Quantum-Safe Pervasive Encryption Journey

Bryan Childs
Product Manager, z/OS Security
bchilds@us.ibm.com

IBM

Enterprise Knights of IBM Z

The Mitigation of Risk

277 days

Average time to identify and contain a data breach

USD 9.44 million

Average cost of a data breach in the United States

See https://www.ibm.com/security for the full 2022 report

Why is the time to act now?

Data is being stolen today with the intent of exposing it tomorrow

Encrypted data lost during a data breach

Data communications over TLS that have been harvested

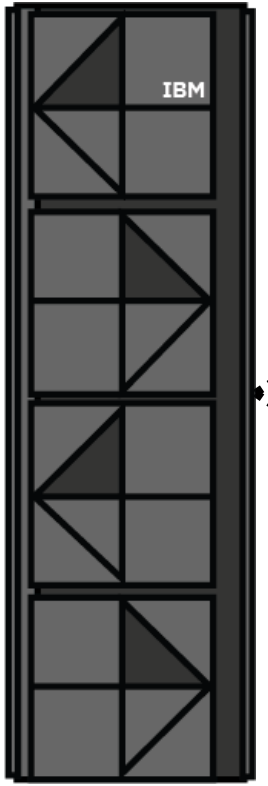
Snapshots of encrypted cloud data

Media that is not encrypted with quantum-safe encryption methods and is improperly disposed or lost

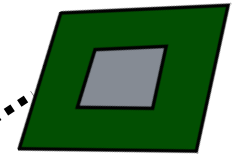
Encryption systems using blackened(wrapped) encryption keys that are public

Data must be protected with strong encryption algorithms like AES using 256-bit keys to be considered quantum-safe

Quantum-Safe encryption components

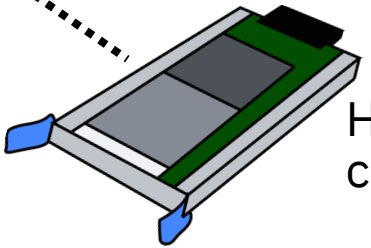


CPACF

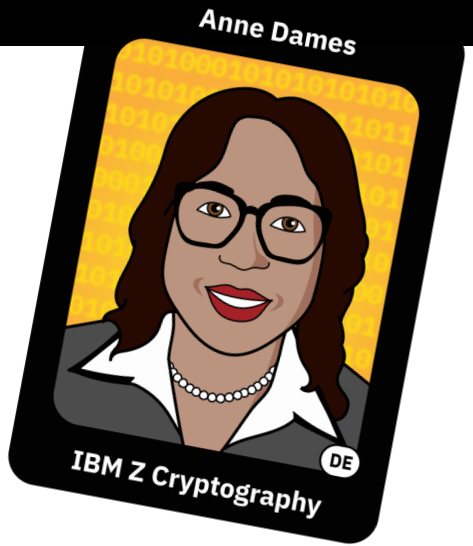


High performance key calculations

Crypto Express 8S



High security key calculations



TKE Workstation

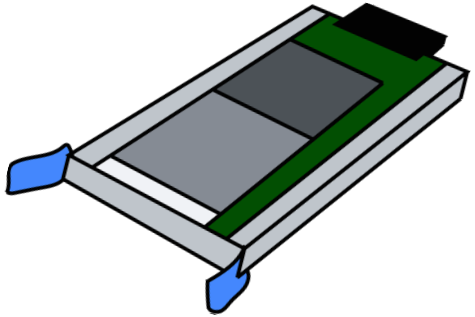
Simplified & secure Master Key usage

ICSF support of CRYSTALS

ICSF support for enhanced quantum-safe algorithms as provided by the Crypto Express8 (CEX8) Coprocessor:

- CRYSTALS-Dilithium keys are used for digital signature operations
- CRYSTALS-Kyber keys are used for key exchange

Crypto Express 8S (CEX8S)



CRYSTALS-Dilithium was first introduced on the z15, but as the NIST evaluation of quantum-safe algorithms continues, new “rounds” of the submitted algorithms are introduced. When the CRYSTAL-Dilithium algorithm progressed to “Round 3” of the evaluation, updates to the key generation algorithms were added. The CEX8 coprocessor added support for the new Round 3 keys, and also added a (8,7) key size in addition to the (6,5) key size previously available.

CRYSTALS-Kyber is a new key type available on the z16 with the CEX8 Coprocessor. When used in combination with Elliptic Curve Diffie-Hellman, it is now possible to use a hybrid approach for exchanging secret keys between business partners using quantum-safe techniques.

