Swiss Re

CF Encryption & SMF Record-signing

99. GSE – Vitznau, Oktober 2024 – Marco Egli

Table of Contents

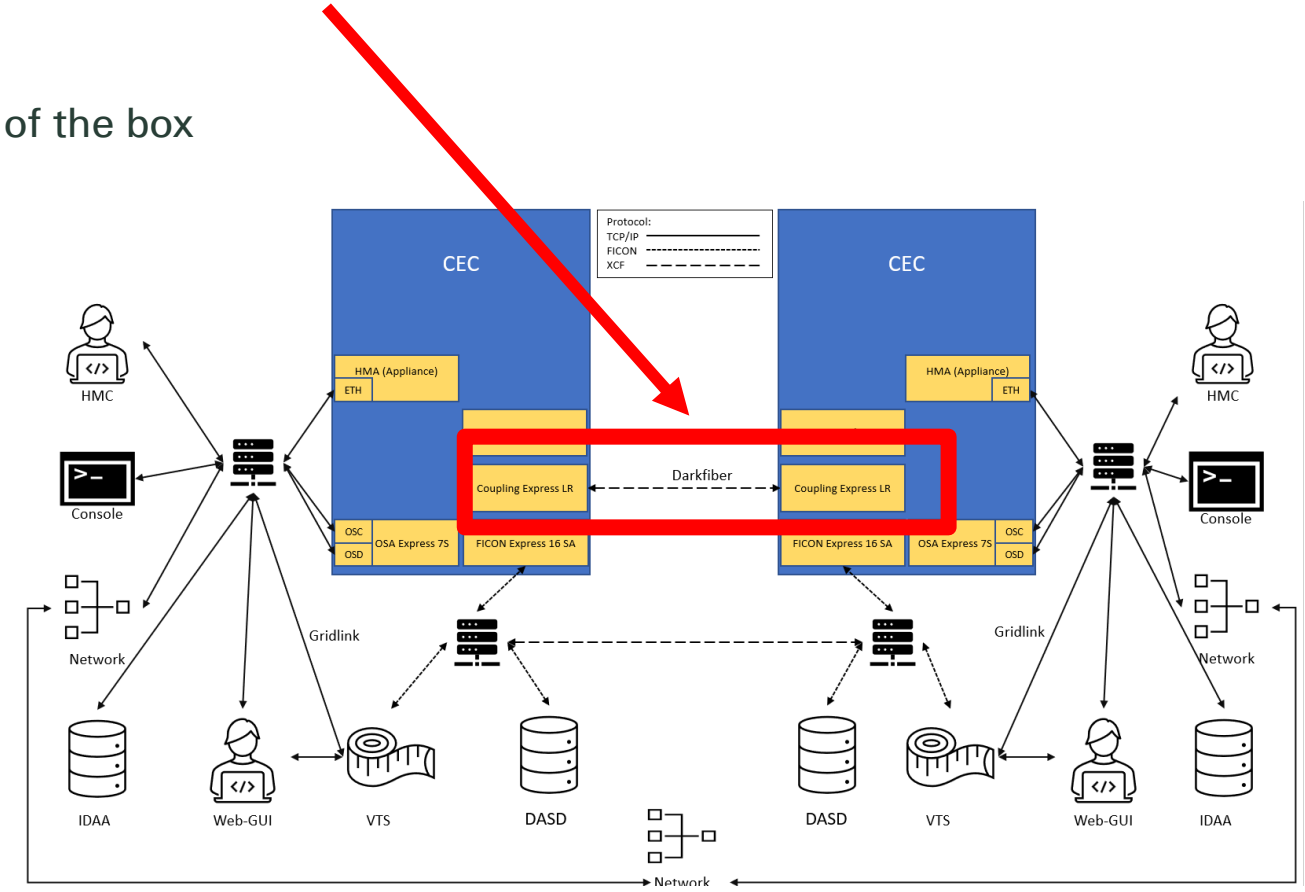
Swiss Re

Coupling Facility Structure Encryption

- Why?
- How?
- Operate it
- What?

Why should I encrypt my Coupling Facility Structure?

- Coupling Facility links (CF links) cannot be encrypted
  - The protocol used to transfer data between the CF is XCF which does not support encryption out of the box
  - Data transferred through CF links is plaintext
- Other cross connections do support encryption out of the box
- Simple to implement at no extra cost
- Part of pervasive encryption concept
  - Part of the pervasive encryption endeavour
- Quantum safe symmetric encryption
  - AES-256 in-memory
- Holistic encryption
  - Data in flight (on the CF links)
  - Data at rest (in the CF structure itself)



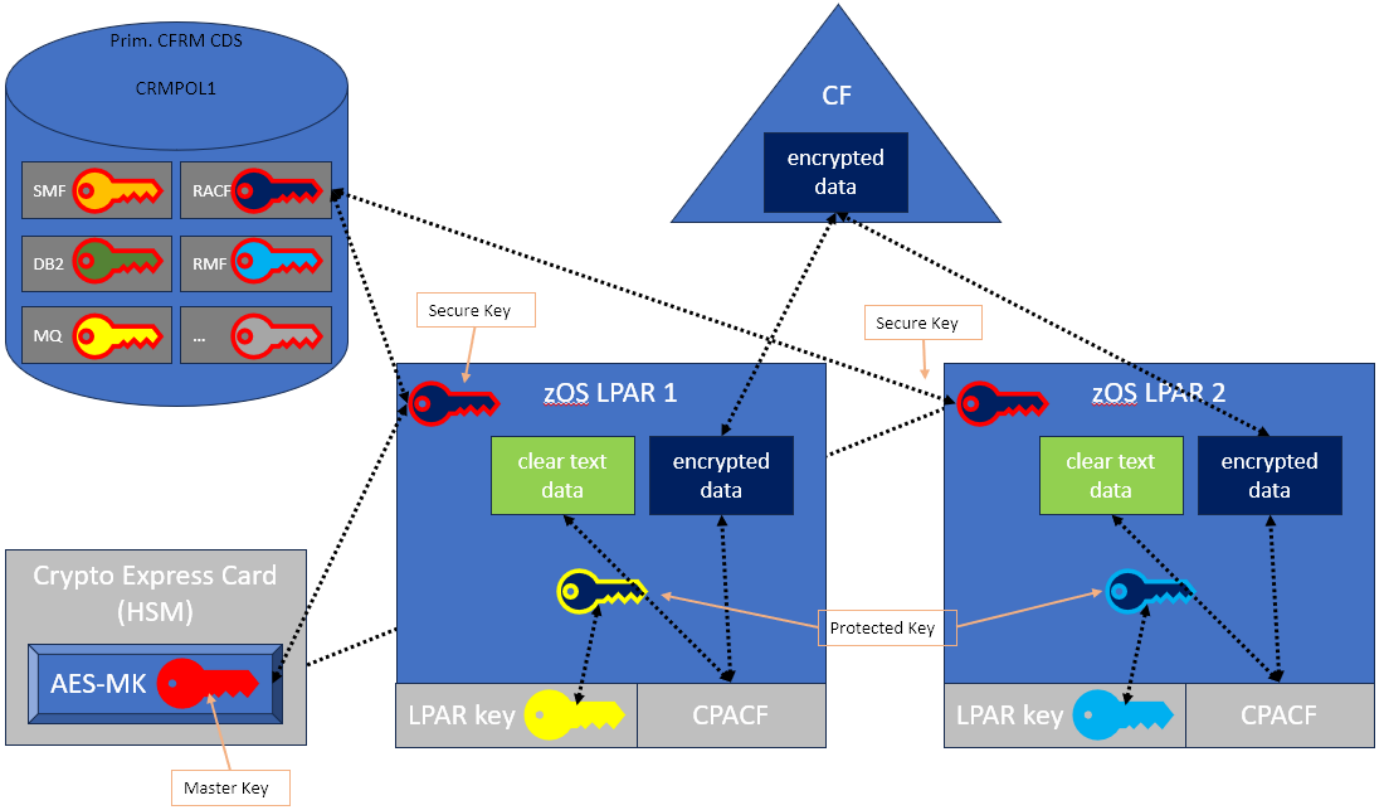
How do I encrypt my Coupling Facility Structure?

