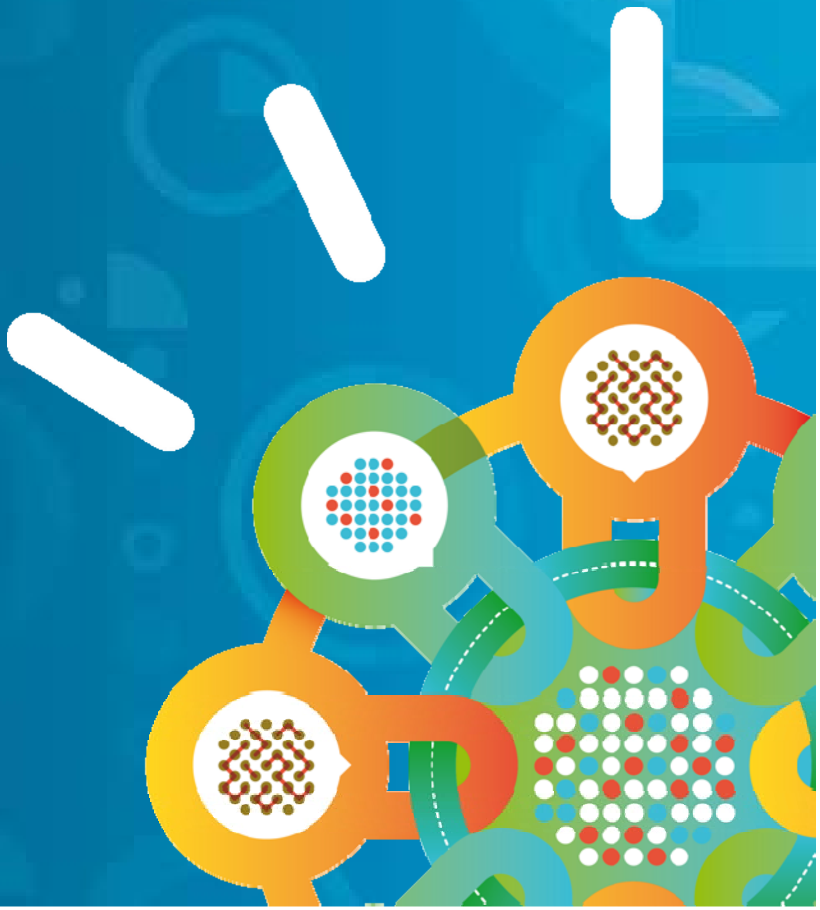
Reference information:

See the following topics in *z/OS Communications Server: New Function Summary* for detailed descriptions that include any applicable restrictions, dependencies, and steps on using the functions

- *Enhanced IDS IP fragment attack detection*
- *Improve auditing of NetAccess rules*
- *AT-TLS support for TLS v1.2 and related features*
- *Improved FIPS 140 diagnostics*
- *Limit defensive filter logging*
- *QDIO Outbound flood prevention*
- *TN3270 client-bound data queueing limit*

Agenda

- Overview of Security Changes
- z/OS Communication Server
- RACF
- ICSF PKI Services
- z/OS ITDS
- zSecure



RACF

Database unload of certificate DNs

The database unload utility (IRRDBU00) is enhanced to provide extended processing for fields such as the certificate field in profiles in the DIGTCERT class. This allows information, such as the subject's distinguished name, the issuer's distinguished name, and the signature algorithm to be unloaded.

Restricting access to a zFS file system

To restrict access to a zFS file system, you can define a general resource profile in the FSACCESS class. You can then use RACF commands to restrict z/OS UNIX access to the specified zFS file system for most users and allow selected users and groups to remain eligible to access the file system. This method supports an improved audit posture by enabling the RACF administrator to demonstrate a single point of control for restricting access to one or more file systems that might contain sensitive or personal data.

RACF

Remove BPX.DEFAULT.USER Profile

Default OMVS segment support is no longer provided regardless of whether the BPX.DEFAULT.USER profile is defined in the FACILITY class. z/OS UNIX users or groups must have OMVS segments that are defined for user and group profiles with unique UIDs and GIDs. Alternatively, you can use RACF support for automatically generating unique UIDs and GIDs on demand for users and groups that do not have OMVS segments that are defined.