Quantum-Safe clarifications

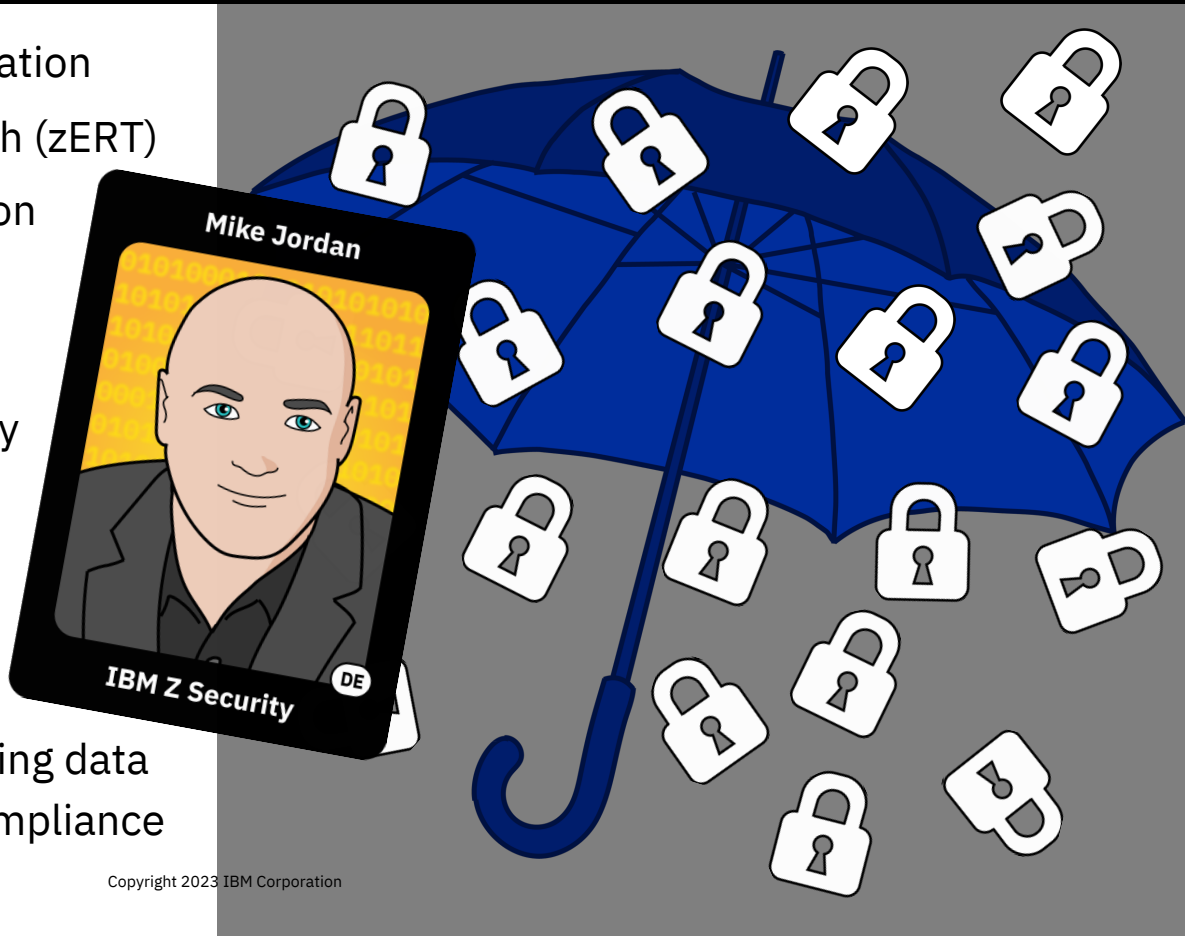
z/OS Data Set Encryption is considered Quantum-Safe (AES-256)
Quantum-Safe digital certificates' definition pending
Quantum-Safe network encryption definition pending

