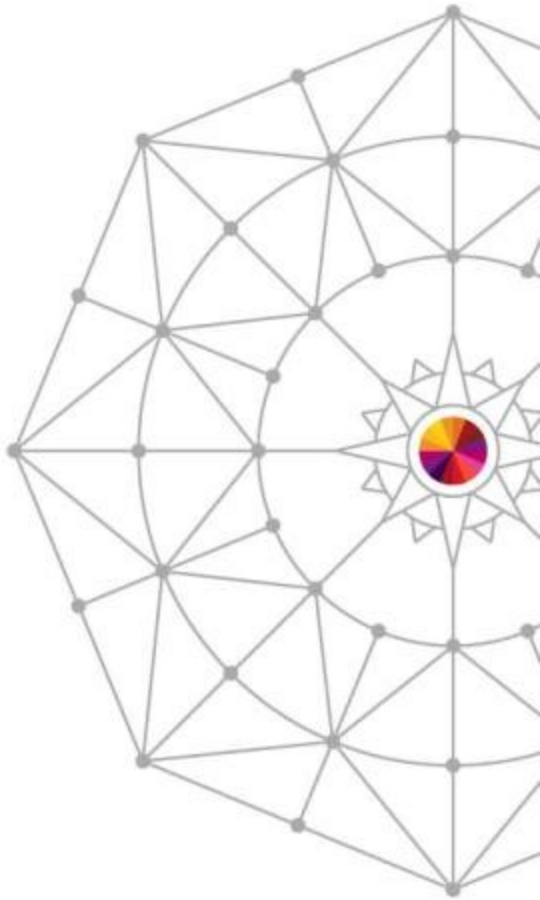
#SHAREorg

SHARE
Technology · Connections · Results

ICSF Update

Steven R. Hart
IBM

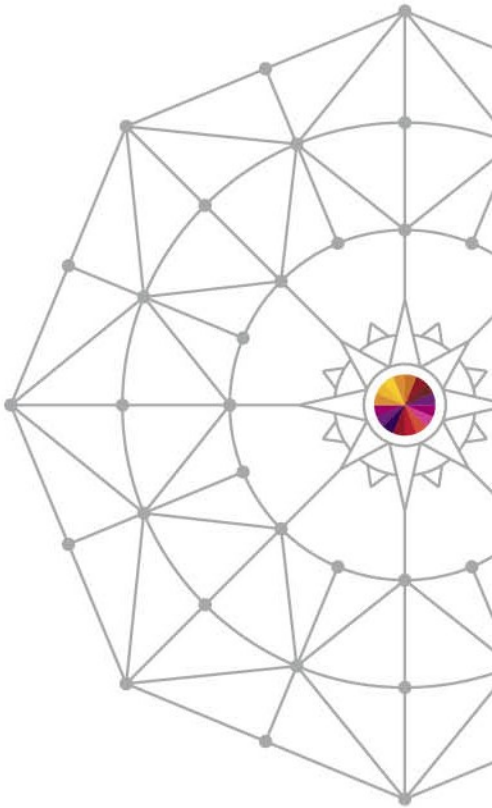
March 10, 2014
Session Number 14956



SHARE in Anaheim

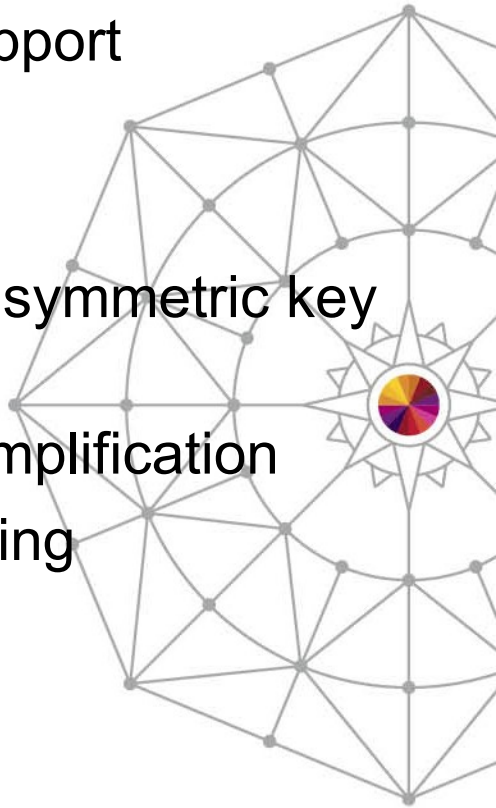
ICSF FMID HCR77A1

- Cryptographic support for z/OS V1R13-V2R1
  - Web deliverable only
  - HCR77A0 is in the base of z/OS V2R1
  - GA September 20, 2013



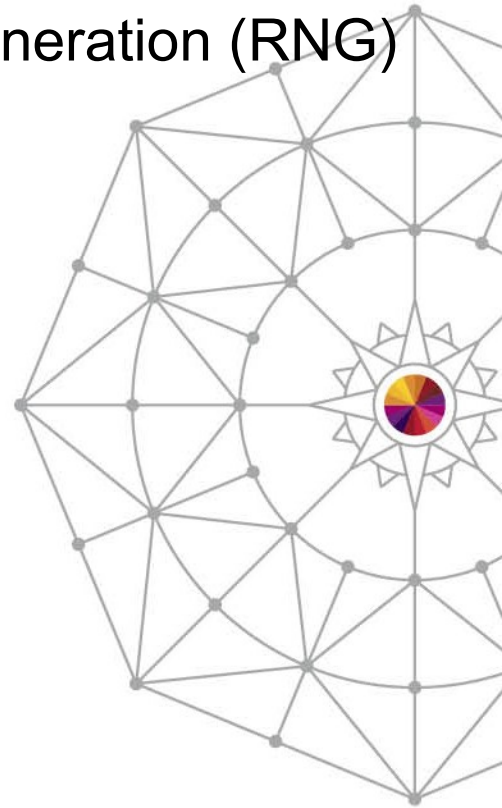
New Features

- Expanded EMV (EuroPay, MasterCard, Visa) Support
- Unique Key Derive IPEK Support
- DESUSECV Support
- Fixed-Length Payload section for variable-length symmetric key tokens
- User Defined Extension (UDX) Reduction and Simplification
- Remote Key Export (RKX) Enhanced Key Wrapping
- Enterprise PKCS #11 Phase 2
- RSA Master Key Set from TKE
- AES MAC Enhancement
- SAF ACEE Selection



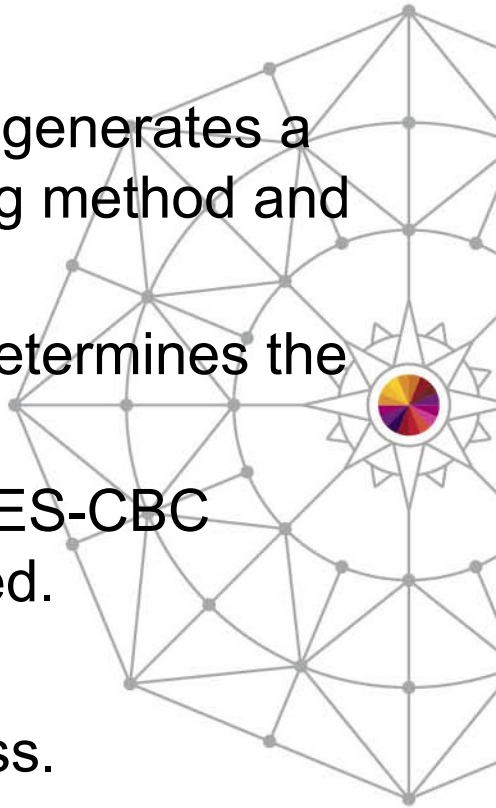
New Features continued

- One Way Hash (OWH) and Random Number Generation (RNG) Access
- Dynamic Special Secure Mode (SSM)
- AP Configuration Simplification
- Improved ICSF CTRACE Support
- CCF Removal
- KDS Key Utilization Statistics
- IQF Access (HCR77A0 and above)
- ICSF HCR77A1 Migration Checks
- DK AES PIN Support (HCR77A0 and above)
- PKT UDX Support (HCR7790 and above)



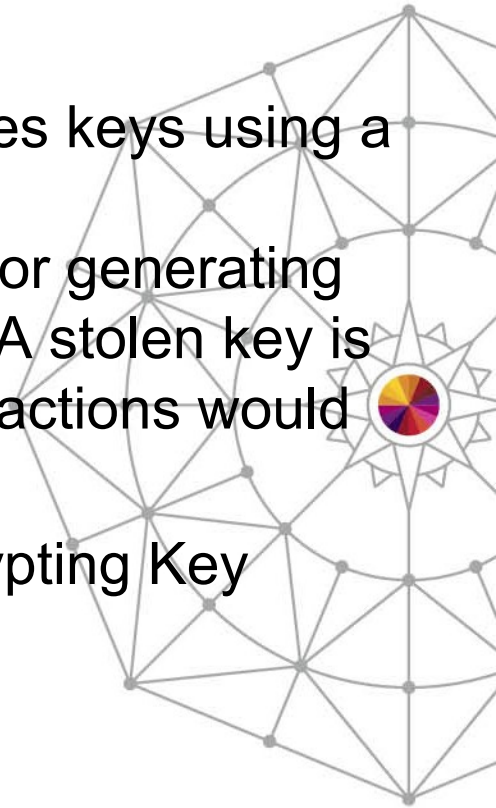
Expanded EMV (EuroPay, MasterCard, Visa) Support

- Problem / Need
  - The Diversified Key Generate callable service generates a key based on a key-generating key, processing method and supplied parameters.
  - The control vector of the key-generating key determines the type of target key that can be generated.
  - The EMV Specification indicates using the TDES-CBC diversification process which was not supported.
- Solution
  - Support the TDES-CBC key generation process.
- Benefit Value
  - Our support aligns with EMV specifications for key diversification.