RACF Remote sharing enhancements

In z/OS V2R1, RACF Remote Sharing (RRSF) is enhanced to use IPv6, if it is enabled on z/OS. It is used for establishing TCP/IP connections with remote RRSF systems and allows a z/OS system with an IPv6 address to be specified on the RACF TARGET command for the TCP(ADDRESS) operand. Also, when using AT-TLS to encrypt data that is sent between RRSF nodes using TCP/IP, stronger cryptography suites can be used in z/OS V2R1, including elliptic curve cryptography (ECC)-based certificates. Support is also added to allow blank lines and comments in RACF parameter library members.

RACF

Reporting certificates in the chain when added and listed

Report to the user the labels used for all the certificates in the chain when the chain is added. Add function to display information about the certificates in the chain.

Enterprise PKCS#11 secure key support

RACF can now use the ICSF Enterprise PKCS#11 secure key support by using the RACDCERT functions to create and manage secure key on the TKDS for the certificate and the retrieval of the certificate through the R_datalib callable service.

RACF support for DB2 V11

In DB2® V11, DB2 is enhancing cache management for RACF permissions when DB2 listens to RACF ENF events to determine when to purge the cache. In addition to DB2 listening to RACF ENF events 62 and 71, RACF ENF event 79 is added.

IRRDBU00: Additional Certificate Information

- **The RACF Database Unload Utility (IRRDBU00) unloads basic information about digital certificates into the 0560 (“General Resource Certificate Data Record”). This record contains:**
  - The record type (“0560”)
  - The name of the general resource profile which contains the certificate
  - The class (“DIGTCERT”)
  - The date and time from which the certificate is valid
  - The date and time from which the certificate is no longer valid
  - The type of key associated with the certificate
  - The key size
  - The last eight bytes of the last certificate signed with this key
  - A sequence number for certificates within a ring
- **What's missing? The issuer's distinguished name (IDN) and the subject's DN (SDN)of the certificate!**
  - This information is encoded within the certificate
  - Maps/mungs to the profile name, but given the profile name, you can't get the IDN or SDN

&RACUID in BPX.UNIQUE.USER

- **Clients who are using BPX.UNIQUE.USER to assign z/OS UNIX information to user IDs will be able to specify of &racuid in the home directory field of the model user's OMVS segment.**
  - `ALTUSER BPXMODEL OMVS(HOME(/u/&racuid))`

- **The appropriate user ID will be substituted for &racuid when a new OMVS segment is created for a user using BPX.UNIQUE.USER**
  - In upper case if “&RACUID” is specified
  - In lower case if any lower case characters are specified

- **Notes**
  - Only the first occurrence of &racuid is substituted
  - If the substitution would result in a path name exceeding the 1023 character maximum then substitution is not performed.
  - If sharing the RACF database with a downlevel system, substitution will not be performed on the downlevel system

JES2/JES3: SAF Check for Job Input Class

- **JES2 and JES3 are planning to perform a SAF check to verity a user's ability to use a job class**
  - Applied to both the “traditional” 36 single character classes as well as the planned up-to-eight character job classes
  - Does not apply to the “special” job classes STC and TSU
- **The resource name that is checked is:**
  - JESJOBS.*nodename.jobclass.jobname*
- **Controlled by these profiles:**
  - JES.JOBCLASS.OWNER in the FACILITY class
    - If this profile is defined, then authorization checks are performed for job owners
  - JES.JOBCLASS.SUBMITTED in the FACILITY class
    - If this profile is defined, then authorization checks are performed for job submitters

RACF

RACDCERT enhancement

This enhancement prevents the deletion of a certificate that was used for generating a request, but also grant clients an override mechanism to delete it when needed.

Health check for digital certificate expiration

Applications that rely on certificates might experience an interruption if a certificate that is used by the application or one of the users of the application is allowed to expire. RACF is introducing a new health check, RACF_CERTIFICATE_EXPIRATION, which identifies certificates that are stored in the RACF database that are expired or are about to expire.