This Quantum-Safe journey is a natural continuation of Pervasive Encryption

Pervasive encryption umbrella

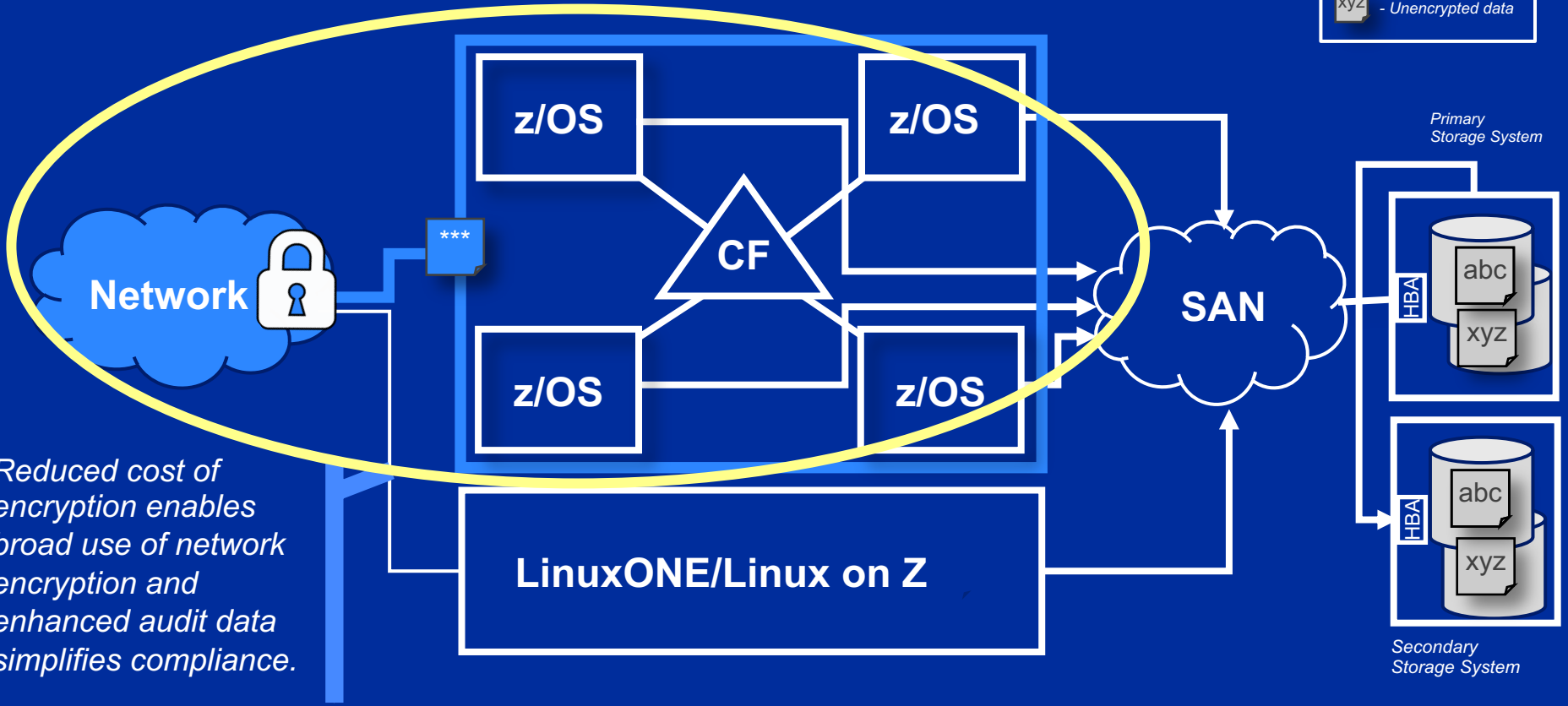
An umbrella of encryption differentiation

- z/OS Encryption Readiness Tech (zERT)
- z/OS Coupling Facility encryption
- z/OS Data Set Encryption (DSE)
- z/OS JES spool encryption
- Fibre Channel Endpoint Security
- and more



Addressing a critical need in mitigating data breach risk and simplifying audit compliance