Unique Key Derive IPEK Support

- Problem / Need
  - The Unique Key Derive callable service derives keys using a base derivation key and derivation data.
  - Each key uses the previous key as the base for generating the next key, then throws away the previous. A stolen key is only good for a single transaction; other transactions would not be affected.
  - Customers need to know the Initial Pin Encrypting Key (IPEK) for a particular device.

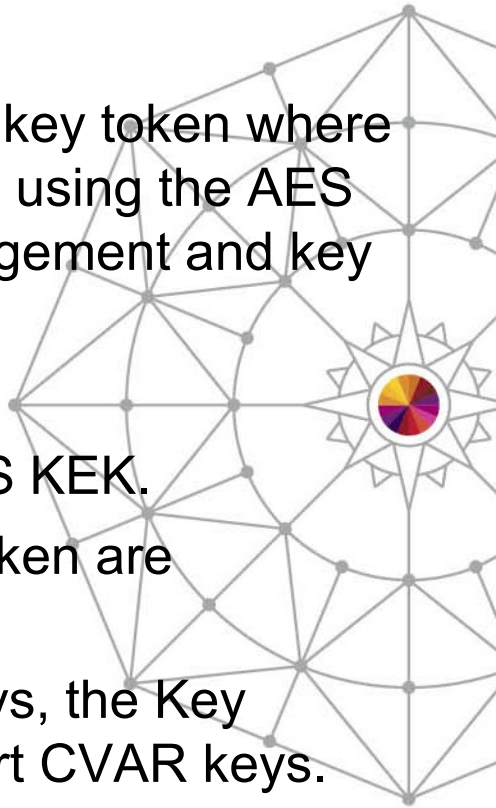


Unique Key Derive IPEK Support

- Solution
  - Return the initial pin encryption key (IPEK) derived from the base derivation key (BDK) and initial derivation data in a TDES token or TR-31 key block.
- Benefit / Value
  - The BDK does not need to be shared with remote devices. Instead the IPEK can be generated from the BDK and loaded onto a device with its own unique serial number. Both the device and the issuer can generate the same set of keys independently and communicate encrypted messages.

DESUSECV Support

- Problem / Need
  - DESUSECV is a type of variable-length symmetric key token where the DES key and its control vector (CV) is wrapped using the AES key wrapping method. This ensures that key management and key usage fields are maintained from export to import.
    - External only (not encrypted under a MK).
    - Uses AESKWCV key wrapping method and AES KEK.
    - Key-management and key-usage fields in the token are unused/reserved.
    - Now that DES keys can be wrapped by AES keys, the Key Token Build2 service must be updated to support CVAR keys.

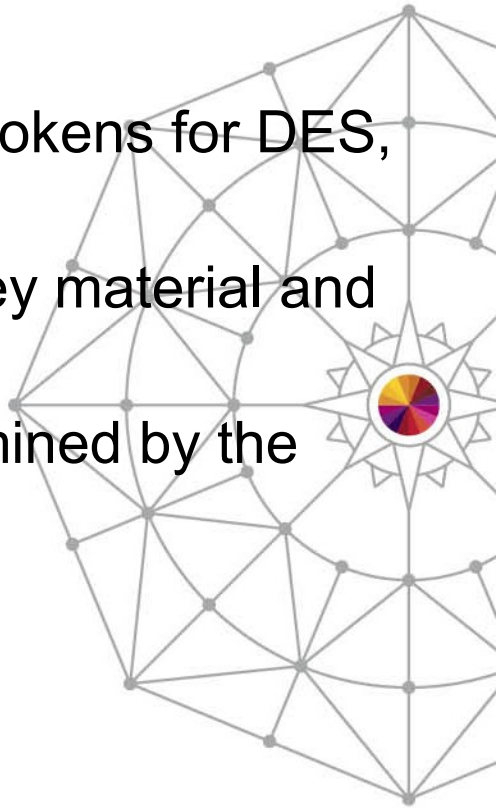


DESUSECV Support

- Solution
  - New DESUSECV key token to contain AES-wrapped DES key along with its CV.
- Benefit / Value
  - The control vector is maintained during DES key wrapping.
  - AES provides stronger encryption.

Fixed-Length Payload section for variable-length symmetric key tokens

- Problem / Need
  - ICSF supports variable-length symmetric key tokens for DES, AES and HMAC keys.
  - The payload section contains the encrypted key material and padding bytes up to the nearest multiple of 8.
  - The length of the encrypted key can be determined by the payload length.

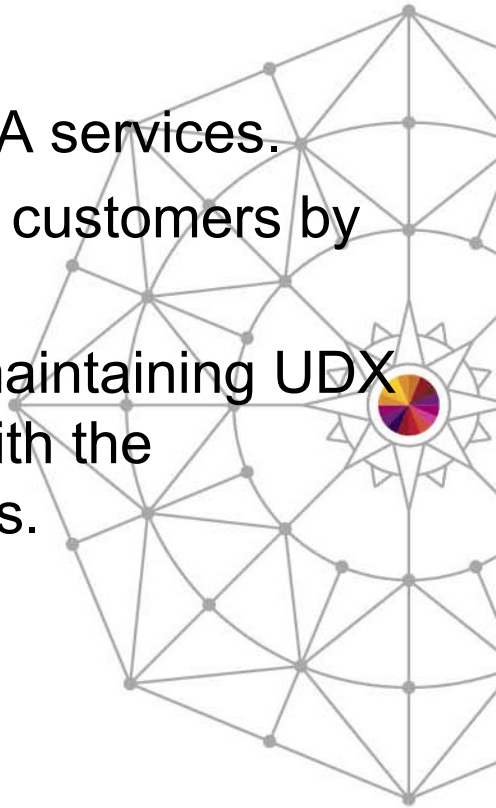


Fixed-Length Payload section for variable-length symmetric key tokens

- Solution
  - Use fixed-length payloads to obscure the length of the encrypted key.
    - New key types, such as DESUSECV, will use fixed-length payloads.
    - AES CIPHER, IMPORTER and EXPORTER keys will have options to choose whether to create a token with the fixed-length or variable-length payload.
    - Other AES keys will use fixed-length payloads.
    - HMAC keys will continue to use variable-length payloads.
- Benefits
  - Ability to conceal the length of the encrypted key within a variable-length symmetric key token.

User Defined Extension (UDX) Reduction and Simplification

- Problem / Need
  - A UDX is a custom extensions to the base CCA services.
  - UDXes are provided under contract to specific customers by IBM Global Business Services.
  - The IBM effort and expense associated with maintaining UDX packages in the field is growing problematic with the proliferation of CCA releases and interim MCLs.



User Defined Extension (UDX) Reduction and Simplification

- Solution
  - Three new services were added to the CCA 4.4 code base (available with CEX4C and CEX3C cryptographic coprocessors) and surfaced to z/OS customers through the following ICSF callable services.
    - Authentication Parameter Generate – CSNBAPG
      - Generates an authentication parameter and returns it encrypted using the supplied key.

User Defined Extension (UDX) Reduction and Simplification

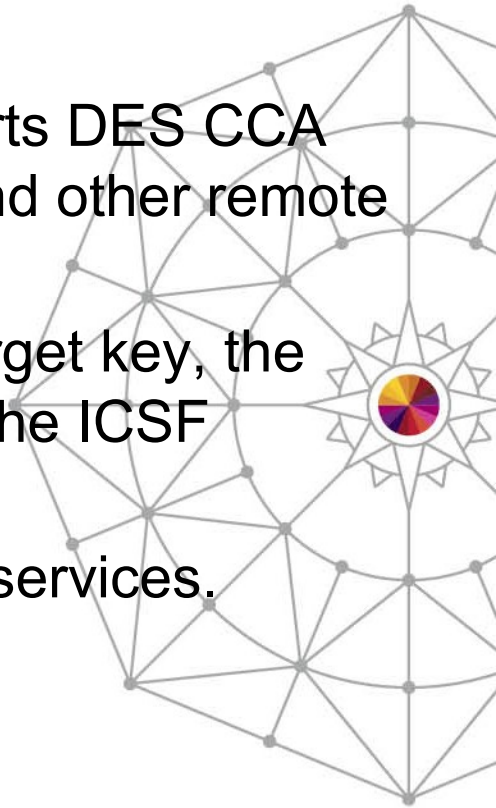
- Recover PIN From Offset – CSNBPFO
  - Calculates the encrypted customer-entered PIN from a PIN generating key, account information, and an IBM-PINO offset. The customer-entered PIN is returned in a PIN block formatted to the PIN profile and PAN data specifications and encrypted with supplied key supplied.
- Symmetric Key Export with Data – CSNDSXD
  - Export a symmetric key, along with application supplied data, encrypted with an RSA key using the PKCS-1.5 block type 2 formatting algorithm.

User Defined Extension (UDX) Reduction and Simplification

- Benefits
  - Absorbing UDX functions into the CCA base reduces maintenance costs.
  - The UDX functions become generally available to all customers.

Remote Key Export (RKX) Enhanced Key Wrapping

- Problem / Need
  - The Remote Key Export callable service exports DES CCA and DES RKX keys for distribution to ATMs and other remote devices.
  - To change the wrapping method used for a target key, the user must use the DEFAULTWRAP option in the ICSF options data set.
  - This is a global option that affects other ICSF services.