RACF

- **The RACF_AIM_STAGE Health Check examines your application identity mapping (AIM) setting and flags as an exception if you are at a stage less than stage 3.**
  - Stage 0: No AIM support; only mapping profiles are used
  - Stage 1: Mapping profiles are used; alternate index created and managed, but not used
  - Stage 2: Alternate index create, managed, and used; mapping profiles maintained.
  - Stage 3: Only alternate index maintained and used. Mapping profiles deleted.
- **Moving from each stage requires the execution of the IRRIRA00 utility.**
- **AIM stage 2 or stage 3 is needed for certain RACF functions**

RACF

- **The RACF_UNIX_ID Health Check determines whether RACF will automatically assign unique z/OS UNIX System Services identities when users without OMVS segments use certain UNIX services**
  - If you are not relying on RACF to assign UIDs and GIDs, the check informs you that you must continue to assign z/OS UNIX identities
  - If you are relying on the BPX.DEFAULT.USER support, the check issues an exception
  - If you are relying on the BPX.UNIQUE.USER support, the check will verify requirements and indicate if any exceptions are found
    - FACILITY class profile BPX.UNIQUE.USER must exist
    - RACF database must be at Application Identity Mapping (AIM) stage 3
    - UNIXPRIV class profile SHARED.IDS must be defined
    - UNIXPRIV class must be active and RACLISTed
    - FACILITY class profile BPX.NEXT.USER must be defined and its APPLDATA field must contain valid ID values or ranges

RACF

- **The RACF_CERTIFICATE_EXPIRATION health check finds the certificates in the RACF database expired or about to expire**
  - Expiration window is an installation-defined value with a default of 60 days.
  - Valid expiration window values are 0-366 days
- **For each certificate, the check displays:**
  - The certificate “owner” ('SITE', 'CERTAUTH', or 'ID(*user_id*)')
  - The certificate label
  - The end date
  - The trust status
  - The number of rings to which the certificate is connected
- **The check only flags as exceptions those certificates which are TRUSTED.**

RACF

- **The RACF_SENSITIVE_RESOURCES check has been updated to check these new “static” resources names:**
  - BPX.DEBUG/FACILITY
  - BPX.WLMSERVER/FACILITY
  - IEAABD.DMPAKEY/FACILITY
  - MVS.SLIP/OPERCMDS
  - SUPERUSER.PROCESS.GETPSENT/UNIXPRIV
  - SUPERUSER.PROCESS.KILL/UNIXPRIV
  - SUPERUSER.PROCESS.PTRACE/UNIXPRIV

RACF

- **RACF is planning on updating the RACF_SENSITIVE_RESOURCES to check these new "dynamic" resources names:**
  - CSVAPF.*data_set_name*/FACILITY, excluding
    - CSVAPF.MVS.SETPROG.FORMAT.DYNAMIC
  - CSVDYLPA.ADD.*module_name/*FACILITY
  - CSVDYNEX.*exit_name*.*function.modname*/FACILITY, *excluding*
  - CSVDYNL.*lnklstname. Function*/FACILITY*excluding*
    - CSVDYNL.*lnklstname*.DEFINE CSVDYNL.*lnklstname.*UNDEFINE)

- **No validation is performed on the dynamic portion of these resource names (for example *data_set_ name, module_name,lnklstname*)**