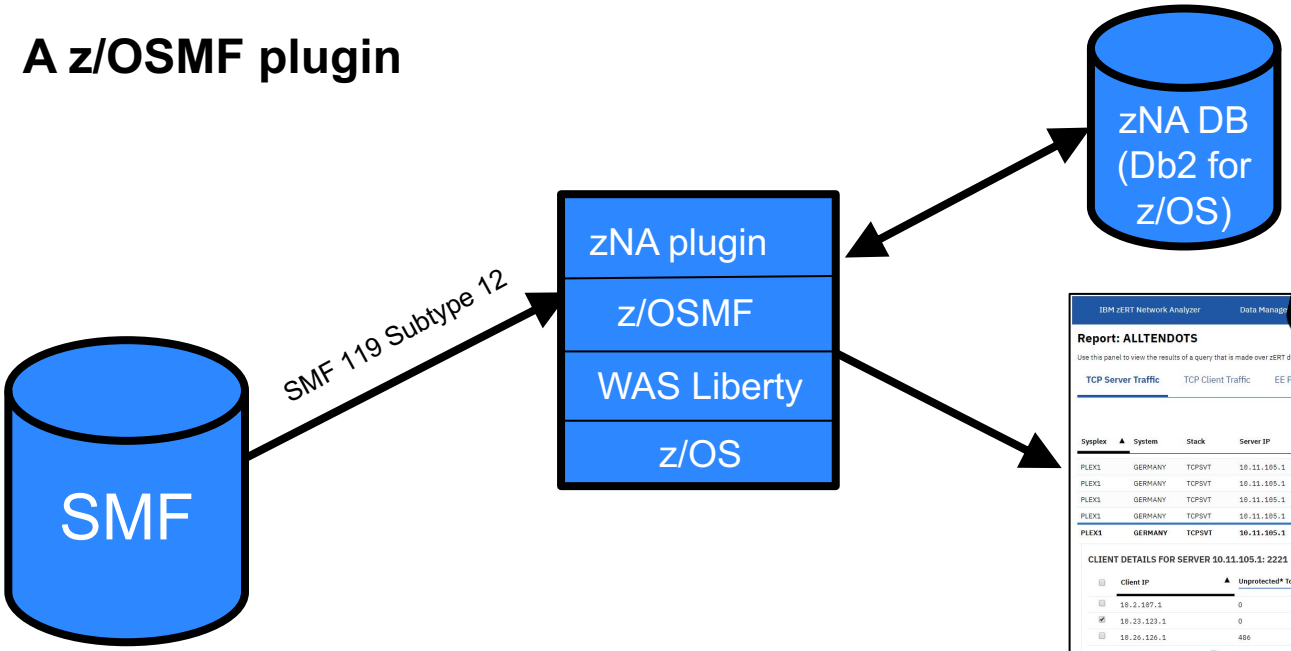
Blueprint #1: z/OS network encryption

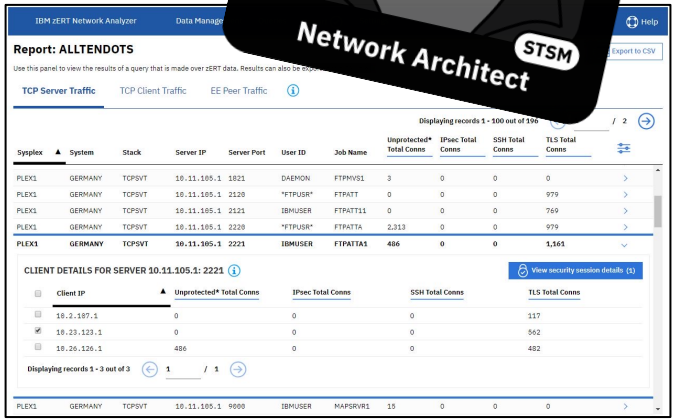


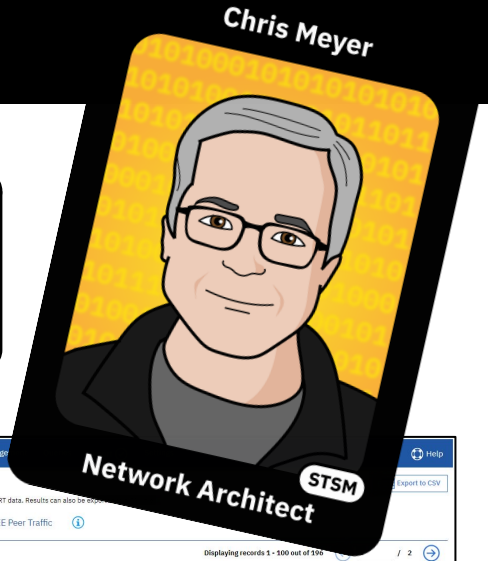
Reduced cost of encryption enables broad use of network encryption and enhanced audit data simplifies compliance.

The zERT Network Analyzer (1 of 3)

A z/OSMF plugin







Web UI makes zERT data consumable for **z/OS network security administrators**

The zERT Network Analyzer (2 of 3)

IBM z/OS Management Facility

Welcome user3 | IBM

- Welcome
- Notifications
- Workflows
- Configuration
- Consoles
- Links
- z/OS Classic Interfaces
- z/OSMF Administration
- z/OSMF Settings
- Analysis
  - IBM zERT Network Analyzer

Refresh

Welcome × | IBM zERT Networ... ×

IBM zERT Network Analyzer | Data Management | Queries | Report | Se

Manage Queries

Manage Queries

Use this panel to manage existing queries saved to IBM zERT Network Analyzer.

SAVED QUERIES

Refresh queries list

Name	Description				
[illegible]	Traffic to all 10.0.0.0/8 servers	Run query	Edit query	Export query	Delete query
ALL WEAK TLS PROTECTION	Look for any SSLv2, SSLv3 and TLSv1.0	Run query	Edit query	Export query	Delete query
	SCOPE FILTERS: *No scope filters specified for this query*	SECURITY FILTERS: TLS protocol version SSL 2.0, SSL 3.0, TLS 1.0			
BATCH 7 WORKLOAD	Check workload for [illegible]	[illegible]	Edit query	Export query	Delete query
FVT	*No description provided*	Run query	Edit query	Export query	Delete query
MARCH 23-25	All traffic between these two dates	Run query	Edit query	Export query	Delete query
MG-1 DATE TCP FILTERS	Mike's query	Run query	Edit query	Export query	Delete query
PLEX 1 WEAK OR CLEAR	Plex 1 traffic with weak TLS or no protection	Run query	Edit query	Export query	Delete query
SHOW ME EVERYTHING	Display everything currently in the database	Run query	Edit query	Export query	Delete query

User-built queries allow you to zero in on exactly the scope of records and security filters you're interested in.

The zERT Network Analyzer (3 of 3)

IBM z/OS Management Facility

Welcome user3 | IBM

- Welcome
- Notifications
- Workflows
- Configuration
- Consoles
- Links
- z/OS Classic Interfaces
- z/OSMF Administration
- z/OSMF Settings
- Analysis
  - IBM zERT Network Analyzer

Refresh

Welcome × | IBM zERT Networ... ×

IBM zERT Network Analyzer | Data Management | Queries | Repo

Report: ALL WEAK TLS PROTECTION

Use this panel to view the results of a query that is made over zERT data. Results can also be expor

TCP Server Traffic | TCP Client Traffic | EE Peer Traffic

Displaying records 1 - 18 out of 18 1 / 1

Sysplex	System	Stack	Server IP	Server Port			Unprotected* Total Conns	IPsec Total Conns	SSH Total Conns	TLS Total Conns
PLEX1	GERMANY	TCPSVT	10.11.105.8		IBMUSER	REXECD	0	0	0	10
PLEX1	GERMANY	TCPSVT	10.11.201.	925	IBMUSER	TNPRC925	0	0	0	778