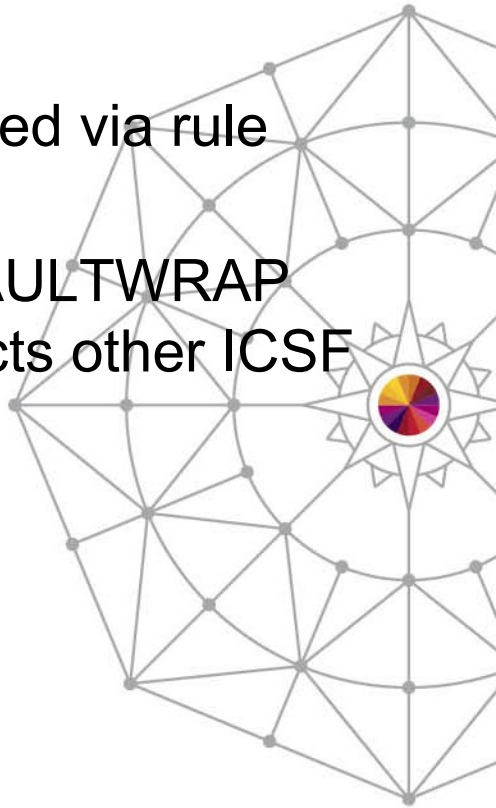


Remote Key Export (RKX) Enhanced Key Wrapping

- Solution
  - Add rule array keywords to the CSNDRKX service to indicate the key wrapping method to be used for output DES CCA key tokens:
    - USECONFIG - Specifies that the configuration setting for the default wrapping method is to be used to wrap the key. This is the default.
    - WRAP-ENH - Specifies that the new enhanced wrapping method is to be used to wrap the key.
    - WRAP-ECB - Specifies that the original wrapping method is to be used.
    - ENH-ONLY - Specify this keyword to indicate that the key once wrapped with the enhanced method cannot be wrapped with the original method. This restricts translation to the original method.

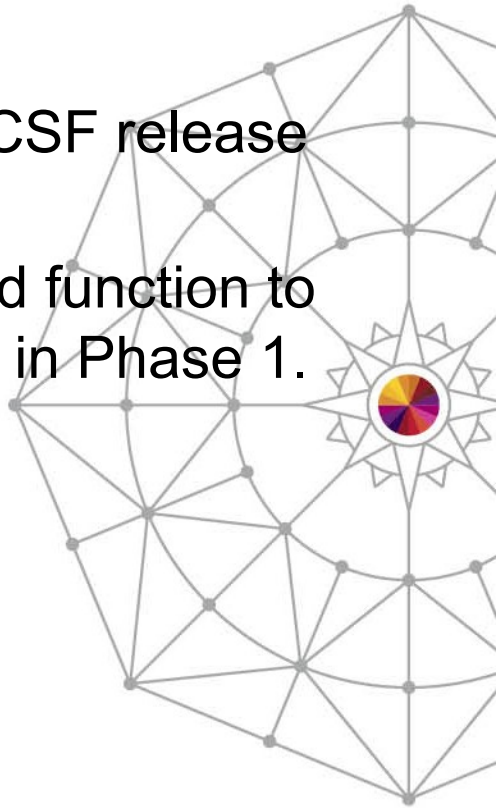
Remote Key Export (RKX) Enhanced Key Wrapping

- Benefits
  - Remote key wrapping methods may be specified via rule array keywords to the RKX service.
  - RKX does not have to rely on the global DEFAULTWRAP option in the ICSF options data set which affects other ICSF services.



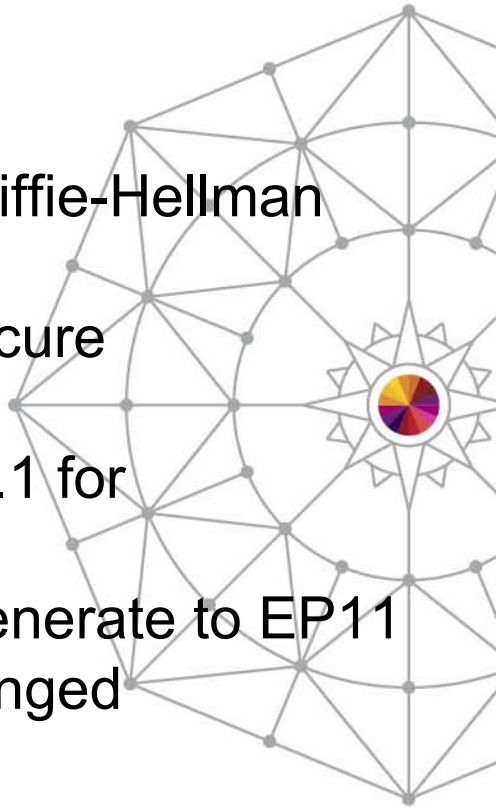
Enterprise PKCS #11 Phase 2

- Problem / Need
  - Enterprise PKCS #11 Phase 1 was added in ICSF release HCR77A0.
  - This support provides additional algorithms and function to Enterprise PKCS #11 that were not completed in Phase 1.



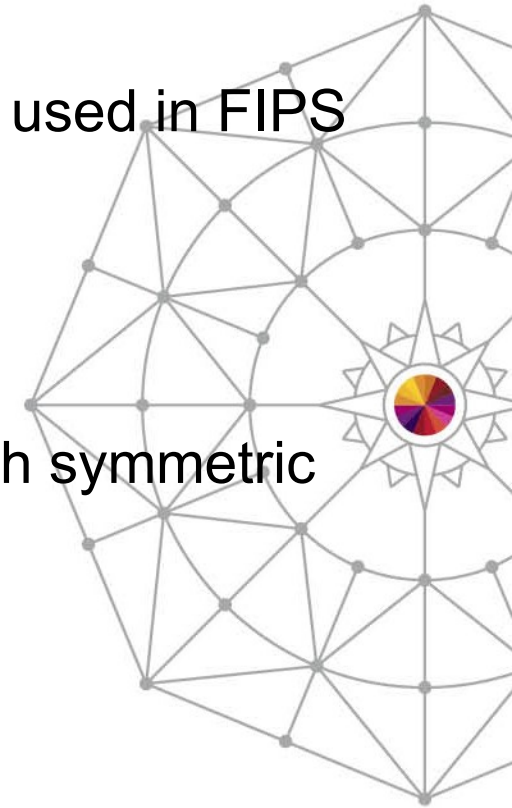
Enterprise PKCS #11 Phase 2

- Solution
  - ICSF and P11 Firmware Updates
    - Secure Diffie-Hellman and Elliptic Curve Diffie-Hellman keys
    - Key derivation will allow base key to be secure
    - Secure RSA-PSS
      - Mechanism introduced in PKCS #11 v2.1 for signing/verifying digital signatures
    - Offload DSA and DH domain parameter generate to EP11
    - Allow compliance mode of a key to be changed



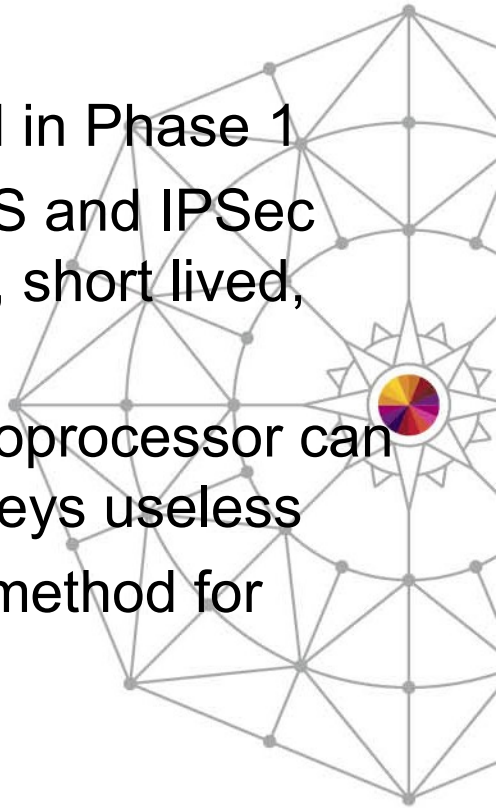
Enterprise PKCS #11 Phase 2

- ICSF Updates
  - Allow clear key brainpool EC curves to be used in FIPS mode
  - Clear key RSA-PSS
  - Secure key Brainpool EC
    - CEX4P already allowed BP
  - Allow Wrap/Unwrap of symmetric keys with symmetric keys



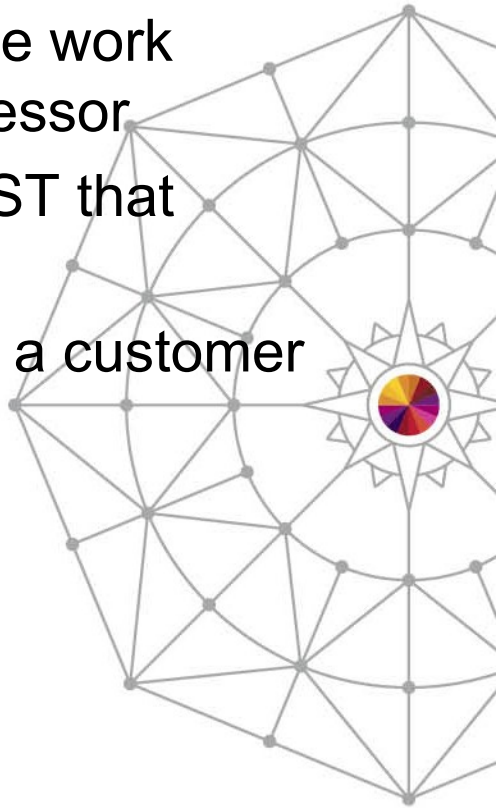
Enterprise PKCS #11 Phase 2

- Benefits
  - Add secure key support for algorithms skipped in Phase 1
  - Secure base keys on key derivation allows TLS and IPSec base keys to be secure and still produce clear, short lived, and better performance session keys
  - Changing the compliance mode of the EP11 coprocessor can now be done without making existing secure keys useless
  - RSA-PSS mechanism is considered stronger method for signing/verifying digital signatures