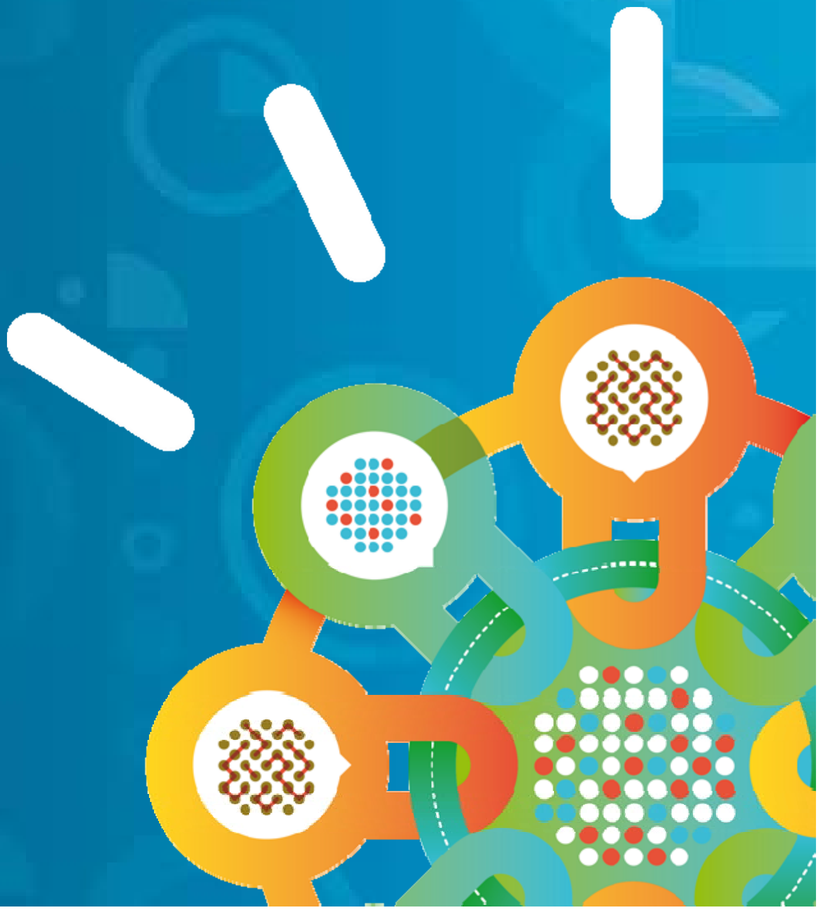
RACF

Reference information:

- *z/OS Security Server RACF Callable Services*
- *z/OS Security Server RACF Command Language Reference*
- *z/OS Security Server RACF Data Areas*
- *z/OS Security Server RACF Macros and Interfaces*
- *z/OS Security Server RACF Messages and Codes*
- *z/OS Security Server RACF Security Administrator's Guide*
- *z/OS Security Server RACF System Programmer's Guide*
- *z/OS UNIX System Services Planning*
- *z/OS Security Server RACROUTE Macro Reference*
- *z/OS Migration*
- *IBM Health Checker for z/OS: User's Guide*

Agenda

- Overview of Security Changes
- z/OS Communication Server
- RACF
- ICSF PKI Services
- z/OS ITDS
- zSecure



ICSF PKI Services

PKI Services: Enterprise PKCS#11 secure key support

PKI Services can now create secure keys in TKDS during certificate creation and return a PKCS#12 package containing the secure key to the requester.

PKI Services: RFC 5280 and 4523 currency

Enable PKI Services to optionally create the path length value in the Basic Constraints extension to restrict a CA from signing another subordinate CA. Also, PKI Services provides an option to specify the binary attribute when posting a certificate or CRL to LDAP to suit the need of different types of LDAP servers.

PKI Services: Extended Validation (EV) certificate

This enhancement supports the RDNs needed for Extended Validation (EV) certificates, from z/OS PKI Services, that requires validation on certificates.

ICSF PKI Services

PKI Services: Certificate administration support

Enable multiple PKI Services administrators granular control to perform different actions on different types of certificates on different domains and provide them the visibility of the signing algorithm when reviewing requests and certificates to ensure compliance with enterprise security policy.

System SSL: Transport Layer Security (TLS) protocol version 1.2

TLS V1.2 protocol support is provided according to RFC 5246, for establishing secure connections between two communicating partners. TLS V1.2 adds support for exploiters to use higher strength cryptographic ciphers. TLS V1.2 main objectives are to replace the standard SHA-1/MD5 pseudorandom function (PRF) with a cipher-based PRF based on SHA-256, add support for SHA-256 based ciphers and allow client applications to specify what signature/hash values are supported for digital signatures.

ICSF PKI Services

System SSL: Suite B Cryptography

System SSL is enhanced to provide Suite B Cryptography based on RFC 5430 - Suite B Profile for Transport Layer Security. RFC 5430 defines an implementation of the TLS V1.2 protocol that conforms to the Suite B guidelines. Suite B defines a set of security levels that require the key establishment and authentication algorithms that are used in a TLS session to be based on Elliptic Curve Cryptography (ECC) and the encryption algorithm to be AES based.

The security levels are:

- 128-bit security level corresponds to an elliptic curve size of 256 bits and AES-128
- 192-bit security level corresponds to an elliptic curve size of 384 bits and AES-256

ICSF PKI Services

System SSL: Enhanced DSA Support

System SSL's **gskkyman** certificate utility and Certificate Management (CMS) APIs are being enhanced to support 2048-bit DSA key pairs and DSA digital signatures using SHA-224 and SHA-256.