SECURITY SESSION DETAILS FOR SERVER 10.11.201.3:

View client details

TLS Session Details | Cryptographic Details

Client IP	Protocol Versi	Negotiated Cipher	Key Exchange Alg	Symm Encryption Alg	Message Auth Alg
10.2.14.1	TLSv1.0	0035	RSA	AES CBC 256	HMAC-SHA1
10.2.16.103	TLSv1.0	0035	RSA	AES CBC 256	HMAC-SHA1
10.23.123.1	TLSv1.0	0035	RSA	AES CBC 256	HMAC-SHA1

Displaying records out of 3 1 / 1

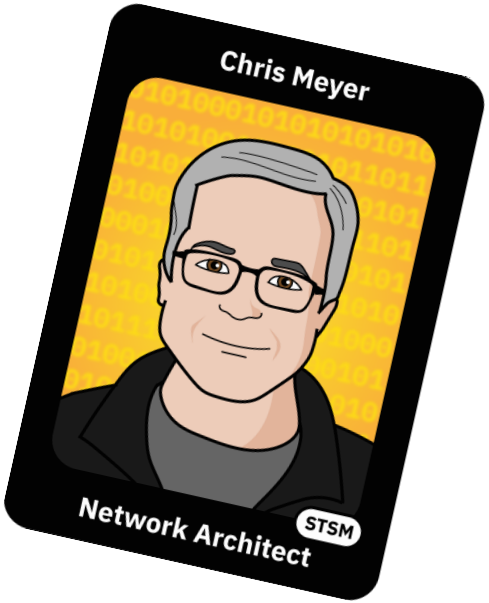
PLEX1	GERMANY	TCPSVT	10.11.201.3	951	IBMUSER	TNPRCAT3	0	0	0	239
PLEX1	GERMANY	TCPSVT	10.11.201.3	2020	*FTPUSR*	FTPTLS1	0	0	0	11

Results are displayed in a format that allows you to drill down from a server-level summary to the specifics of each individual customer.

zERT Enforcement (z/OS 2.5)

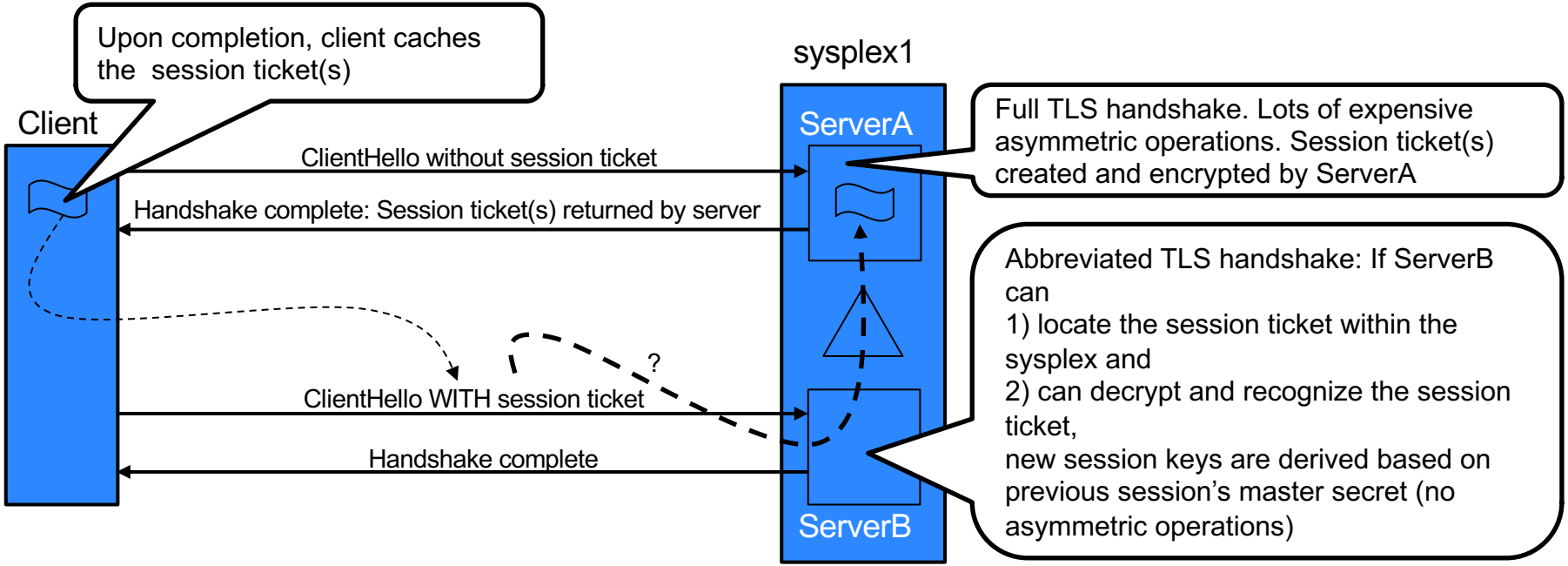
What makes zERT Enforcement so special?