Enterprise PKCS #11 Phase 2

- Domain parm gen offload moves CPU intensive work currently done in software to the EP11 coprocessor
- Brainpool EC curves supports the ruling by NIST that Brainpool is allowed in FIPS mode
- Wrap/unwrap symmetric with symmetric fulfills a customer requirement

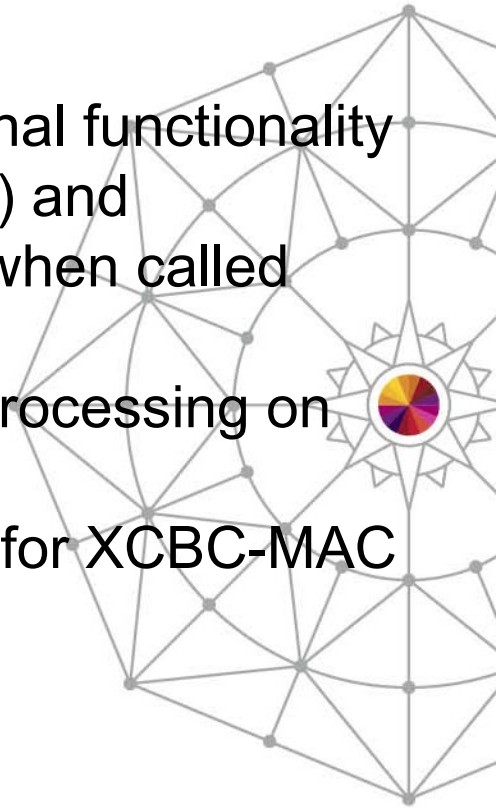


RSA Master Key Set from TKE

- Problem / Need
  - The Trusted Key Entry (TKE) needs to be able to set the RSA Master Key during a disaster recovery procedure.
- Solution
  - A new rule was added to the ICSF CSFPCI Service that allows a RSA Master Key set request from TKE.
- Benefits
  - Additional disaster recovery capability from TKE.

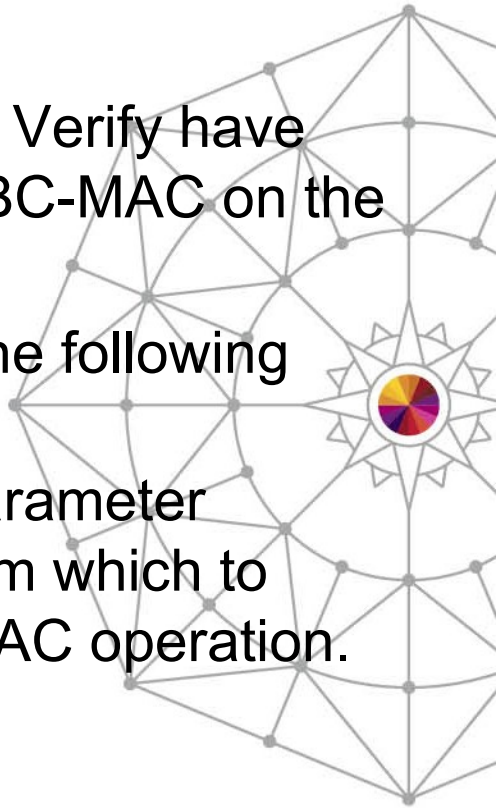
AES MAC Enhancement

- Problem / Need
  - z/OS Communications Server requires additional functionality for the Symmetric MAC Generate (CSNBSMG) and Symmetric MAC Verify (CSNBSMV) services when called with the XCBC-MAC processing rule.
    - Support zero-length text for XCBC-MAC processing on the LAST call of a multi-part operation.
    - Support key lengths greater than 128 bits for XCBC-MAC processing.



AES MAC Enhancement

- Solution
  - Symmetric Mac Generate and Symmetric Mac Verify have been updated to allow zero-length text for XCBC-MAC on the LAST call of a multi-part operation.
  - Both services have been updated to support the following new key rule:
    - KEY-DRV - This specifies that the key parameter contains up to 256 bits of key material from which to derive a 128-bit AES key for the XCBC-MAC operation. Only valid with XCBC-MAC.
- Benefits
  - ICSF behavior more closely follows RFC 3566 and 4434.



SAF ACEE Selection

- Problem / Need
  - IBM Communications Server calls ICSF callable services on behalf of its users that need encryption.
  - This requires IBM Communications Server to obtain access to profiles in the CSFSERV, CSFKEYS, XCSFKEY, and CRYPTOZ classes that protect ICSF keys and services.
  - All users of IBM Communications Server then have the same level of access to ICSF keys and services which is likely unnecessary.
  - IBM Communications Server requested an interface for specifying an ACEE (security context) to be used for authority checking when performing operations on behalf of their callers.

SAF ACEE Selection

- Solution
  - ICSF has provided a new callable service, SAF ACEE Selection (CSFACEE), for authorized callers (either system key or supervisor state) to cause ICSF to use the caller's authority for SAF checking of profiles in CSFKEYS, CSFSERV, XCSFKEY and CRYPTOZ classes.
  - This new callable service takes as input an ENVR object data structure to be used for authorization checks for the requested service.
  - For example, if the direct ICSF callable service call was:

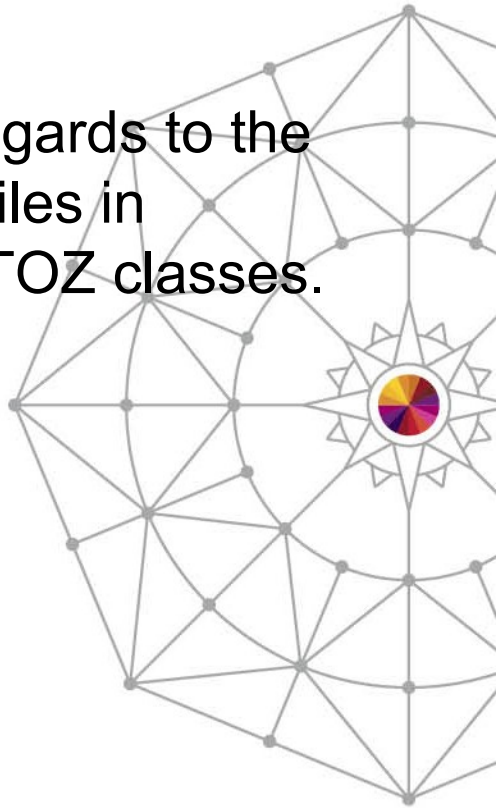
CALL CSFZYX(parm1, parm2, parm3);

  - The invocation via this service would be:

CALL CSFACEE(envr, "CSFZYX ", parm1, parm2, parm3);

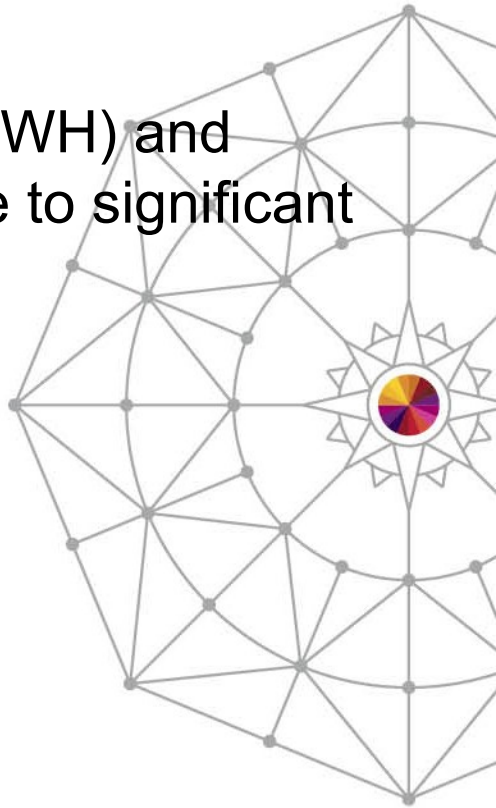
SAF ACEE Selection

- Benefits
  - Authorized callers have more flexibility with regards to the security context used for SAF checking of profiles in CSFKEYS, CSFSERV, XCSFKEY and CRYPTOZ classes.



One Way Hash (OWH) and Random Number Generation (RNG) Access

- Problem / Need
  - CSFSERV SAF checks for One Way Hash (OWH) and Random Number Generation (RNG) contribute to significant CPU consumption.