System SSL: RFC 5280 PKIX certificate and CRL profile currency

The certificate management API, **gsk_validate_certificate_mode()**, is enhanced to accept a new mode value to indicate RFC 5280. The SSL/TLS APIs for setting and getting environment and session attributes are also enhanced to support a new enumeration value to indicate certificate validation is to be performed according to RFC 5280.

ICSF PKI Services

System SSL: SAF key ring validation

In z/OS V1R13, and earlier releases of System SSL, SAF key ring validation was designed to stop full validation at the first CA trust anchor in the SAF key ring. This support gives the capability to the application to indicate that certificate validation using SAF key rings must be performed up to and including the root CA certificate.

The certificate management API, **gsk_validate_certificate_mode()**, is enhanced to accept a new optional parameter to indicate full validation. The SSL/TLS APIs for setting and getting environment attributes are also enhanced to support a new attribute type (GSK_CERT_VALIDATE_KEYRING_ROOT) and two new enumeration values (GSK_CERT_VALIDATE_KEYRING_ROOT_ON and GSK_CERT_VALIDATE_KEYRING_ROOT_OFF) to indicate full or partial validation.

ICSF PKI Services

System SSL: Enterprise PKCS#11 hardware security module

Currently, System SSL supports clear key PKCS #11 token private key objects. With the Crypto Express4S coprocessor configured in Enterprise PKCS #11 mode, support is available for secure PKCS #11 keys. System SSL's PKCS #11 token support is enhanced for secure private keys. This support allows System SSL to use the secure PKCS #11 token private keys in SSL/TLS secure connections that include the Certificate Management APIs (CMS) API interfaces that use private keys.

System SSL: gskkyman certificate creation menus refined

System SSL's **gskkyman** certificate creation menus are refined to step the user of **gskkyman** through different selection menus to define the characteristics of the certificate or certificate request. Depending on what is being created, these characteristics can include certificate authority or user/server certificate, key type, key size, and digital signature algorithm.

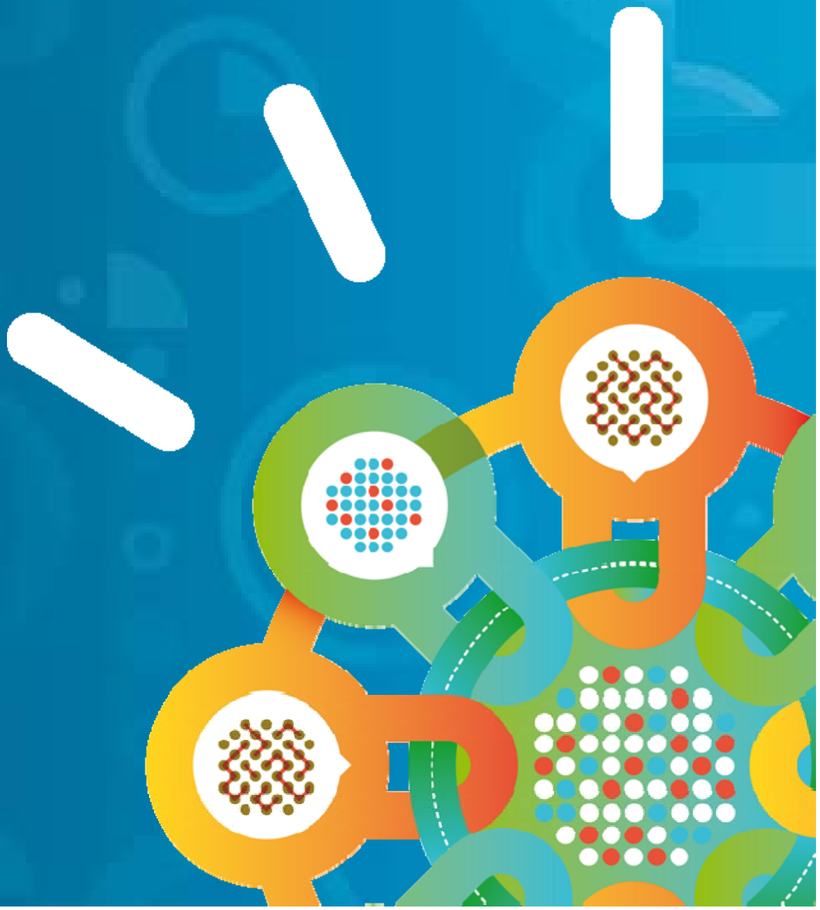
ICSF PKI Services

Reference information:

- *z/OS Cryptographic Services PKI Services Guide and Reference*
- *z/OS Security Server RACF Callable Services*
- *z/OS Security Server RACF Command Language Reference*
- *z/OS Security Server RACF Macros and Interfaces*
- *z/OS Security Server RACF Security Administrator's Guide*
- *z/OS Security Server RACF Data Areas*
- *z/OS Security Server RACF Messages and Codes*
- *z/OS Security Server RACF Security Administrator's Guide*
- *z/OS Security Server RACF System Programmer's Guide*
- *z/OS Security Server RACROUTE Macro Reference*
- *z/OS Cryptographic Services System SSL Programming*

Agenda

- Overview of Security Changes
- z/OS Communication Server
- RACF
- ICSF PKI Services
- z/OS ITDS
- zSecure



z/OS ITDS

- In z/OS V2.1, IBM Tivoli Directory Server (IBM TDS, LDAP) is designed to allow applications, such as those running on Linux clients, to send data to z/OS to be processed by ICSF, leveraging the CryptoExpress4S cards available on zEnterprise servers. This support is designed to allow applications to request secure key cryptographic services from z/OS without exposing the keys in memory. Exploitation of these services is planned to be made available for Linux clients.

z/OS ITDS

In z/OS V2.1, IBM TDS (TDS, LDAP) is designed to support new LDAP extended operations intended to form a foundation, enabling applications running on other systems to encrypt data transmitted over the network, and to store and use objects in ICSF.

This new "crypto-as-a-service“ capability is intended to enable applications to use the secure key storage capabilities of ICSF to provide centralized encryption services, including secure key encryption services while avoiding the need to expose sensitive keys in memory on either z/OS or sending systems.

This new function supports a subset of common cryptographic architecture (CCA) and Enterprise PKCS#11 services, and supports CryptoExpress4S coprocessors when they are configured in Enterprise PKCS#11 mode. This is intended to help centralize key material on z/OS in a way that persists across virtual machine instances to support both active and inactive guests.

The Advanced Crypto Service Provider (ACSP) of the IBM Enterprise Key Management Foundation (EKMF) provides a client programming environment for multiple platforms. It supports both the IBM TDS crypto-as-a-service capabilities, and provides an ACSP Server that can be deployed on z/OS V2.1, z/OS V1.13, and z/OS V1.12 as well as other platforms, and makes financial industry services, and a subset of PKCS#11 programming services, available in an easy-to-consume package.

z/OS ITDS

z/OS V2.1 IBM TDS (LDAP) is designed to comply with NIST SP 800-131A and NSA Suite B by supporting the TLS 1.2 protocol; additionally, support has been added for the TLS 1.1 protocol. IBM TDS and TLS 1.2 provide support for the SHA-256 and SHA-384 algorithms for SSL handshakes, and for AES-GCM ciphers. This is intended to provide better security for LDAP, particularly when used as a user registry, and to help you meet industry standards for security protocols.

z/OS ITDS

Transport Layer Security (TLS) protocol version 1.2

In z/OS V2R1, IBM TDS (TDS, LDAP) introduces support for TLS V1.2 protocol. The TLS V1.2 protocol includes a number of updates to previous versions of the Transport Layer Security (TLS) protocol. This support improves security with secure socket layer communications between IBM Tivoli Directory Server for z/OS client and server. It also includes more cipher suites, and Suite B enablement as provided by z/OS System SSL.

Remote Cryptographic services

By using an LDAP extended operation protocol, distributed applications can now store keys in the persistent key data sets on the host that enables a centralized key management scheme. The remote crypto plug-in extension can be configured to perform PKCS #11 or CCA services functions with ICSF.

ICTX Plug-in

An enhanced ICTX plug-in, which is based on the prior EIM implementation, is now provided with z/OS IBM TDS to perform remote auditing and authorization checking. This enhanced implementation supports 64-bit addressing mode and more bind mechanisms.