- Utilizes zERT stats in-memory (not in SMF)
- Determination made after handshake completes
- Cancels the connection when minimum not met
- Unlike Policy Agent, not limited to AT-TLS usage
- *Auditable minimum network encryption strength!*



Sysplex-wide TLSv1.3 session resumption (z/OS 3.1)

- Prior to 3.1, TLSv1.3 session tickets only worked within a single System SSL instance
- With 3.1, TLSv1.3 session tickets can be shared across multiple instances of the same server application within a sysplex
- Extends the benefit of TLSv1.3 session resumption across the sysplex



Session Ticket Caching configuration (z/OS 3.1)

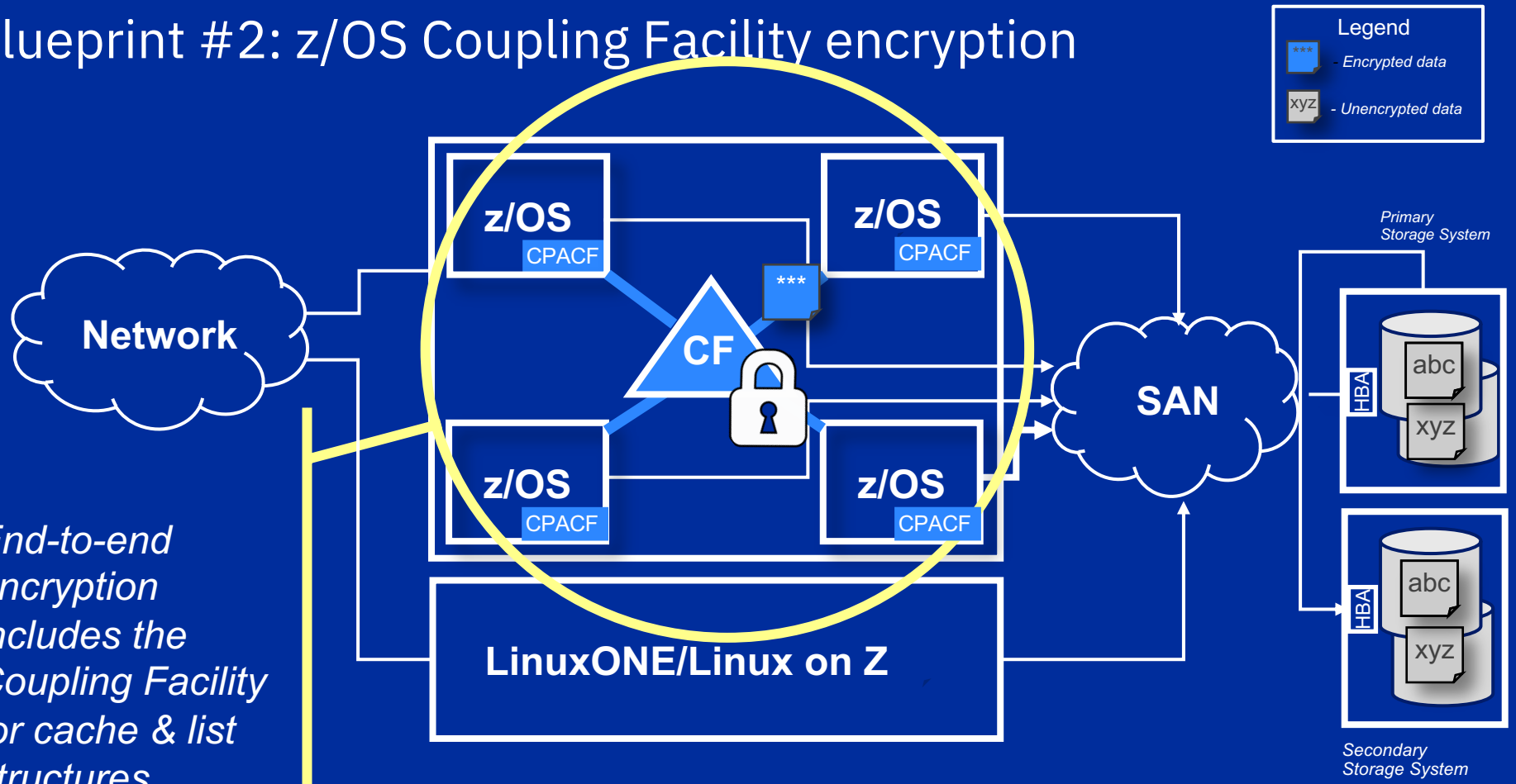
Two new configuration parameters on the TTLSGskAdvancedParms statement:

- GSK_SYSPLEX_SESSION_TICKET_CACHE enables sysplex-wide session ticket support when AT-TLS is acting at the TLS server. The default is Off.

  Note the GSKSRVR task must be started on each z/OS system in the sysplex that is to share session tickets.