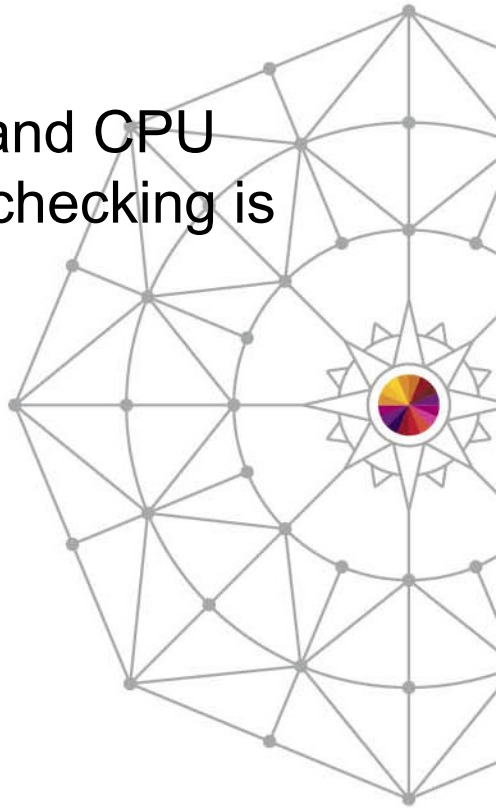


One Way Hash (OWH) and Random Number Generation (RNG) Access

- Solution
  - 2 new resources were added to the XFACILIT SAF resource class for disabling OWH and RNG SAF checking.
  - If the CSF.CSFSERV.AUTH.CSFOWH.DISABLE resource is defined within the XFACILIT class, the SAF authorization check is disabled for this resource.
  - If the CSF.CSFSERV.AUTH.CSFRNG.DISABLE resource is defined within the XFACILIT class, the SAF authorization check is disabled for this resource.

One Way Hash (OWH) and Random Number Generation (RNG) Access

- Benefits
  - Significant improvements in ICSF throughput and CPU utilization for OWH and RNG calls when SAF checking is disabled.



Dynamic Special Secure Mode (SSM)

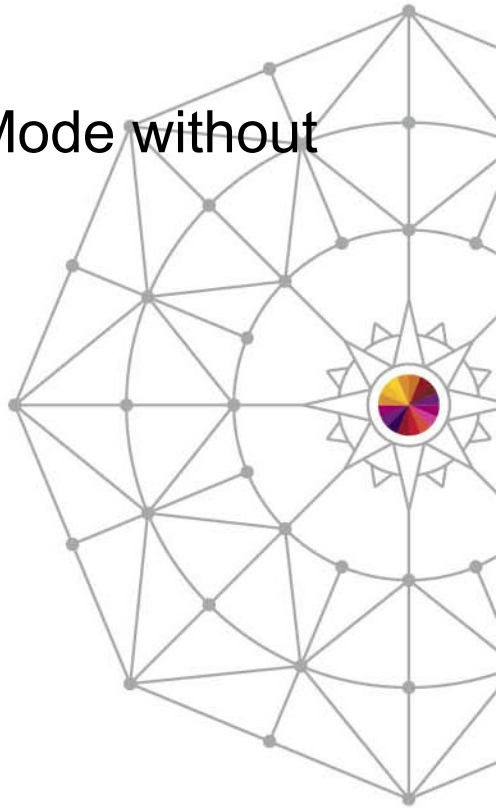
- Problem / Need
  - SSM provides an additional level of control (in addition to CSFSERV SAF authority checking) over access to some services which import clear keys (Secure Key Import – CSNBSKI, CSNESKI; Multiple Secure Key Import – CSNBSKM, CSNESKM; Secure Key Import 2 – CSNBSKI2, CSNESKI2) as well as the Clear PIN Generate – CSNBPGN, CSNEPGN service.
  - Installations usually do not default SSM=YES.
  - They only want it turned on when its needed.
  - Currently this requires an ICSF restart.

Dynamic Special Secure Mode (SSM)

- Solution
  - A new resource, CSF.SSM.ENABLE, was added to the XFACILIT SAF resource class for dynamically enabling SSM.
  - When the CSF.SSM.ENABLE resource is defined, it will be equivalent to having SSM=YES in the option dataset.
  - When the CSF.SSM.ENABLE resource is not defined, then the installation option (startup or default) will be used.
  - The resource will be checked during ICSF startup and each time the XFACILIT class is refreshed.

Dynamic Special Secure Mode (SSM)

- Benefits
  - Ability to dynamically turn on Special Secure Mode without having to restart ICSF.



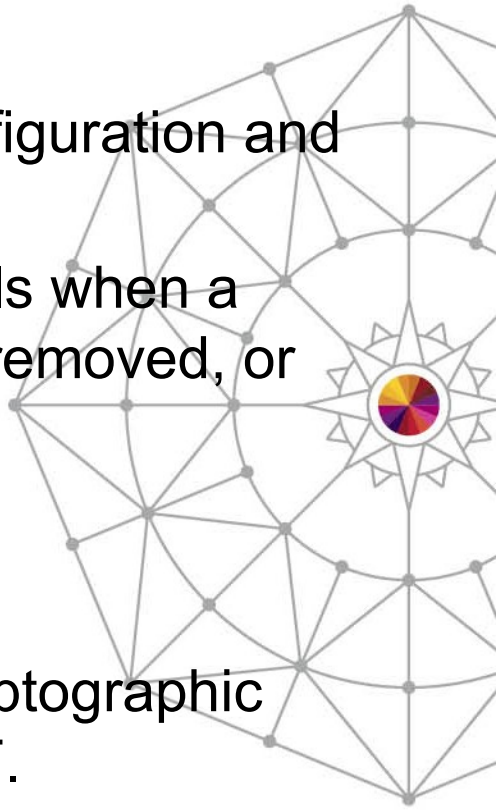
AP Configuration Simplification

- Problem / Need
  - Adjunct Processor (AP) / Cryptographic Coprocessor configuration involves a specific multi step process. Cryptographic Coprocessors must be configured online by the support Support Element (SE) and then activated on the ICSF Cryptographic Coprocessor Management Panel.
  - To reconfigure a Cryptographic Coprocessor you must deactivate it on the ICSF Cryptographic Coprocessor Management Panel and then configure it offline using the SE.
  - When this specific multi step process is not followed ICSF may have difficulty communicating with the Cryptographic Coprocessor.

AP Configuration Simplification

- Solution
  - Redesign of ICSF adjunct processor (AP) configuration and activation.
  - ICSF improvements to better handle SE signals when a Cryptographic Coprocessor has been added, removed, or reconfigured.

- Benefits
  - Better serviceability characteristics for the Cryptographic Coprocessor configuration component of ICSF.

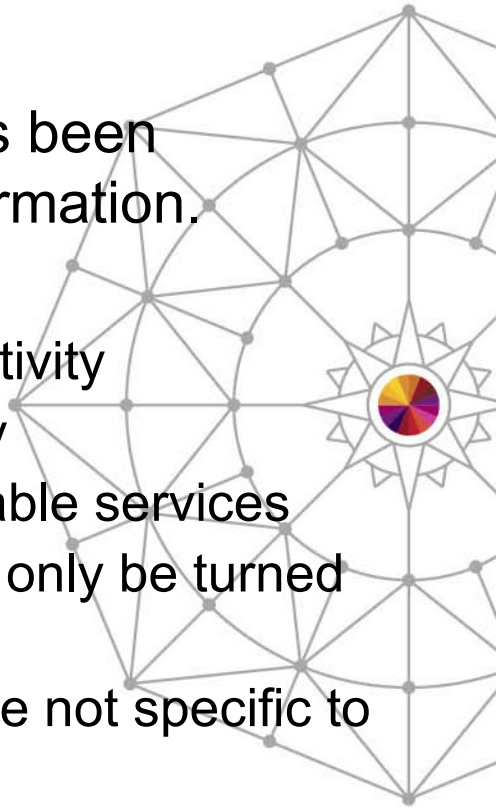


Improved ICSF CTRACE Support

- Problem / Need
  - ICSF CTRACE support provides limited diagnostic information.
  - The ICSF CTRACE buffer is often wrapped causing a loss of useful trace data.

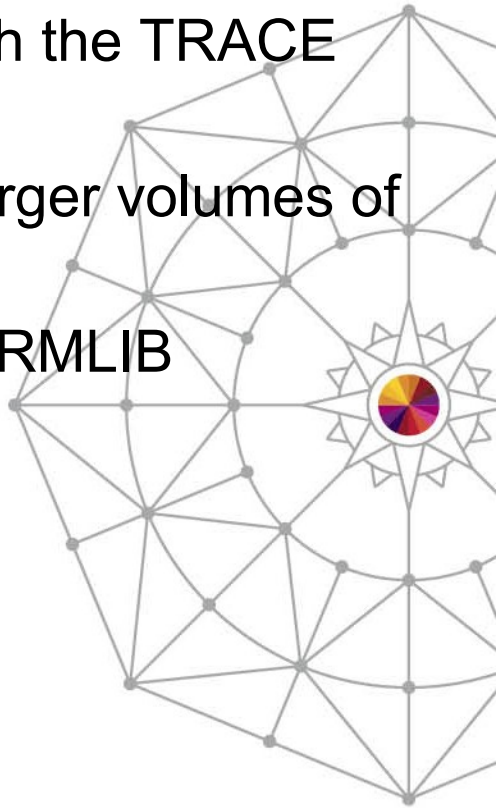
Improved ICSF CTRACE Support

- Solution
  - The ICSF Component Trace record format has been enhanced to provide additional diagnostic information.
  - Granular trace filtering capabilities
    - CARDIO – trace cryptographic coprocessors activity
    - KDSIO – trace CKDS, PKDS, and TKDS activity
    - SYSCALL – trace entry and exit from ICSF callable services
    - DEBUG – special debug mode filter that should only be turned on at the direction of IBM service professionals
    - MIN – trace a minimum set of operations that are not specific to the other filters
    - ALL – trace all ICSF trace records regardless of their filter



Improved ICSF CTRACE Support

- Ability to dynamically change trace options with the TRACE CT command.
- Optional use of external writer for offloading larger volumes of trace data to DASD or Disk.
- CTRACE settings now configurable from a PARMLIB configuration data set (CTICSF00).
- Configurable buffer allocation size.
- Ability to trace by Job Name or ASID.