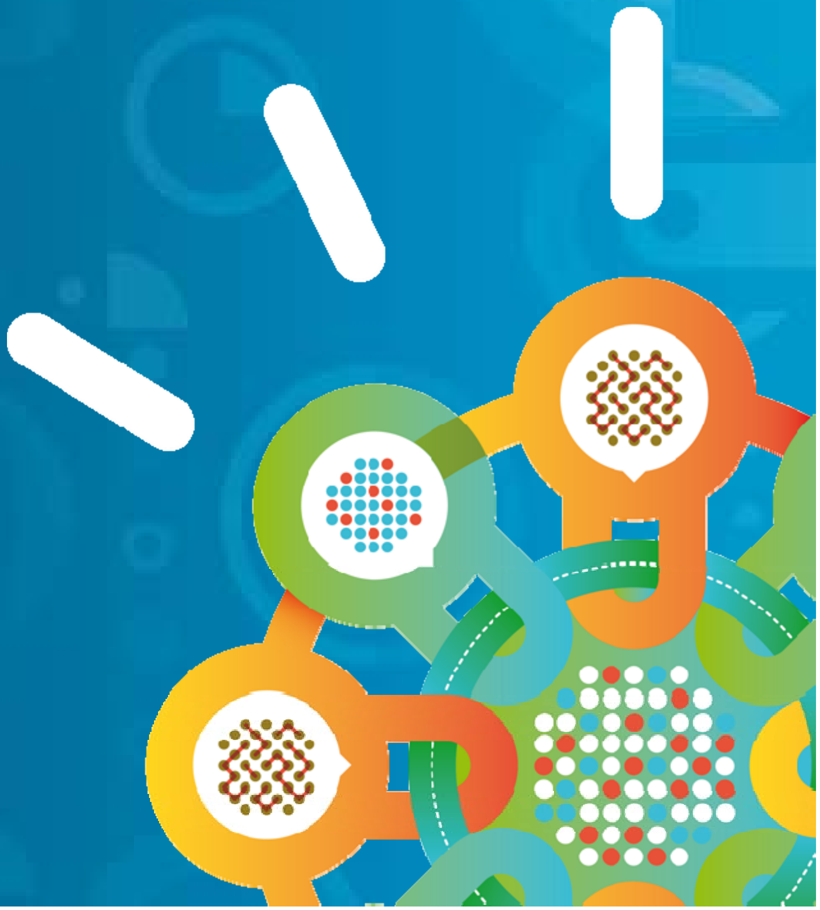
z/OS ITDS

Reference information:

- *z/OS IBM Tivoli Directory Server Administration and Use for z/OS*
- *z/OS IBM Tivoli Directory Server Messages and Codes for z/OS*
- *z/OS IBM Tivoli Directory Server Plug-in Reference for z/OS*
- *z/OS Cryptographic Services ICSF Application Programmer's Guide*
- *z/OS Cryptographic Services ICSF Writing PKCS #11 Applications*
- *z/OS Cryptographic Services System SSL Programming*

Agenda

- Overview of Security Changes
- z/OS Communication Server
- RACF
- ICSF PKI Services
- z/OS ITDS
- zSecure



zSecure

- **Enhanced automated auditing & monitoring support for regulatory compliance**
  - provide the capability to improve results through a comprehensive, automated audit referencing a built-in knowledge base
  - reduce the manual processes for gathering data to support activities for compliance
- **New Digital Certificates management for improved security and reduced complexity**
  - ease of creating, administering, customizing and auditing digital certificates
  - enable user ID tracking in Access Monitor for improved visibility and certificate usage
- **Integrated mainframe security intelligence with QRadar SIEM**
  - enrich real-time collection, normalization & analysis of RACF events to reduce manual security operations
- **Ease of multiple RACF system security administration**
- **z/OS V2R1 currency**

zSecure – DB2

- Collect more resource data from DB2 catalog
  - Databases, Table spaces, Storage groups, Stored procedures, JARs, Sequences
- Show authorized DB2 authids and RACF ids
- Internal DB2 privileges
- Access through DB2 RACF interface
- Analyze / annotate Access Control Matrix
- Many ACL display modes
- Simulate DB2 RACF interface
- Determine which SAF classes are used

zSecure

- RACDCERT command is not simple:
  - It has 25 primary options
  - For some functions, multiple commands are required
  - For example, to generate a new private key for an existing certificate requires usually 4 steps

- Reporting about digital certificates is tedious (no search)

- RACF ISPF user interface is single command oriented and uses command output capturing to allow up/down scrolling