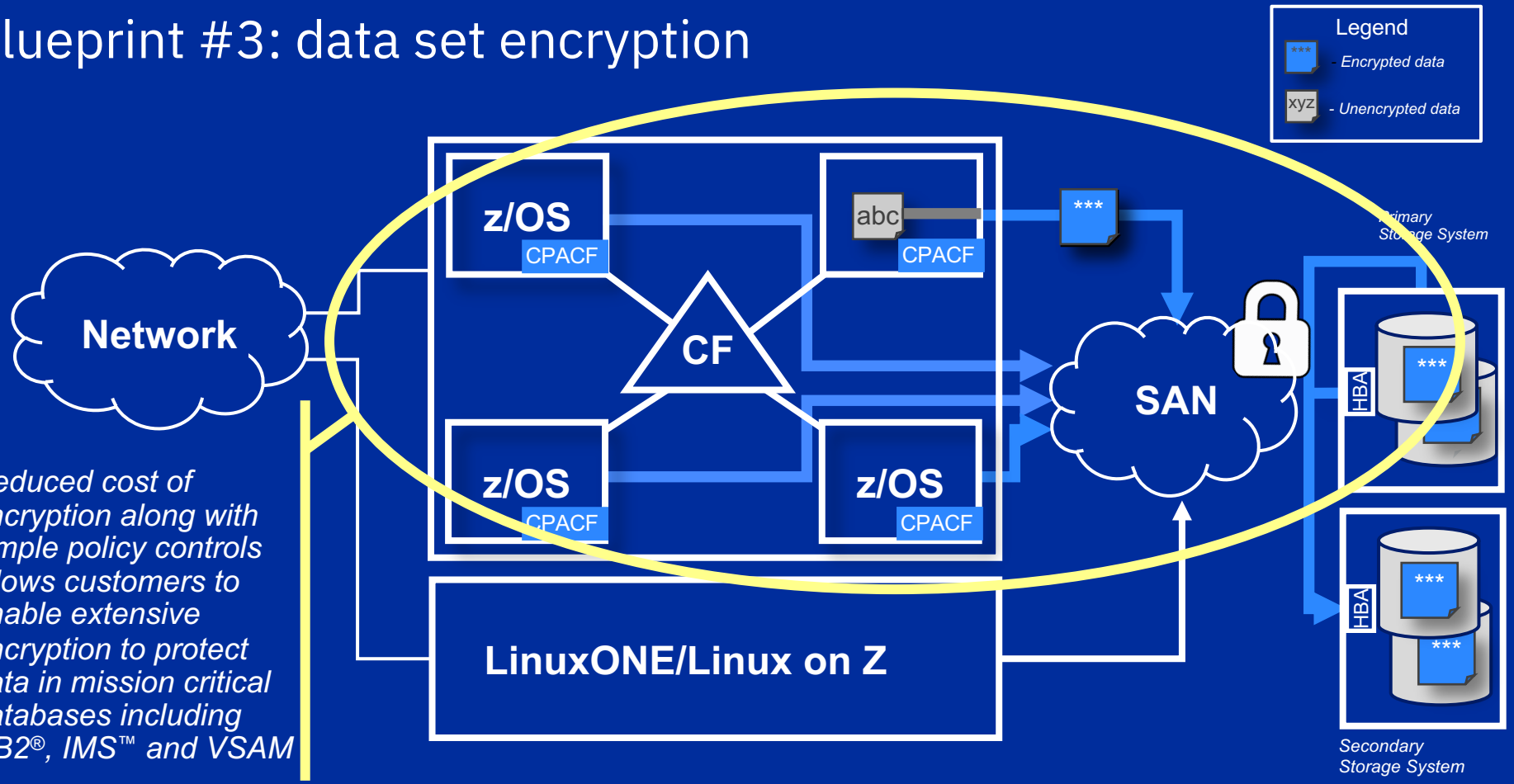
- GSK_SESSION_TICKET_CLIENT_MAXCACHED is an optional parameter that controls the maximum number of session tickets to be cached when AT-TLS is acting as the TLS client. The default is 8.

Blueprint #2: z/OS Coupling Facility encryption



End-to-end encryption includes the Coupling Facility for cache & list structures.