- Controlled with Coupling Facility Resource Management (CFRM) Policy Keyword `ENCRYPT(NO|YES)`
- CFRM does the key management and relies on ICSF
  - CFRM Couple dataset is used to store the keys to en-/decrypt the structure (not the CKDS!)
- Changes to encryption state of an allocated structure occur dynamically through structure rebuild processing
  - `SETXCF START,REBUILD,DUPLEX,STRNAME=<strname>,KEEP=OLD` (if structure is defined as `DUPLEX(ENABLED)`)
  - `SETXCF START,REBUILD,STRNAME=<strname>`

- Requirements (more later)
  - ICSF and at least AES master key must be set and **equal** in all systems sharing the CFRM CDS
  - At least zOS V2R3 with a z14
  - Authorization for selected RACF CL(CSFSERV) profiles

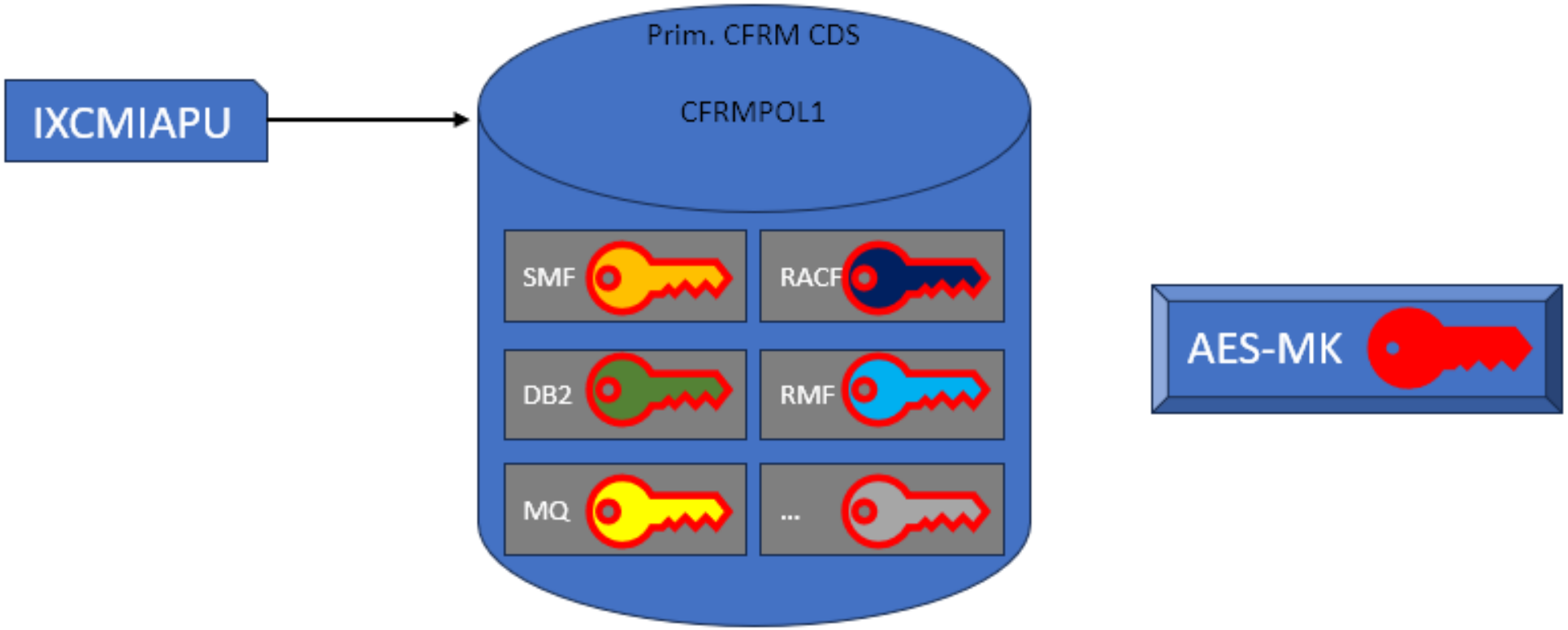
How do I encrypt my Coupling Facility Structure? → Big picture

- Each structure key exists as a protected key in the LPAR to perform the crypto operations
- Fully transparent to consumers of the structure



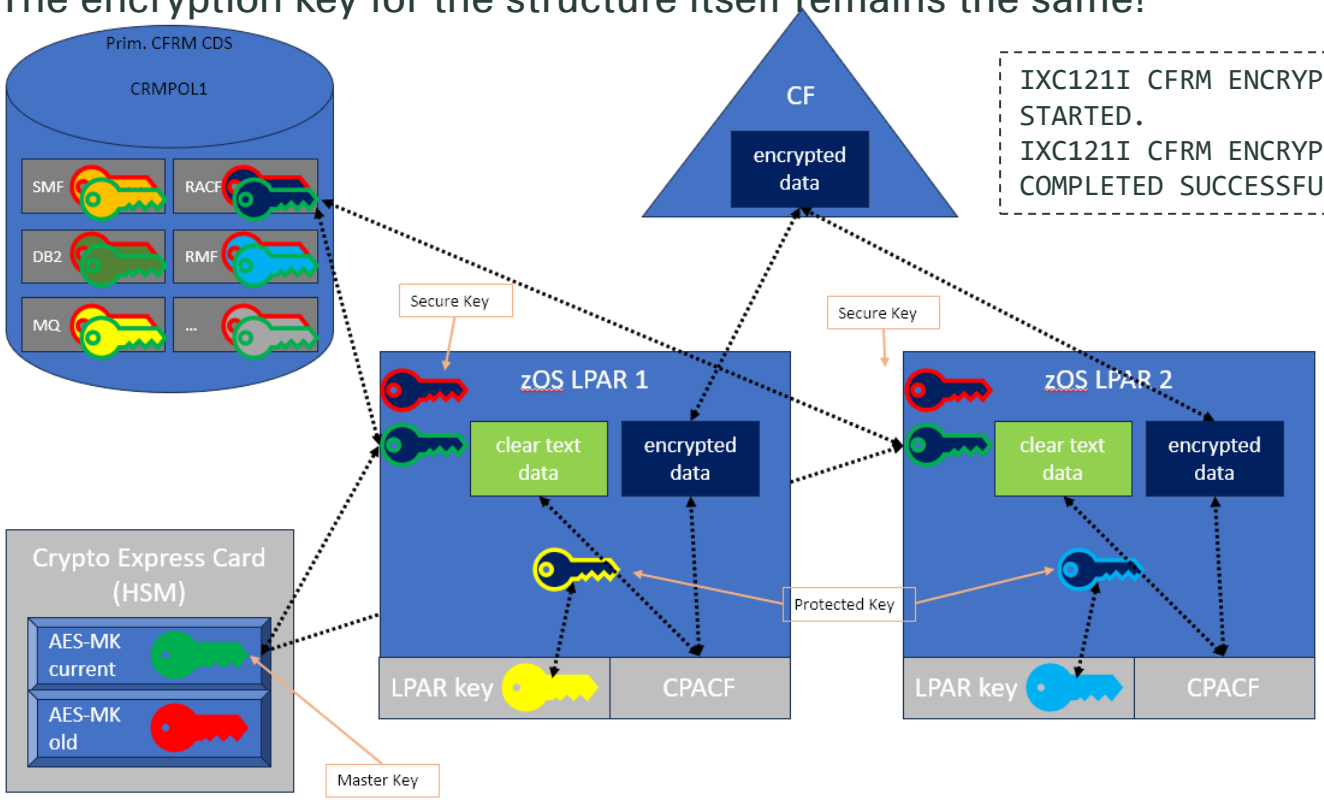
How do I encrypt my Coupling Facility Structure? → Key Storage

- Each structure has its own key that is stored in the CFRM CDS and encrypted by the systems AES master key
- Depending on the amount of different CFRM policies (in CDS) multiple copies of the same key exist