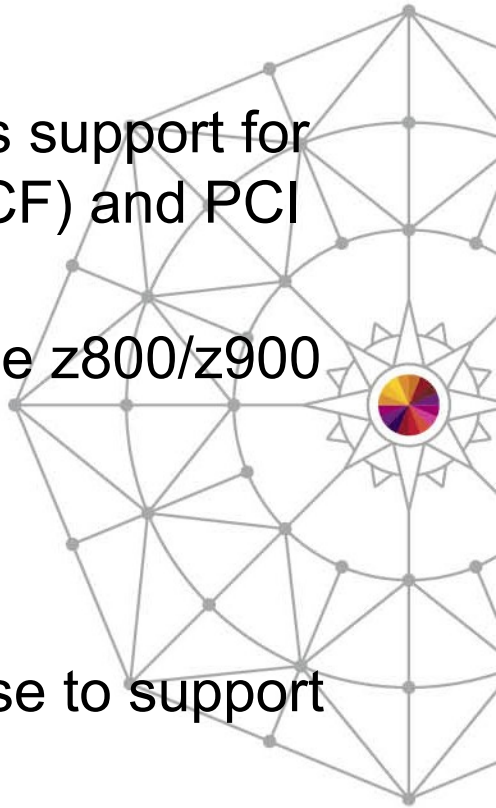


- Benefits
  - Improved serviceability for ICSF.

CCF Removal

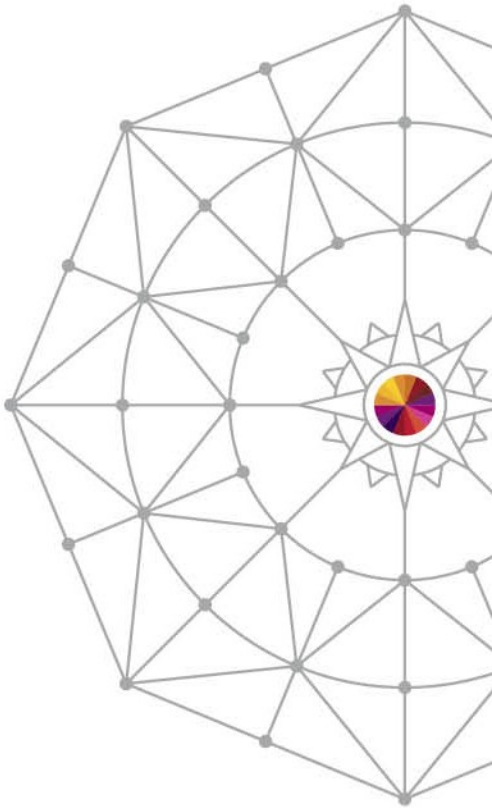
- Problem / Need
  - A large portion of the ICSF code base includes support for legacy Cryptographic Coprocessor Facility (CCF) and PCI Cryptographic Coprocessors.
  - CCF's and PCICC's were last available with the z800/z900 enterprise class servers.

- Solution
  - ICSF WD#12 HCR77A0 is the last ICSF release to support z800/z900 (CCF and PCICC).
  - ICSF WD#13 HCR77A1 removed all CCF and PCICC related code from the component.



CCF Removal

- Benefits
  - Smaller storage footprint
  - Reduced maintenance and development costs
  - Reduced testing environments



KDS Key Utilization Statistics

- Problem / Need
  - ICSF Key Data Sets (CKDS, PKDS, and TKDS) do not maintain statistics for when a cryptographic key was “last referenced”.
  - As ICSF Key Data Sets continue to grow over time it becomes difficult to determine which cryptographic keys are being used and which are stale.

KDS Key Utilization Statistics

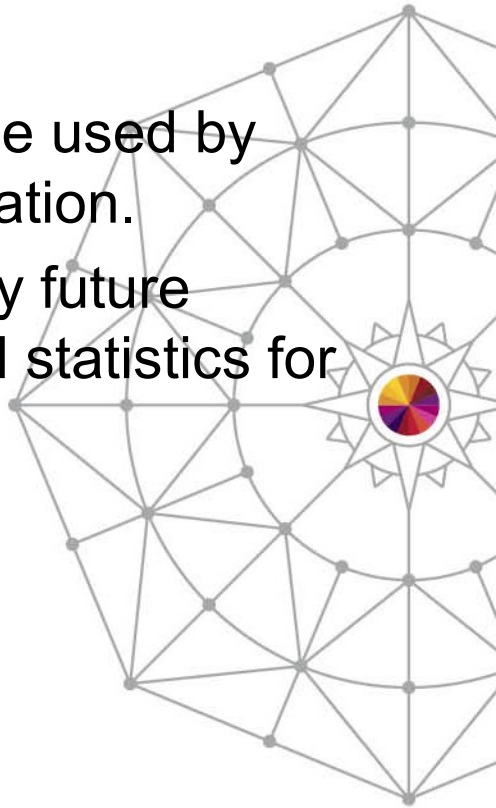
- Solution
  - Provide a new key record format (KDSR) for internally saving meta-data and statistics about each cryptographic key.
  - The Coordination KDS Administration (CSFCRC and CSFCRC6) callable service has be enhanced to perform a coordinated conversion of an old format *KDS to the new KDSR format.
  - Included in this new record format is a section used to track the “last referenced” date for each cryptographic key.

KDS Key Utilization Statistics

- The reference date is the last time a record was used in a cryptographic operation or read, such that the retrieved key may have been used in a cryptographic operation. The read is interpreted as a show of interest, so the reference date is updated.
- A new ICSF startup option, KDSREFDAYS(n), has been added that specifies (in days) how often a record should be written for a reference date/time change.
- KDSREFDAYS(0) means that ICSF will not keep track of key reference dates. The default is KDSREFDAYS(1). The maximum value allowed is KDSREFDAYS(30).

KDS Key Utilization Statistics

- Benefits
  - Cryptographic key reference information can be used by future functions that require this type of information.
  - The new key record format can be extended by future functions that require additional meta-data and statistics for cryptographic keys.

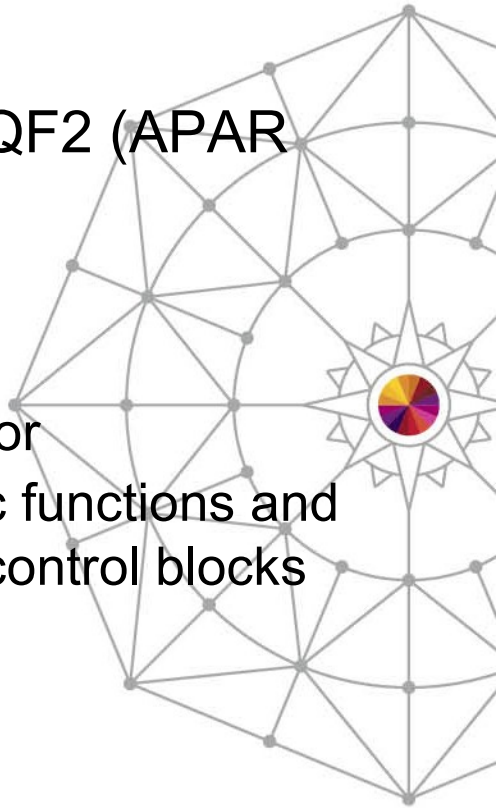


IQF Access (HCR77A0 and above)

- Problem / Need
  - CSFIQF is protected by the CSFSERV class because it can call the cryptographic coprocessor.
  - Some information returned by IQF, such as the availability of certain cryptographic functions and hardware, does not actually require a call to the cryptographic coprocessor.
  - Regardless of the information being requested all calls to IQF include the additional overhead of the SAF check.

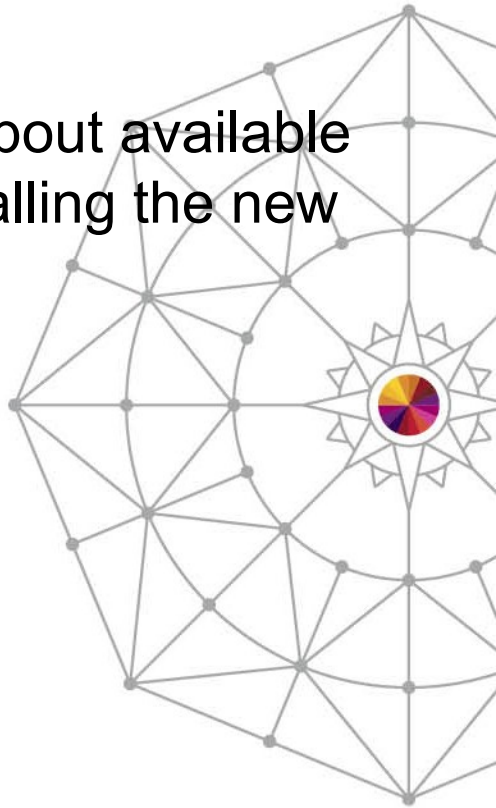
IQF Access (HCR77A0 and above)

- Solution
  - ICSF has added a new callable service, CSFIQF2 (APAR OA41345).
  - This callable service will:
    - NOT be SAF protected
    - NOT make calls to any cryptographic coprocessor
    - Return information about available cryptographic functions and hardware that was collected from various ICSF control blocks