- RACDCERT command cannot be routed using RRSF

zSecure

Built-in standards (C1 / C2 / B1) are considered to be inflexible

- Need to adapt more quickly to external standard updates
- Audit concern principle misses the positive confirmation that it is OK
- Audit concerns not customizable (exceptions / mitigating controls)

Customers create ad-hoc reporting, partly 2-pass queries

- Need something less ad-hoc and easier to customize
- Need something that works almost out of the box
- Need to combine information from many report types
- Need to customize / define who is considered authorized

Scope of external standards is increasing

- Need to collect more settings from more subsystems.

zSecure

- Support newer external standards
  - DISA STIG for z/OS RACF
  - DISA STIG for z/OS ACF2
  - IBM outsourcing GSD331/iSec
- Eliminate need for 2-pass queries
- Show positive compliance, not just non-compliance
- Allow showing progress in compliance efforts
- Support in-standard customization
  - Members with authorized IDs (using STIG naming)
  - Allow rule override (suppression) with reason – visible in reporting
  - Allow creation and seamless integration of site standards

* STIG: Security Technical Implementation Guide; Guidelines from US Defense Information Systems Agency (DISA)

** GSD331: IBM's primary information security controls documentation for Strategic Outsourcing customers

zSecure z/OS V2R1 currency

- ✓New Network Management Interface in Communications Server exploited
- ✓New SMF records for Communications Server supported
- ✓Support reporting about
  - ✓RRSF use of IPV6
  - ✓Flash Memory Paging
- ✓Knowledge base updated for
  - ✓SVCs, Program Calls and PPT entries
  - ✓Resources in the CRYPTOZ resource class
- ✓RACF profile change notification to DB2 suppressed if changes are in RACF-Offline database

zSecure z/OS V2R1 currency

- ✓New resource classes:
  - ✓DB2 Global Variables: M/GDSNGV
  - ✓z/OS PKISERV
  - ✓System Automation: SYSAUTO
- ✓New RACF field:
  - ✓CERTGREQ: Gencert was issued for DIGTCERT
- ✓SMF changes:
  - ✓SMF 92 subtype 11 → SMF 92 subtype 16/17
    - ✓Supported in UI, and SMF 92(16) sent to QRadar
  - ✓Added SMF 104 (RMF distributed platform)
  - ✓Added SMF 90(36) (SET CON)

zSecure z/OS V2R1 currency

- ✓JES changes:
  - ✓8-char jobclasses
  - ✓Jobclass checking
    - ✓New fields in SYSTEM newlist
  - ✓New exits (59/60)
- ✓System Parameters:
  - ✓IPLPARM
    - ✓5 new fields IPLPARM_* in system newlist

zSecure

- **Reference information:**
- *IBM Security zSecure Release information*
- *IBM Security zSecure CARLa-Driven Components Installation and Deployment Guide*
- *IBM Security zSecure Admin and Audit for RACF Getting Started*
- *IBM Security zSecure Admin and Audit for RACF User Reference Manual*
- *IBM Security zSecure Audit for ACF2 Getting Started*
- *IBM Security zSecure Audit for ACF2 User Reference Manual*
- *IBM Security zSecure Alert User Reference Manual*
- *BM Security zSecure Command Verifier User Guide*
- *IBM Security zSecure CICS Toolkit User Guide*
- *IBM Security zSecure Messages Guide*
- *IBM Security zSecure Quick Reference*
- *IBM Security zSecure Visual Client Manual*

System z Security Portal

IBM urges all z/OS users to get registered for the System z Security Portal and to keep current with security and system integrity fixes.

Security and system integrity fixes are included in Recommended Service Upgrades (RSUs), and maintaining RSU currency can help you minimize exposure to security and integrity issues.

The System z Security Portal is intended to help you stay current with security and system integrity fixes.

The System z Security Portal now also provides Associated Common Vulnerability Scoring System (CVSS) V2 ratings for new APARs.

Because widespread specifics about a vulnerability could increase the likelihood that an attacker could successfully exploit it

In response to many customer requests to maintain the confidentiality of any vulnerability information reported to IBM, this information is available only to registered z/OS customers who agree not to distribute it to others.

Questions

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT SYSTEMS AND PRODUCTS ARE IMMUNE FROM THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

IBM®

ibm.com/security