How do I encrypt my Coupling Facility Structure? → AES master key change

- When the AES master key changes, all CF structure keys in the CFRM CDS will be re-encrypted.
  →No need to re-encrypt the structure data itself, only the protected key needs to be rewrapped.
- The encryption key for the structure itself remains the same!




```
IXC121I CFRM ENCRYPT CHANGE-MK PROGRESS: CHANGE MASTER KEY PROCESSING
STARTED.
IXC121I CFRM ENCRYPT CHANGE-MK PROGRESS: CHANGE MASTER KEY PROCESSING
COMPLETED SUCCESSFULLY.
```

How do I encrypt my Coupling Facility Structure? → Implementation - Define

- Add parameter `ENCRYPT(YES)` to a structure in the CFRM Policy and write it to CDS with IXCMIAPU. Run it with `REPORT(YES)` to get the key details reported.

```
//STEP1   EXEC PGM=IXCMIAPU
//SYSPRINT DD  SYSOUT=*
//SYSIN    DD  *
     DATA TYPE(CFRM) REPORT(YES)
     DEFINE POLICY NAME(CFRMPOL1) REPLACE(YES)
     CF   NAME(CF1)       TYPE(008561)
          MFG(IBM)        PLANT(02)
          SEQUENCE(<serial1>)
          PARTITION(1F)    SITE(SITE1)
          CPCID(00)       DUMPSPACE(4096M)
     CF   NAME(CF2)       TYPE(008561)
          MFG(IBM)        PLANT(02)
          SEQUENCE(<serial2>)
          PARTITION(1F)    SITE(SITE2)
          CPCID(00)       DUMPSPACE(4096M)
     STRUCTURE NAME(OPERLOG) INITSIZE(512M) SIZE(768M)
               MINSIZE(512M)
               DUPLEX(ENABLED)
               FULLTHRESHOLD(90)
               ALLOWAUTOALT(YES)
               PREFLIST(CF1,CF2)
               ENCRYPT(YES)
/*
```

IXCMIAPU output

```
IXC748I CRYPTOGRAPHIC KEY TOKENS ENCIPHERED UNDER THE CURRENT
  MASTER KEY FOR STRUCTURES SPECIFYING DATA ENCRYPTION

STRUCTURE NAME(OPERLOG) SIZE(768M)
   INITSIZE(512M)
   MINSIZE(512M)
   FULLTHRESHOLD(90)
   ALLOWAUTOALT(YES)
   DUPLEX(ENABLED)
   PREFLIST(CF1,CF2)
   ENCRYPT(YES)  /* Key Generated: 03/28/2025 11:47:46.672941 */
```

*only an extract of the policy is shown for better readability

How do I encrypt my Coupling Facility Structure? → Implementation - Activate

- Activate the CFRM Policy that has been written by IXCMIAPU in 'Define' Step
  - `SETXCF START,POLICY,TYPE=CFRM,POLNAME=<polname>`
    `→ IXC511I START ADMINISTRATIVE POLICY <polname> FOR CFRM ACCEPTED`
  - Leads to pending policy changes
    `→IXC512I POLICY CHANGE IN PROGRESS FOR CFRM 405`
    `TO MAKE <polname> POLICY ACTIVE.`
    `xx POLICY CHANGE(S) PENDING.`
- Rebuild the structure to encrypt it
  - If structure is DUPLEX(ENABLED)
    - `SETXCF STOP,REBUILD,DUPLEX,STRNAME=<strname>,KEEP=OLD`
    - `SETXCF START,REBUILD,STRNAME=<strname>`
  - If structure is DUPLEX(DISABLED)
    - `SETXCF START,REBUILD,STRNAME=<strname>`
- Verify the Policy is active – ALL rebuild activities must be completed
  `→ IXC513I COMPLETED POLICY CHANGE FOR CFRM. 593`
  `<polname> POLICY IS ACTIVE.`

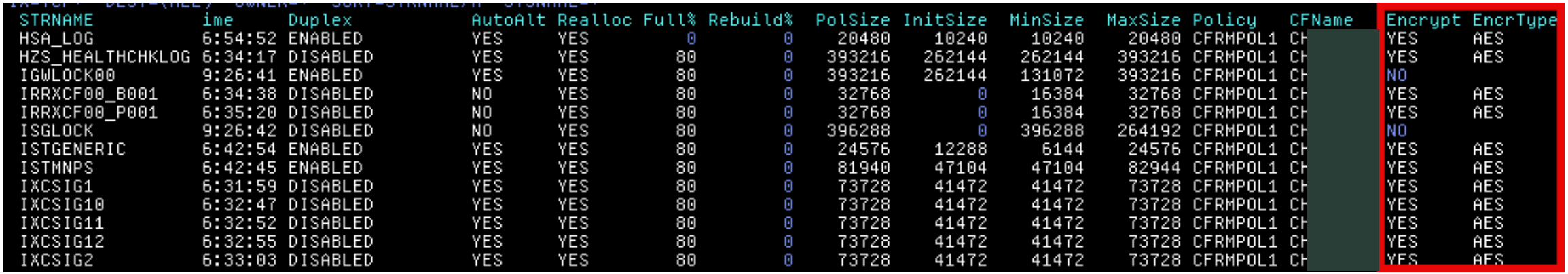
How do I encrypt my Coupling Facility Structure? → Implementation - Verify

- Various places to check the encryption status
- System Command: `D XCF,STR,STRNAME=OPERLOG`

```
IXC360I  14.33.41  DISPLAY XCF 427
STRNAME: OPERLOG
 STATUS: REASON SPECIFIED WITH REBUILD START:
           POLICY-INITIATED
         DUPLEXING REBUILD
           METHOD: SYSTEM-MANAGED
             AUTO VERSION: DF54C89D 3A99BA58
           PHASE: DUPLEX ESTABLISHED
[--content intentionally removed--]
  ENFORCEORDER    : NO
  EXCLUSION LIST IS EMPTY
  ENCRYPT         : YES
```

How do I encrypt my Coupling Facility Structure? → Implementation - Verify

- Various places to check the encryption status
- SDSF – 'CFS' panel

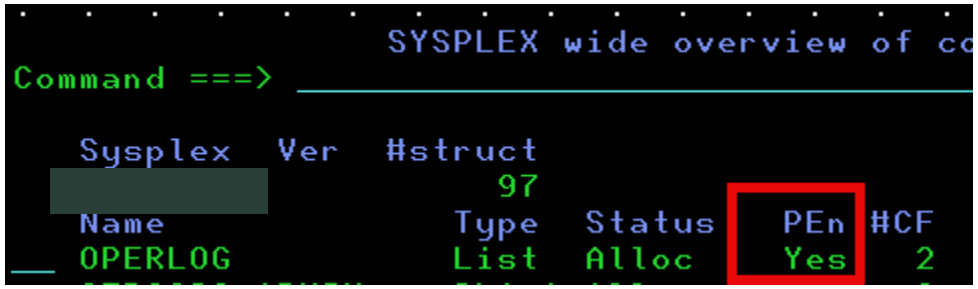


STRNAME	ime	Duplex	AutoAlt	Realloc	Full%	Rebuild%	PolSize	InitSize	MinSize	MaxSize	Policy	CFName	Encrypt	EncrType
HSA_LOG	6:54:52	ENABLED	YES	YES	0	0	20480	10240	10240	20480	CFRMPOL1	CF	YES	AES
HZS_HEALTHCHKLOG	6:34:17	DISABLED	YES	YES	80	0	393216	262144	262144	393216	CFRMPOL1	CF	YES	AES
IGWLOCK00	9:26:41	ENABLED	YES	YES	80	0	393216	262144	131072	393216	CFRMPOL1	CF	NO	
IRRXCF00_B001	6:34:38	DISABLED	NO	YES	80	0	32768	0	16384	32768	CFRMPOL1	CF	YES	AES
IRRXCF00_P001	6:35:20	DISABLED	NO	YES	80	0	32768	0	16384	32768	CFRMPOL1	CF	YES	AES
ISGLOCK	9:26:42	DISABLED	NO	YES	80	0	396288	0	396288	264192	CFRMPOL1	CF	NO	
ISTGENERIC	6:42:54	ENABLED	YES	YES	80	0	24576	12288	6144	24576	CFRMPOL1	CF	YES	AES
ISTMNPS	6:42:45	ENABLED	YES	YES	80	0	81940	47104	47104	82944	CFRMPOL1	CF	YES	AES
IXCSIG1	6:31:59	DISABLED	YES	YES	80	0	73728	41472	41472	73728	CFRMPOL1	CF	YES	AES
IXCSIG10	6:32:47	DISABLED	YES	YES	80	0	73728	41472	41472	73728	CFRMPOL1	CF	YES	AES
IXCSIG11	6:32:52	DISABLED	YES	YES	80	0	73728	41472	41472	73728	CFRMPOL1	CF	YES	AES
IXCSIG12	6:32:55	DISABLED	YES	YES	80	0	73728	41472	41472	73728	CFRMPOL1	CF	YES	AES
IXCSIG2	6:33:03	DISABLED	YES	YES	80	0	73728	41472	41472	73728	CFRMPOL1	CF	YES	AES