IQF Access (HCR77A0 and above)

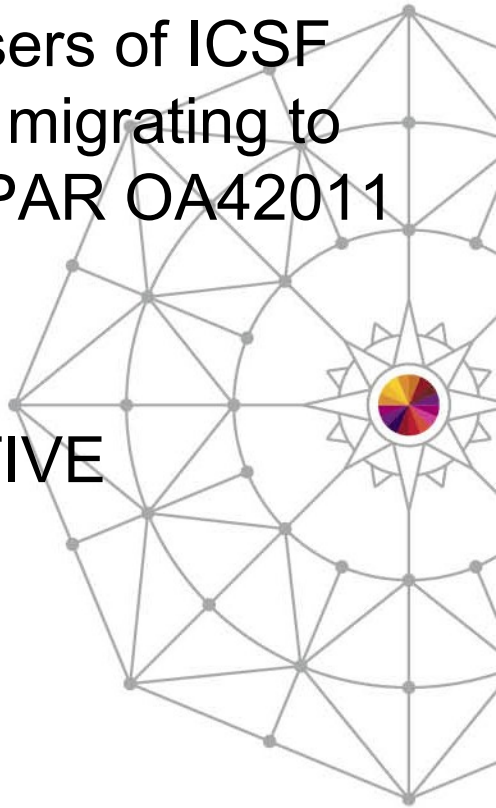
- Benefits
  - SAF check is not required to get information about available cryptographic functions and hardware when calling the new IQF2 service.



ICSF HCR77A1 Migration Checks

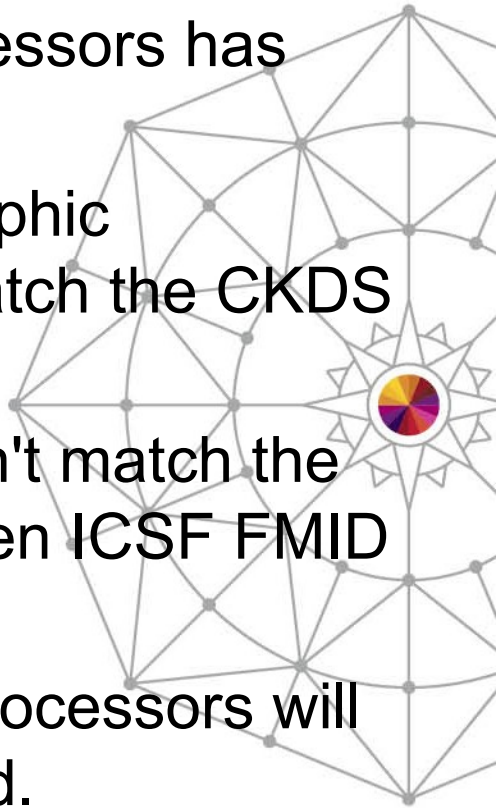
- The following new migration checks are for users of ICSF FMIDs HCR77A0 and earlier releases who are migrating to FMID HCR77A1 or newer releases of ICSF (APAR OA42011).

  - ICSFMIG77A1_COPROCESSOR_ACTIVE
  - ICSFMIG77A1_UNSUPPORTED_HW
  - ICSFMIG77A1_TKDS_OBJECT



ICSFMIG77A1_COPROCESSOR_ACTIVE

- The activation of CCA cryptographic coprocessors has changed for HCR77A1 and newer.
- This migration check detects CCA cryptographic coprocessors with master keys that don't match the CKDS and PKDS.
- A coprocessor that has master keys that don't match the CKDS and PKDS will not become active when ICSF FMID HCR77A1 is started.
- This migration check will indicate which coprocessors will not become active when HCR77A1 is started.



ICSFMIG77A1_UNSUPPORTED_HW

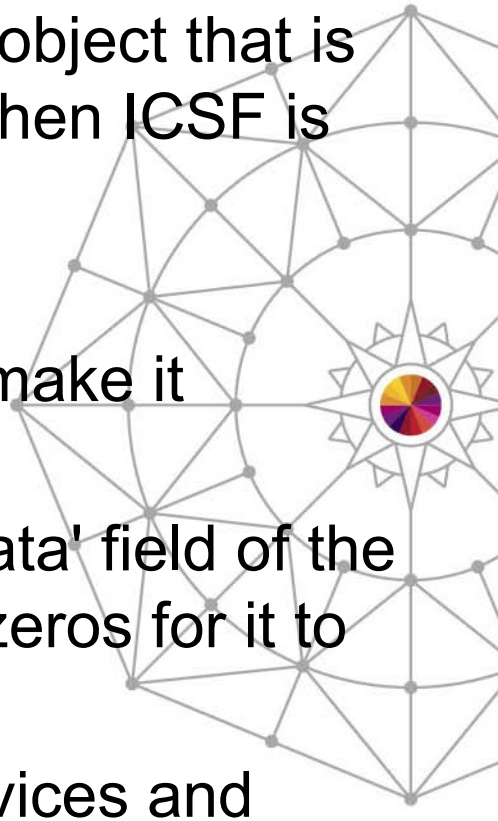
- The HCR77A1 release does not support IBM Eserver zSeries 800 and 900 systems.
- This migration check will indicate if your system is supported or not by HCR77A1 and newer releases.
- Available via APAR OA42011 back to HCR7770.

ICSFMIG77A1_TKDS_OBJECT

- In the HCR77A1 release, ICSF introduced a common key data set record format for CCA key tokens and PKCS #11 tokens and objects. This new format adds new fields for key utilization and metadata. Because of the size of the new fields, some existing PKCS #11 objects in the TKDS may cause ICSF to fail to start.
- The problem exists for TKDS object records with large objects. The 'User data' field in the existing record can not be stored in the new record format if the object size is greater that 32,520 bytes. The TKDSREC_LEN field in the record has the size of the object. If the 'User data' field is not empty and the size of the object is greater than 32,520 bytes, the TKDS can not be loaded.

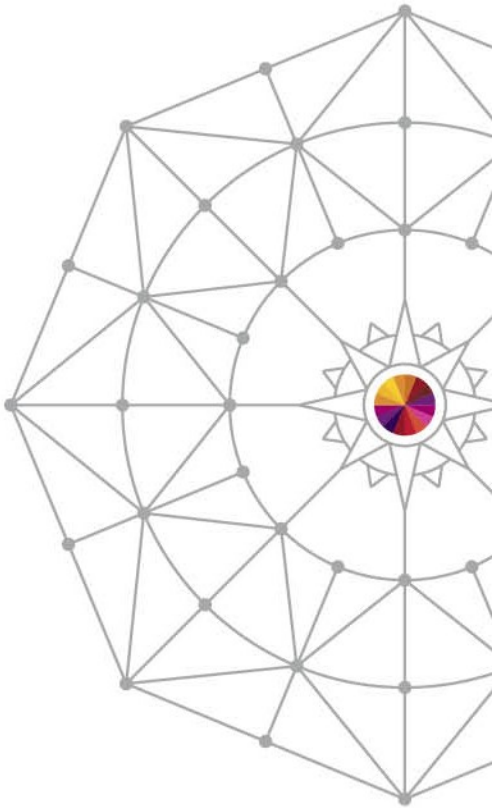
ICSFMIG77A1_TKDS_OBJECT

- This migration check will detect any TKDS object that is too large to allow the TKDS to be loaded when ICSF is started.
- The problem can be corrected by:
  - Modifying the attributes of the object to make it smaller, if possible.
  - Removing the information in the 'User data' field of the object. The 'User data' field must be all zeros for it to be ignored.
  - Copying the object using PKCS #11 services and deleting the old object.
  - Deleting the object.



DK AES PIN Support (HCR77A0 and above)

- Problem / Need
  - Existing PIN system uses TDES keys.
  - There's a need for an AES based PIN system.

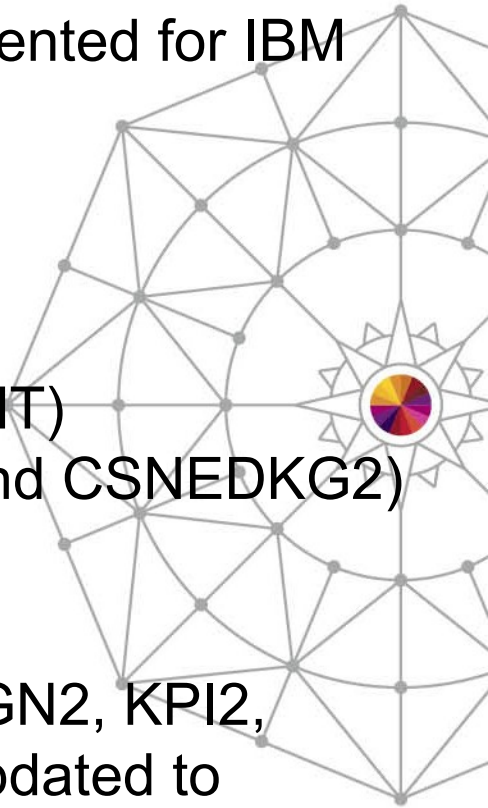


DK AES PIN Support (HCR77A0 and above)

- Solution
  - **Phase 1** of this solution was delivered in 4Q2013 via **HCR77A0 (WD #12)** and **HCR77A1 (WD #13) SPEs** (APAR OA42246). All DK AES PIN services and required key management service updates were implemented for IBM System x. Only a required subset of this support was implemented for IBM System z.
  - These financial services are based on the PIN methods of and meet the requirements specified by the German Banking Industry Committee, Die Deutsche Kreditwirtschaft, also known as DK. The intellectual property rights regarding the methods and specification belongs to the German Banking Industry Committee.