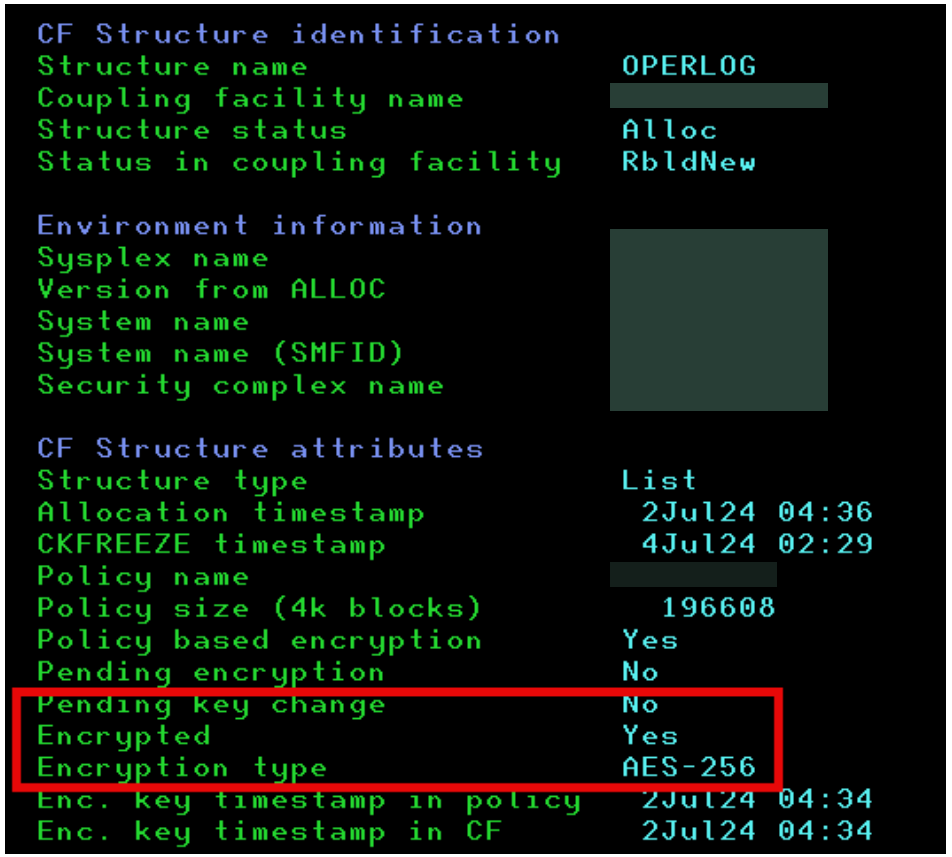
- Idea ZOS-I-4156 was rejected to add N/A into Encrypt column for not eligible structures (LOCK)

How do I encrypt my Coupling Facility Structure? → Implementation - Verify

- Various places to check the encryption status
- zSecure – Sysplex overview



- zSecure – RE.K.C panel (Resources, Keys, Coupling)



How do I operate encrypted structures? → Status check

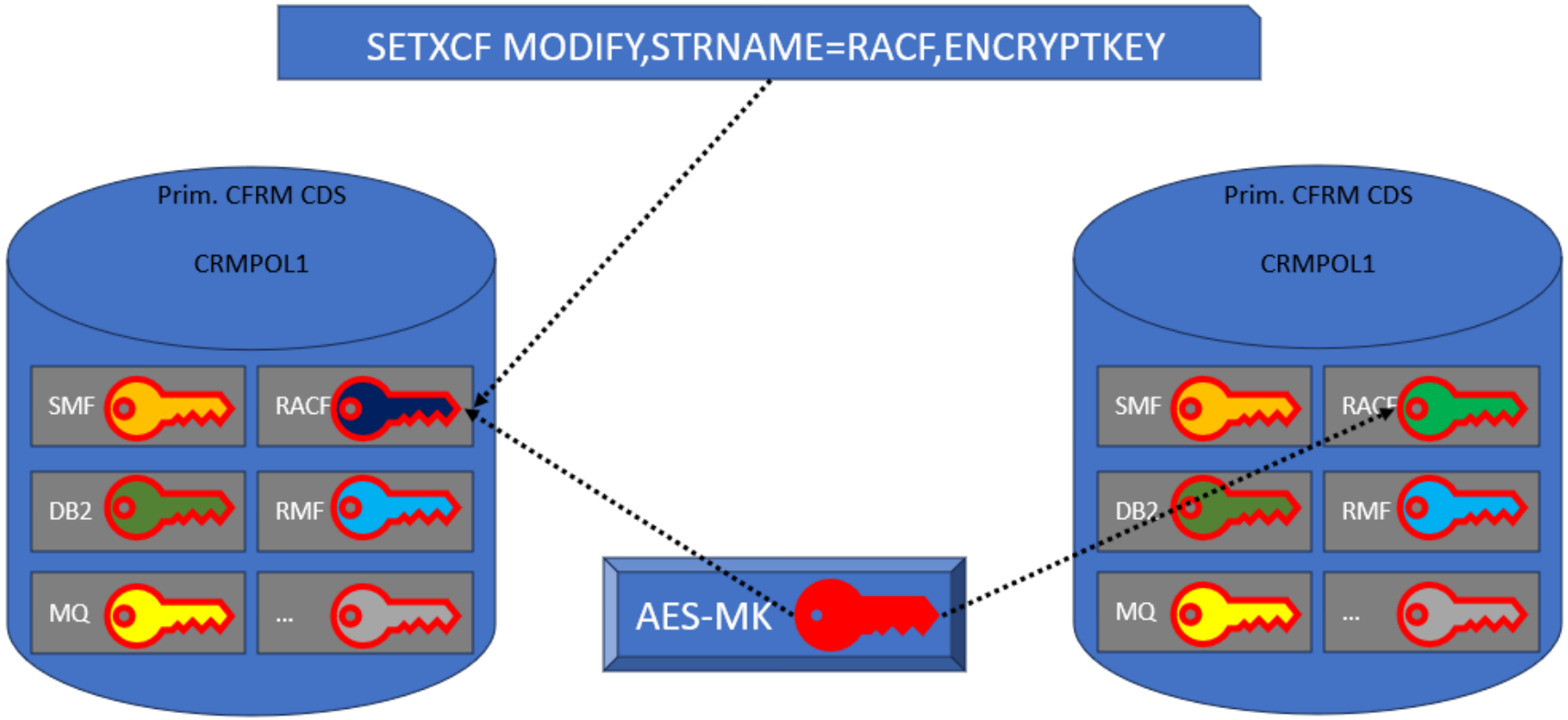
- List the structures that are encrypted
  - `D XCF,STR,STRNAME=<strname>,STATUS=ENCRYPTED`
- List the structures that are not encrypted
  - `D XCF,STR,STRNAM=<strname>,STATUS=NOTENCRYPTED`
- List the structures whose encryption state does not match the ENCRYPT specification in the active CFRM policy
  - `D XCF,STR,STRNAM=<strname>,STATUS=ENCMISMATCH`

Remark:

Similar views are available in SDSF ‘CFS’ panel or in Netview ‘INGCF’ panel

How do I operate encrypted structures? → Change Structure AES key

- CF structure keys do not change automatically but can be triggered manually



How do I operate encrypted structures? → Change Structure AES key

- Trigger an AES key change for a coupling structure
  - `SETXCF MODIFY,STRNAME=<strname>,ENCRYPTKEY`

```
→ IXC562I SETXCF COMMAND TO MODIFY THE ENCRYPTION KEY FOR STRUCTURE(S) IN CFRM POLICY ENCRYPT ACCEPTED
→ IXC512I POLICY CHANGE IN PROGRESS FORCFRM
     TO MAKE ENCRYPT POLICY ACTIVE.
     1 POLICY CHANGE(S) PENDING.
→ IXC121I CFRM ENCRYPT STATUS CHANGE: ADMINISTRATIVE DATA KEYS HAVE
     BEEN UPDATED.
→ IXC563I SETXCF COMMAND COMPLETED: ENCRYPTION KEY
     CHANGED IMMEDIATELY FOR 0 STRUCTURE(S),
     ENCRYPTION KEY CHANGE PENDING FOR 1 STRUCTURE(S)
```

- Resolve the pending action on the structure
  - If structure is DUPLEX(ENABLED)
    - `SETXCF STOP,REBUILD,DUPLEX,STRNAME=<strname>,KEEP=OLD`
    - `SETXCF START,REBUILD,STRNAME=<strname>`
  - If structure is DUPLEX(DISABLED)
    - `SETXCF START,REBUILD,STRNAME=<strname>`

What can I encrypt and how does it affect my performance?

- No noticeable CPACF consumption increase
- No measured delay in DB2 processing
  - Checking DB2 Accounting records have not shown differences in Jobs accessing either encrypted or unencrypted group buffer pool data
  - No measured or perceived performance decrease
- Structures form type CACHE, LIST and SERLIST can be encrypted
  - Data in ‘entries’ and ‘adjunct’ will be encrypted
- LOCK structures cannot be encrypted (those contain anyway no user data)
  - Controls and metadata are not encrypted

What to pay special attention to?

- A structure key can exist more than once, depending on the number of Policies in the CDS
- Structure key change does not trigger automatically a re-encipherment
  - Manual actions are required: `STOP REBUILD,DUPLEX [...]` and/or `START REBUILD [...]`
- The AES master key on the system where the job runs must be the same used by other systems in the Sysplex where the encrypted structures are used.
  - For example, if XCF signal structures are encrypted the same master AES key must as well be present in GDPS systems
- AES master key must be set before IPL
  - Load in XCF-Local mode (or monoplex to install the AES master key)
  - Load AES master key via TKE into the LPARs domain
- Copy the CDS to a DR-location or another Sysplex, the same AES master key must be available that was used when the IXCMIAPU utility created the keys
  - Ensure that the master key used to wrap the encryption keys in the CDS is the same as the one used by that new Sysplex

What do I need to exploit this fancy stuff?

- AES master key in CCA co-processor
- CPACF must be available
- z14 or newer
- zOS 2.3 or newer
- RACF authorizations to ICSF services or TRUSTED
- IXCMIAPU job submitter with appropriate access to CL(CSFSERV) CSFKGN and CSFKYT profiles
- APAR OA51879 for the metrics (SMF 74(4)).
- APAR OA52003 for RMF support
- APAR OA52060 for zOS toleration

References

- IBM Documentation – Encrypting coupling facility structure data
  - https://www.ibm.com/docs/en/zos/3.1.0?topic=resources-encrypting-coupling-facility-structure-data
- GSE UK Virtual Conference 2021 (no direct link found but the one via google works)
  - https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjJhMbdscyIAxVUxAIHHTT5CWEQFnoECBwQAQ&url=https%3A%2F%2Fconferences.gse.org.uk%2F2021%2Fpresentations%2F5BC.pdf&usg=AOvVaw3KLta6AW5o9LaFII_TXF93&opi=89978449
- IBM Z Security Conference (video) - Pervasive encryption in z_OS_ CF structures and log streams
  - https://mediacenter.ibm.com/media/Pervasive+encryption+in+z_OS_+CF+structures+and+log+streams/1_2xdzlewq

Swiss Re

SMF Record Signing

- Why?
- How?
- Operate it
- What?

Why should I sign my SMF Records?

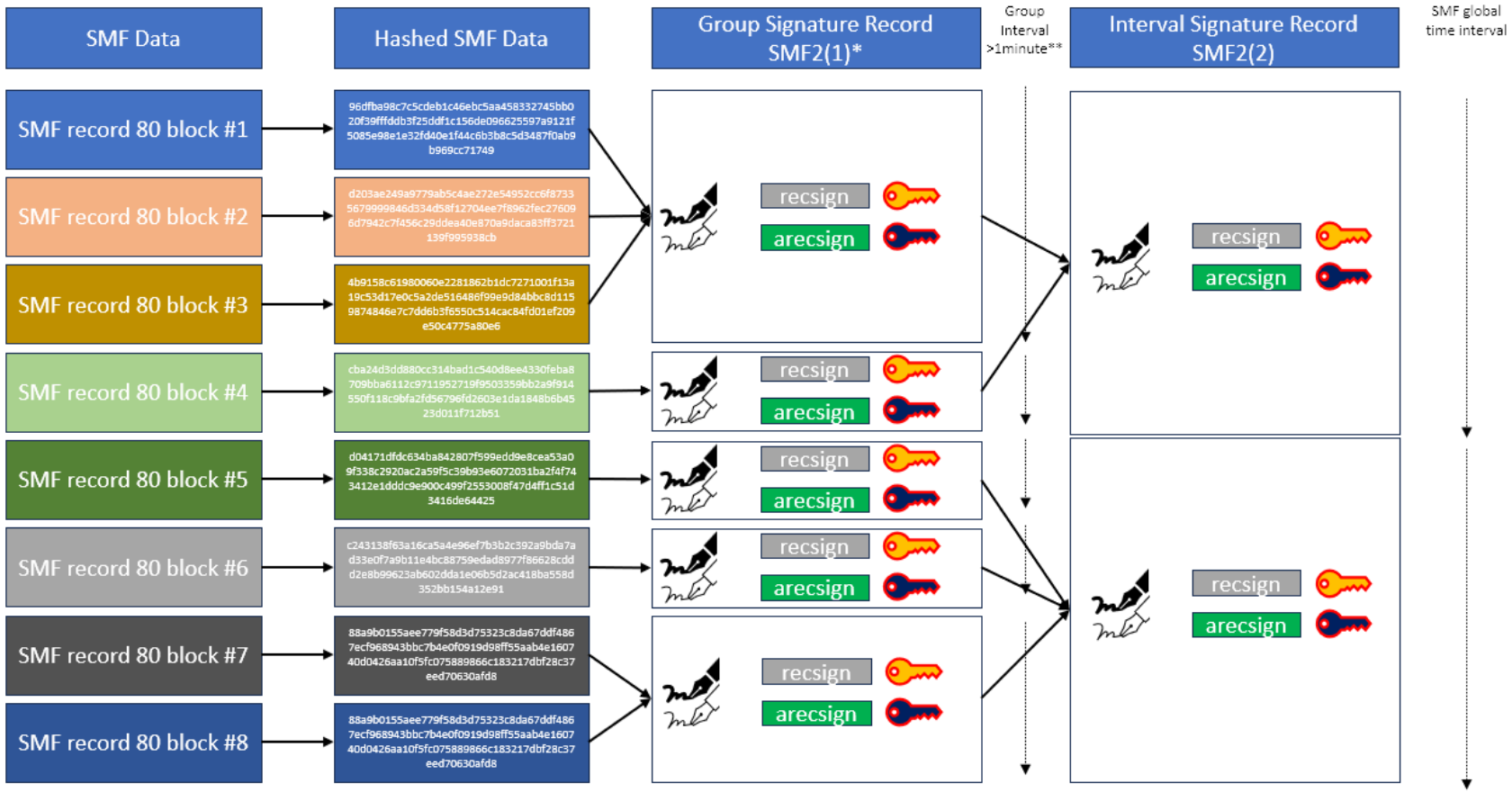
- Create Tamper Proof SMF Records
  - Useful to attest that created SMF records were not tampered with after creation
  - Potential manual interventions and updates will invalidate the records
- Simple to implement at no extra cost
- Audit proof verification
- Segregation of duties and taking control back from the zOS Admin to the Security Auditor for assurance

How do I sign my SMF Records?

- Create Public/Private Key Pair and store in TKDS
- Update `SMFPRMxx` Member with `RECSIGN` and `ARECSIGN` keyword and activate it (`SET SMF=xy`)
- Done
- Unfortunately, not that straight forward as CF encryption so let's have a look at it step by step

How do I sign my SMF Records? → Big picture

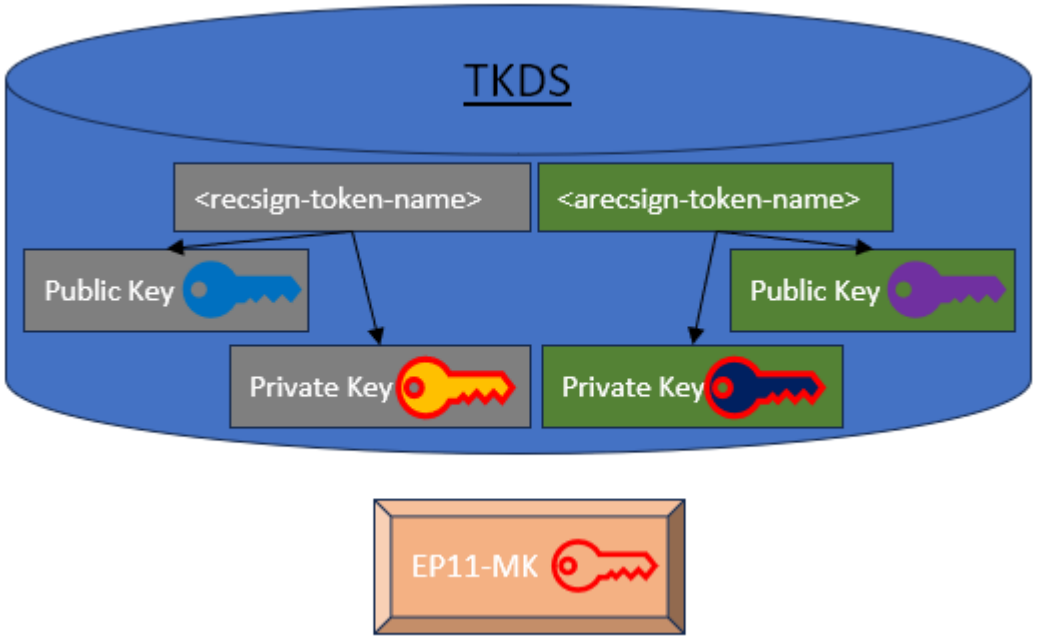
- SMF data is signed on its way to the System Logger



*It is only illustrative to outline that the group signatures are signed 'periodically'
**Periodically according the manual means that after 1minute the group is signed, but it waits for the records being written, hence it can even be 1minute and 2s but as a rule of thumb, it's 1minute a potentially few seconds

How do I sign my SMF Records? → Key Storage

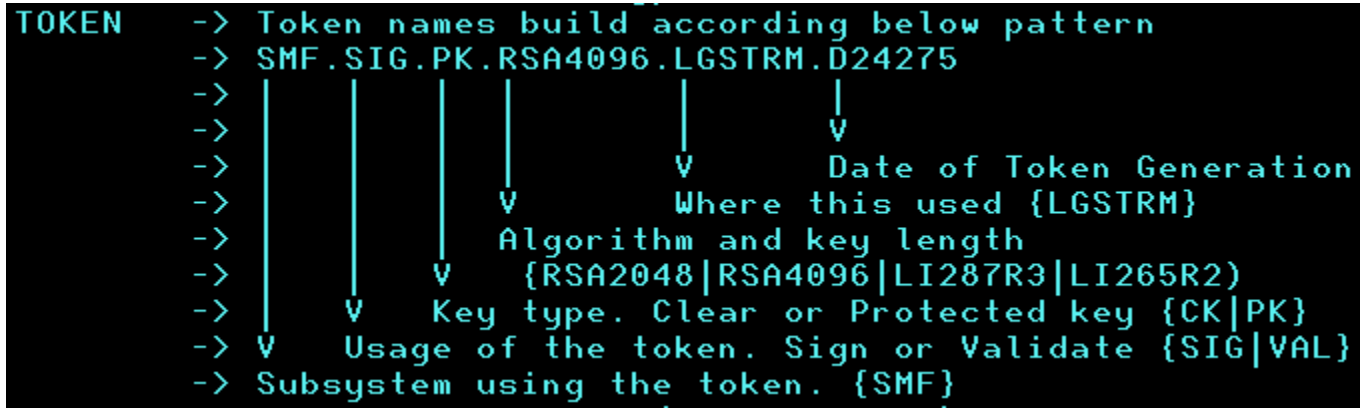
- Each Token has its own key pair stored in the TKDS and encrypted by the systems EP11 master key
- The Token is referenced in in the SMFPRMxx member not the key



How do I sign my SMF Records? → Implementation - Key and Token part 1

- Add the Token to the TKDS
- Generate RSA or ECC keypair for ‘classic’ algorithm
- Generate Dilithium-8-7 R3 or Dilithium-6-5 R2 key pair for ‘alternate’ algorithm
- Token must be exactly 32 characters
  - Consider good naming conventions that might include (to understand its usage in ICSF/zSecure Reports as there can be many other Tokens in the system):
    - Subsystem using the Token
    - Usage of the Token
    - Key type associated
    - Algorithm used
    - Where used
    - Date of Token (Key pair) issuance

    sample: `SMF.SIG.PK.RSA4096.LGSTRM.D24221`



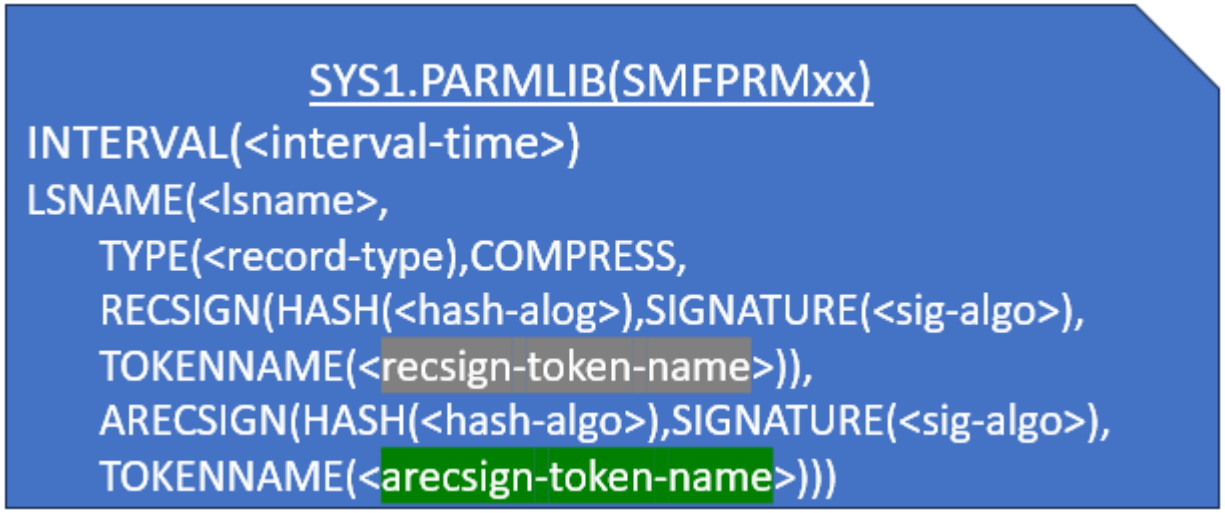
How do I sign my SMF Records? → Implementation - Key and Token part 2

- 4* JCLs to implement our setup with different REXXs calling ICSF services
  - Recommended to call REXX with IKJEFT1A to return REXX internal return codes back to the caller (Job)
  - Steer the Jobs with symbols
  - REXX to consume input values and call ICSF service CSFPGKP for RSA and LI2
  - Export the public key from the source (creating) system and import in a single system (production) for centralized validation
    - not yet possible – more at the end