DK AES PIN Support (HCR77A0 and above)

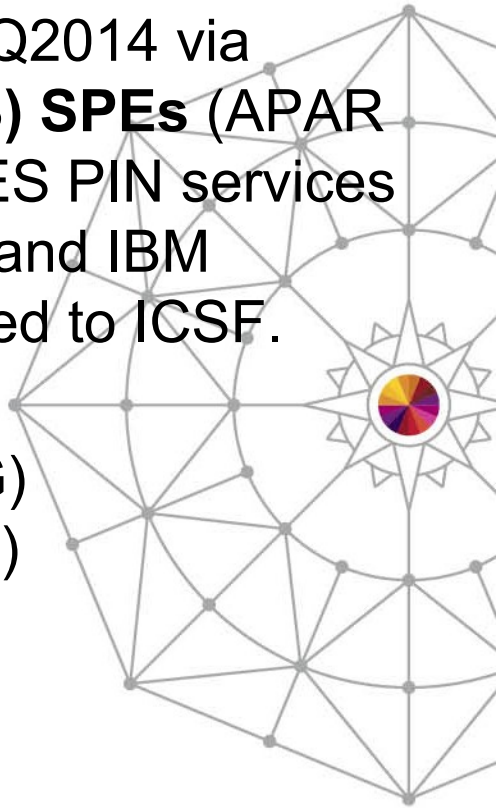
- The following subset of services were implemented for IBM System z in phase 1:
  - DK PIN Verify (CSNBDPV)
  - DK PIN Change (CSNBDPC)
  - DK PAN Modify in Transaction (CSNBDPMT)
  - Diversified Key Generate2 (CSNBDKG2 and CSNEDKG2)
  - DK Random PIN Generate (CSNBDRPG)
- Existing key management services (KTB2, KGN2, KPI2, SKI2, SYI2, SYX, KYT2, KTR2, RKA) were updated to support the new AES key types (DKYGENKY, MAC, PINCALC, PINPROT, and PINPRW).



DK AES PIN Support (HCR77A0 and above)

- **Phase 2** of this solution will be delivered in 1Q2014 via **HCR77A0 (WD #12)** and **HCR77A1 (WD #13) SPEs** (APAR OA43906). ICSF will add all remaining DK AES PIN services to provide full support on both IBM System x and IBM System z. The following services will be added to ICSF.

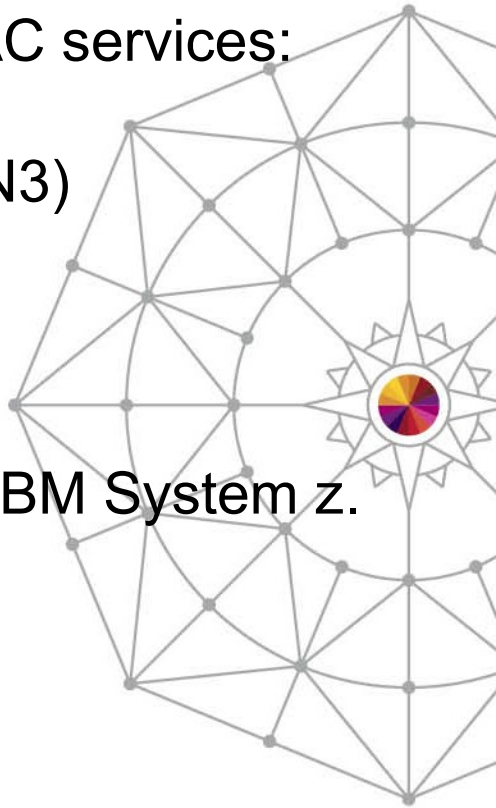
  - DK Deterministic PIN Generate (CSNBDDPG)
  - DK PRW Card Number Update (CSNBDPNU)
  - DK PAN Translate (CSNBDPT)
  - DK Regenerate PRW (CSNBDRP)
  - DK PRW CMAC Generate (CSNBDPCG)



DK AES PIN Support (HCR77A0 and above)

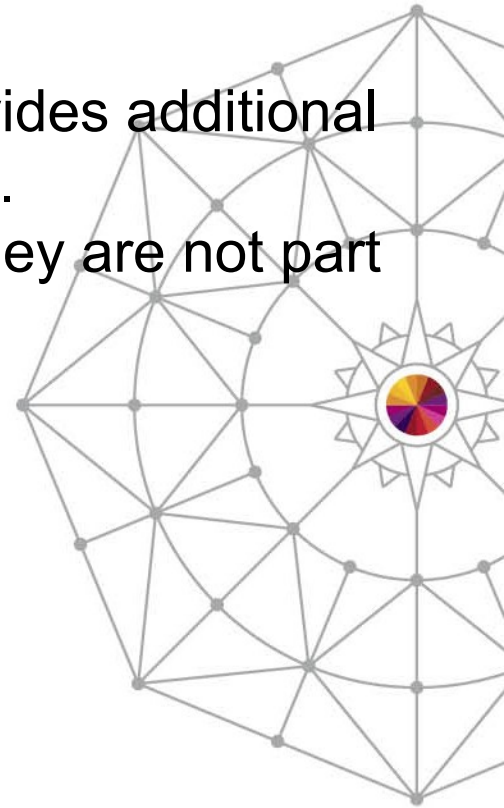
- Additionally, ICSF will support new AES-CMAC services:
  - MAC Generate2 (CSNBMGN2, CSNBMGN3)
  - MAC Verify2 (CSNBMVR2, CSNBMVR3)

- Benefits
  - New AES PIN System for IBM System x and IBM System z.



PKT UDX Support (HCR7790 and above)

- **Problem / Need**
  - The PKT User Defined Extension (UDX) provides additional formats for wrapping external RSA CRT keys.
  - UDXes are expensive to maintain because they are not part of the CCA base.

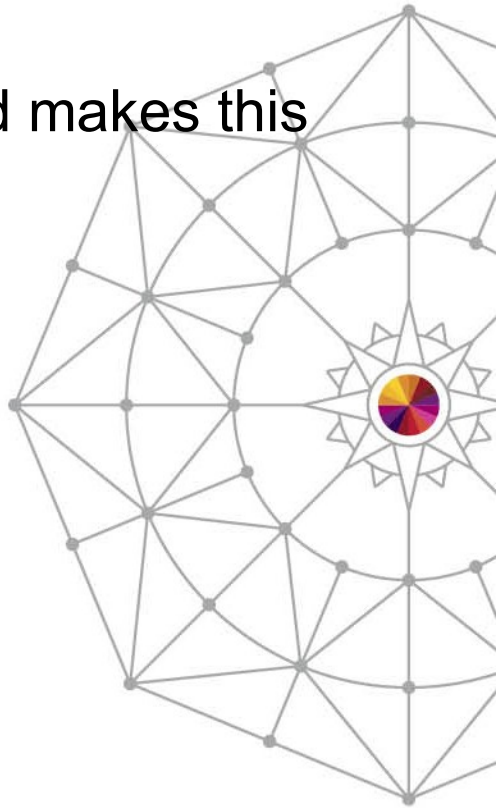


PKT UDX Support (HCR7790 and above)

- **Solution**
  - Integrate this UDX into the CCA base by adding 3 new rule array keywords to the ICSF PKA Key Translate, CSNDPKT, callable service (APAR OA43816).
  - The 3 new rule array keywords translate an external RSA CRT token to 3 new external formats:
    - EMVDDA - This keyword indicates translating an external RSA CRT key into EMV DDA format.
    - EMVDDAE - This keyword indicates translating an external RSA CRT key into EMV DDAE format.
    - EMVCRT - This keyword indicates translating an external RSA CRT key into EMV CRT format.

PKT UDX Support (HCR7790 and above)

- **Benefits**
  - UDX reduction relieves maintenance cost and makes this function generally available to all customers.



Toleration APAR OA42014

- ICSF releases HCR7790 and HCR77A0 require toleration support to avoid attempting to use DESUSECV keys.
- ICSF releases HCR7790 and HCR77A0 require toleration support to avoid attempting to use variable-length symmetric key tokens with fixed-length payloads or to share a CKDS with variable-length symmetric key tokens with fixed-length payloads.
- ICSF releases HCR7790 and HCR77A0 require toleration support to avoid attempting to re-encipher a CKDS with variable-length symmetric key tokens with fixed-length payloads.
- Releases of ICSF prior to HCR77A1 require coexistence support to recognize a KDS is in KDSR format and fail ICSF startup.
- Releases of ICSF prior to HCR77A1 require coexistence support to prevent re-encipherment and refreshing of KDSs in KDSR format.

Toleration APAR OA42014

- Releases of ICSF prior to HCR77A1 require coexistence support to allow the use of TKE interface CSFPCI to set the RSA master key in preparation for disaster recovery.
- This APAR will NOT allow any of the following:
  - key management or usage of variable-length symmetric key tokens that have fixed-length payloads. These key tokens can only be read from the CKDS.
  - key management or usage of DESUSECV key tokens
  - a CKDS with variable-length symmetric key tokens that have fixed-length payloads to be re-enciphered
  - ICSF to start with KDS that is in KDSR format
  - re-encipherment or refreshing of a KDS in KDSR format

Reference

- SA22-7520 ICSF Systems Programmer's Guide
- SA22-7521 ICSF Administration Guide
- SA22-7522 ICSF Application Programmer's Guide