**examples can be shared; it was not possible to include them here as they are too extensive for a presentation*

How do I sign my SMF Records? → Implementation - SMFPRMxx

- Add the RECSIGN and ARECSIGN parameters to the Logstreams designated for signing
  - `RECSIGN(HASH(<hash-algo>),SIGNATURE(<sig-algo>),TOKENNAME(<recsign-token-name>))`
  - `ARECSIGN(HASH(<hash-algo>),SIGNATURE(<sig-algo>),TOKENNAME(<arecsign-token-name>))`



How do I sign my SMF Records? → Implementation - Activate

- Activate the updated SMFPRMxx member dynamically
  - SET SMF=xx

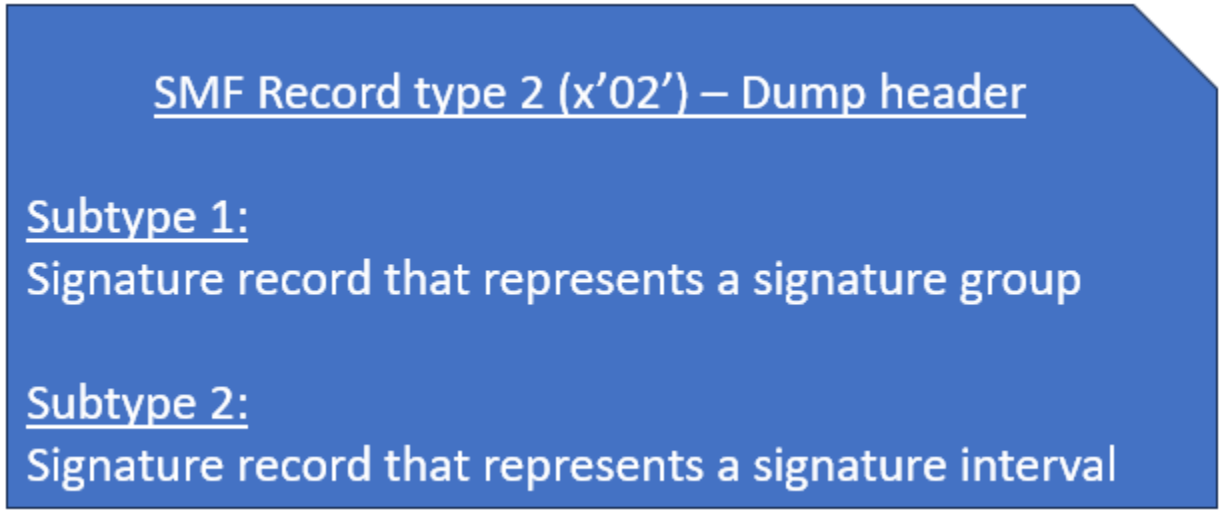
```
IEE252I MEMBER SMFPRMxx FOUND IN SYS1.PARMLIB
[removed IEF196I messages]
IFA711I LOGSTREAM PARAMETERS ARE IN EFFECT
IFA714I 14.55.57 SMF STATUS 633
          LOGSTREAM NAME                BUFFERS        STATUS
        A-IFASMF.<ls-name-aa>             796930        CONNECTED
        A-IFASMF.<ls-name-bb>            2810202        CONNECTED
        A-IFASMF.<ls-name-cc>            6985134        CONNECTED
        A-IFASMF.<ls-name-dd>                  0        CONNECTED
        A-IFASMF.<ls-name-ee>           31975945        CONNECTED
        A-IFASMF.<ls-name-ff>                  0        CONNECTED
        A-IFASMF.INMEM               1986903399        IN-MEMORY
IEE536I SMF      VALUE xx NOW IN EFFECT
```

How do I sign my SMF Records? → Implementation - Verify

- Display SMF options to verify if the expected changes are in effect
  -
```
D SMF,O
IEE967I 15.03.43 SMF PARAMETERS 813
[--data left intentionally--]
LSNAME(IFASMF.<ls-name-aa>,ARECSIGN(HASH(SHA512),
TOKENNAME(<arecsign-token-name>),SIGNATURE(LI2)),
RECSIGN(HASH(SHA512),
TOKENNAME(<recsign-token-name>),SIGNATURE(RSA)),
COMPRESS,TYPE(1:11)) -- PARMLIB
LSNAME(IFASMF.<ls-name-bb>,ARECSIGN(HASH(SHA512),
TOKENNAME(<arecsign-token-name>),SIGNATURE(LI2)),
RECSIGN(HASH(SHA512),
TOKENNAME(<recsign-token-name>),SIGNATURE(RSA)),
COMPRESS,TYPE(12:24)) -- PARMLIB
```

How do I sign my SMF Records? → Where is it stored?

- Digital Signatures are stored in SMF type 2 record (which is the dump header)
  - Subtype 1 stores grouped signature
  - Subtype 2 stores interval-based signature
  - New data included in these records includes counts of records included, start and end times of the data included and the hashing and signature methods.

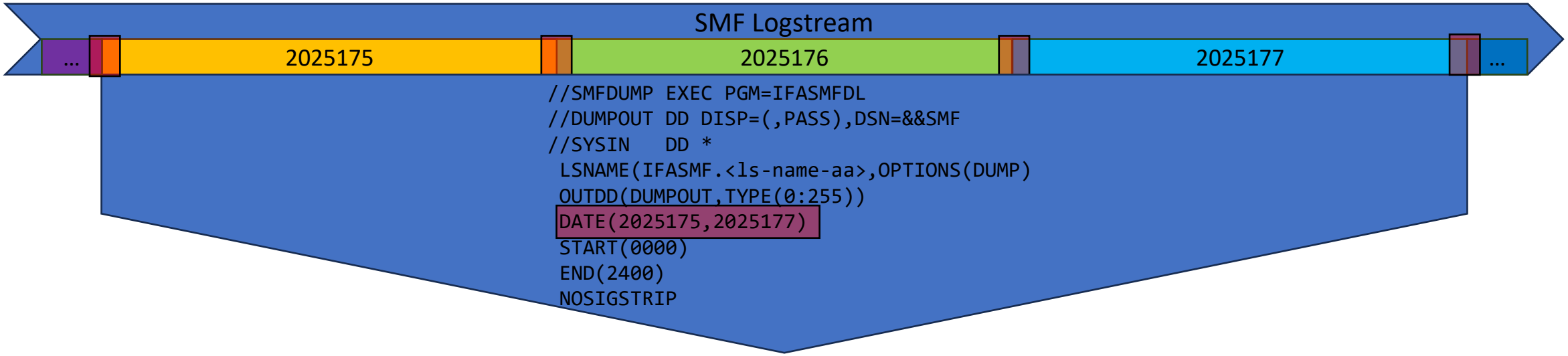


Data included in these records includes counts of records included, start and end times of the data, the hashing and signature methods

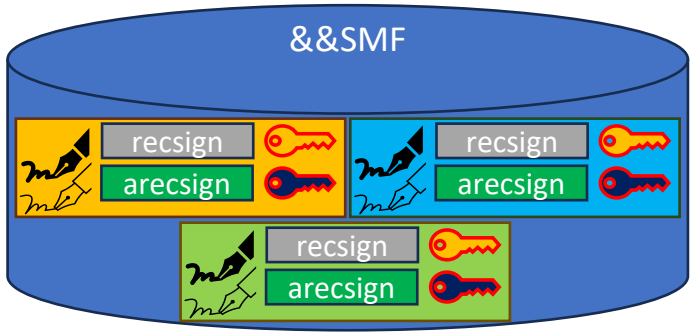
How do I operate SMF signing? → New Token and Key Pair

- Add new Token
- Generate new Key pair
- Update `SMFPRMxx` with new token
- Activate `SMFPRMxx` with `SET SMF=xx`
- Verify with `D SMF,O`
- Validate data afterwards with SMF dump process and `SIGNVALIDATE|ASIGNVALIDATE`

How do I operate SMF signing? → Signature Verification




```
//SMFVALID EXEC PGM=IFASMFDP
//DUMPIN   DD DISP=OLD,DSN=&&SMF
//DUMPUT   DD DUMMY
//SYSIN DD *
INDD(DUMPIN,OPTIONS(DUMP))
OUTDD(DUMPUT,TYPE(0:255))
DATE(2025176,2025176)
START(0000)
END(2400)
SID(system-id)
SIGNVALIDATE(HASH(<hash-alog>),TOKENNAME(<recsign-token-name>))
ASIGNVALIDATE(HASH(<hash-alog>),TOKENNAME(<arecsign-token-name>))
```




```
 RECORD VALIDATION REPORT FOR <system-id>
RECORD   RECORD   VALIDATION      VALIDATION START       VALIDATION END       RECORDS        GROUPS     INTERVALS
  TYPE  SUBTYPE      FAILURE            DATE-TIME            DATE-TIME     VALIDATED     VALIDATED     VALIDATED
    80       *            N   06/25/2025-00:00:00  06/25/2025-23:59:59    20,940,410         1,444            96
    82      42            N   06/25/2025-00:00:00  06/25/2025-23:59:59     1,288,109         1,428            96
    82      46            N   06/25/2025-00:00:00  06/25/2025-23:59:59     1,155,987             7            96
    82      47            N   06/25/2025-00:00:00  06/25/2025-23:59:59            61             7            96
    83       3            N   06/25/2025-00:00:00  06/25/2025-23:59:59       690,695         1,413            96
VALIDATION SUCCEEDED
```

What to pay special attention to? 1/2

- Special Considerations for the times around midnight, as signatures can overlap into the next calendar day.
- If IFASMFDL uses single day input only, a validation with START(0000) END(24000) might fail

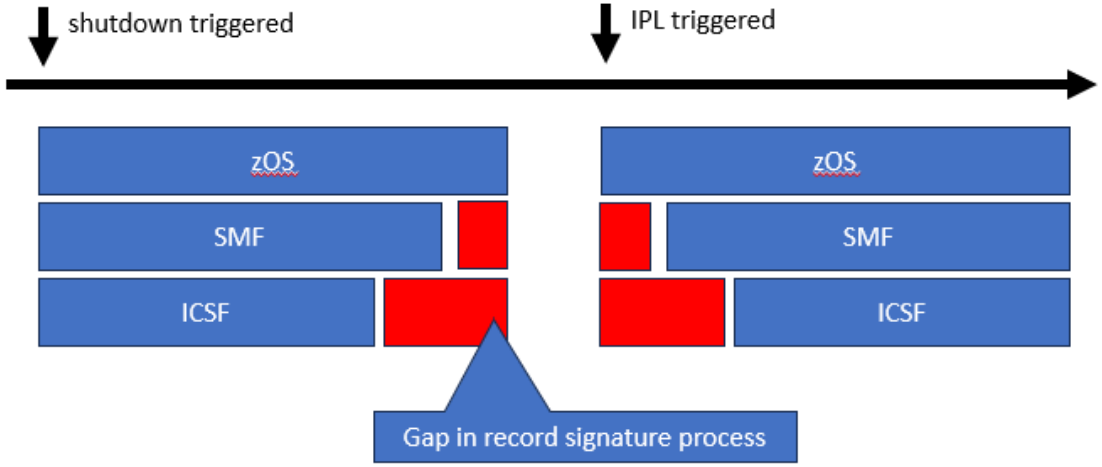
```
IFA010I END(2400) -- SYSIN
IFA010I START(0000) -- SYSIN
   [--content intentionally removed--]
IFA020I DUMPOUT  -- NULLFILE
IFA741I UNABLE TO PERFORM SMF SIGNATURE VALIDATION
IFA742I SMF SIGNATURE VALIDATION FAILED DUE TO
        INCONSISTENT RECORDS - RECORDS DO NOT MATCH EXPECTED COUNTS
 RECORD   RECORD   VALIDATION      VALIDATION START       VALIDATION END       RECORDS        GROUPS     INTERVALS
        TYPE  SUBTYPE      FAILURE             DATE-TIME            DATE-TIME     VALIDATED     VALIDATED     VALIDATED
          16       *            N   05/20/2025-00:00:00  05/20/2025-23:59:59         2,550           635            96
          23       *            Y   05/20/2025-00:00:00  05/20/2025-23:45:00            95            95            95
          41       1            N   05/20/2025-00:00:00  05/20/2025-23:45:00           258            43            95
          41       2            N   05/20/2025-00:00:00  05/20/2025-23:45:00           258            43            95
          41       3            N   05/20/2025-00:00:00  05/20/2025-23:45:00            90            90            95
          87       1            N   05/20/2025-00:00:00  05/20/2025-23:45:00           361           324            95
          88       1            N   05/20/2025-00:00:00  05/20/2025-23:45:00         2,280            95            95
          88      11            N   05/20/2025-00:00:00  05/20/2025-23:45:00         2,200           109            95
          90       *            N   05/20/2025-00:00:00  05/20/2025-23:45:00             1             1            95
         103      13            N   05/20/2025-00:00:00  05/20/2025-23:45:00            95            95            95

     VALIDATION FAILED: INCONSISTENT RECORDS - RECORDS DO NOT MATCH EXPECTED COUNTS
```

What to pay special attention to? 2/2

- Naming convention of the Token (32 Characters fix)
  - Validation relies on the public key, but the token must match the one used during signing. This creates challenges for our process and naming conventions, as the key should be relevant to the validation itself - not tied to the token name.
    - https://ideas.ibm.com/ideas/ZOS-I-4303
- Key Type available (CEX card support especially for LI2) and to be used 'protected key' -> Y or 'clear key' -> T
- Lifecycle of the keys
  - Take notes when they are switched – maybe two tokens for one day
- How to incorporate the validation into the dump process
  - Not yet very resource and user friendly as the same data must be processed twice 1. IFASMFDL then 2. IFASMFDP
    - https://ideas.ibm.com/ideas/ZOS-I-4274
- Validation can only be performed for a single system (SID)

- During shutdown and IPL 'corrupted' signed SMF records reported as ICSF is not available all the time
  - (extremely simplified and only a rough representation of the problem)



Additional information

- SMF signing is active for all our records in all our environments
- Validation currently on an ad-hoc base – planned to incorporate into daily process
- IBM recommends to use RELATIVEDATE and OPTION(ARCHIVE) instead of DATE and OPTION(DUMP)
  - RELATIVEDATE is cumbersome in daily operations and restarts few days later require JCL updates
  - ARHIVE deletes dumped records in logstream – however, we still require them for other processes
- Case TS017593416 still open to address an 'unknown' problem – RC and RSN are reported as 'N/A'
  → Records are signed and can be validated properly – only issued during activation time
  → IBM can reproduce the issue but still looking for the root cause

```
IFA740E UNABLE TO PERFORM SMF SIGNATURE GENERATION 780
FOR LOGSTREAM IFASMF.<ls-name-aa>
UNEXPECTED ERROR IN SMF SIGNATURE PROCESSING
IFA743I SMF SIGNATURE GENERATION FAILURE DIAGNOSTIC INFORMATION 782
FOR LOGSTREAM IFASMF.<ls-name-aa>
TOKENNAME
HASH N/A SERVICE NAME N/A
RC=N/A RSN=N/A
```

References

- IBM Documentation to setup and use digitally signed SMF Records
  - https://www.ibm.com/docs/en/zos/3.1.0?topic=records-setting-up-using-digitally-signed-smf
- IBM Github für ICSF
  - https://github.com/IBM/ICSF-Education/tree/main
- ICSF Return and reason code
  - https://www.ibm.com/docs/en/zos/3.1.0?topic=iccrc-return-codes-reason-codes
- Ideas to vote for related to SMF signatures (BCP_SMF/ICSF and zSecure)
  - ICSF - Enhance IFA742I SMF SIGNATURE VALIDATION FAILED - signature failure → https://ideas.ibm.com/ideas/ZOS-I-4257
  - ICSF - Enhance IFA742I SMF SIGNATURE VALIDATION FAILED - provided tokens → https://ideas.ibm.com/ideas/ZOS-I-4256
  - ICSF - Enhance IFA742I SMF SIGNATURE VALIDATION FAILED - in regards of inconsistent records → https://ideas.ibm.com/ideas/ZOS-I-4255

Any questions?

Legal notice