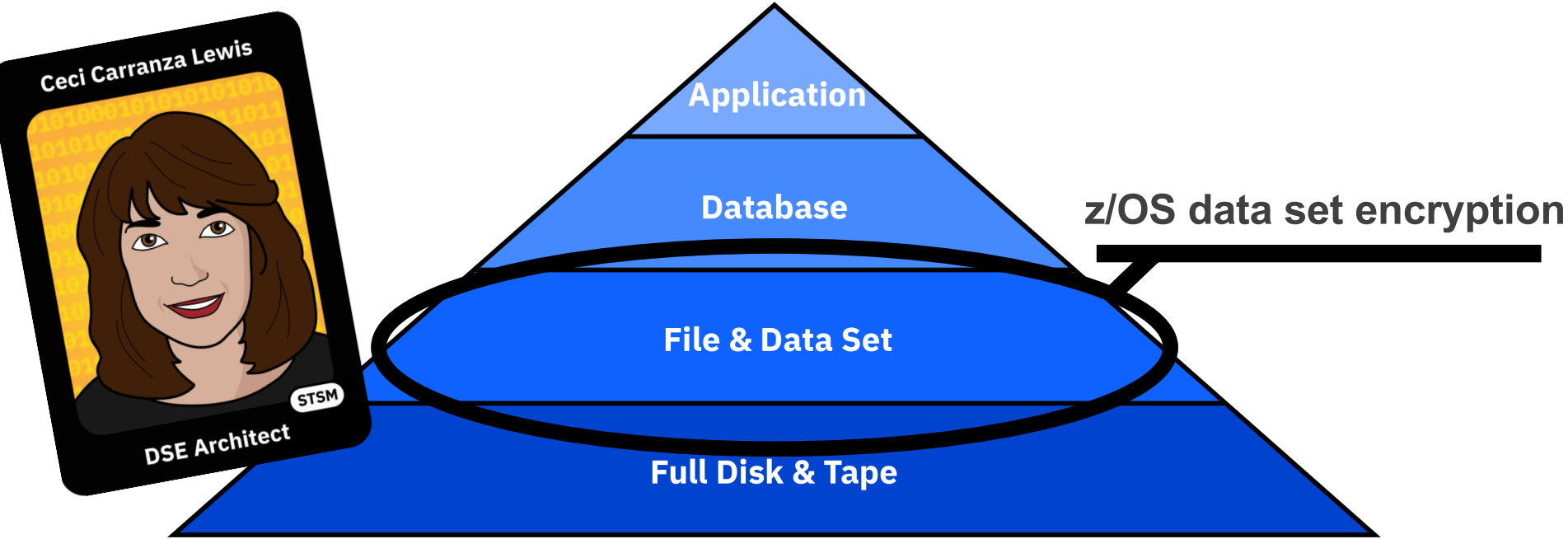
Blueprint #3: data set encryption



Reduced cost of encryption along with simple policy controls allows customers to enable extensive encryption to protect data in mission critical databases including DB2®, IMS™ and VSAM

The Encryption Pyramid: DSE

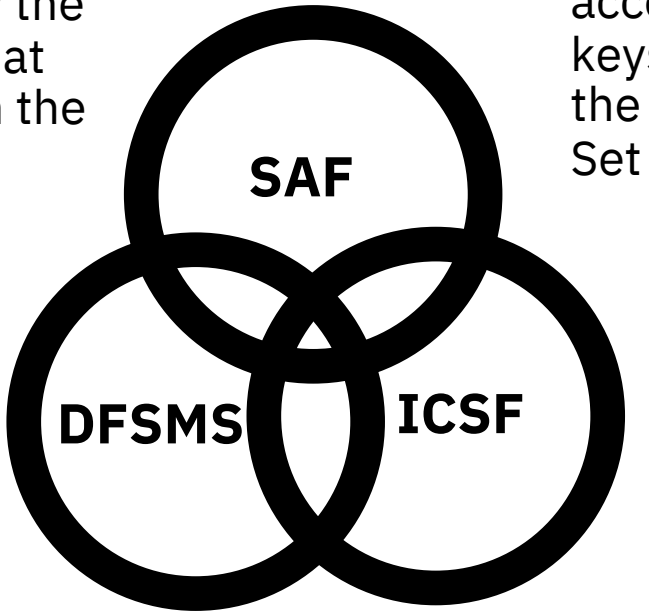
Cost-effective encryption of data at rest to *satisfy compliance* requirements



Components of z/OS data set encryption

DATASET profiles are denoted for Data Set Encryption by the presence of a **key label** that corresponds to a profile in the **CSFKEYS** class.

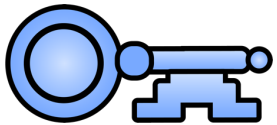
The **CSFKEYS** class controls access to the cryptographic keys in ICSF Key Stores, e.g. the Cryptographic Key Data Set (CKDS).

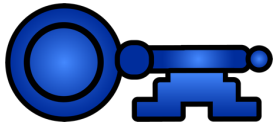


DFSMS will respond to the presence of the **key label**, check the user's access to **CSFKEYS**, and interact with ICSF for the associated protected key.

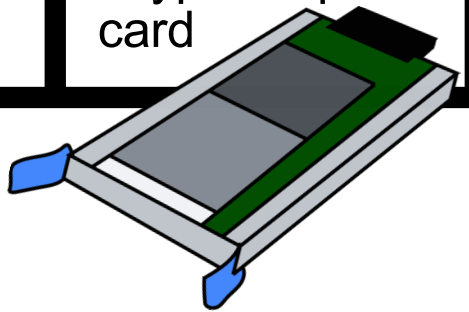
The **CSFSERV** class controls access to ICSF's cryptographic services & its TSO panel utilities.

Contrasting Master & Operational Keys





Key Type	Storage Location	Purpose
Operational Key	key store	Used to encrypt & decrypt z/OS data sets.
Master Key	Crypto Express card	Used to encrypt / “wrap” an Operational Key to securely store it.



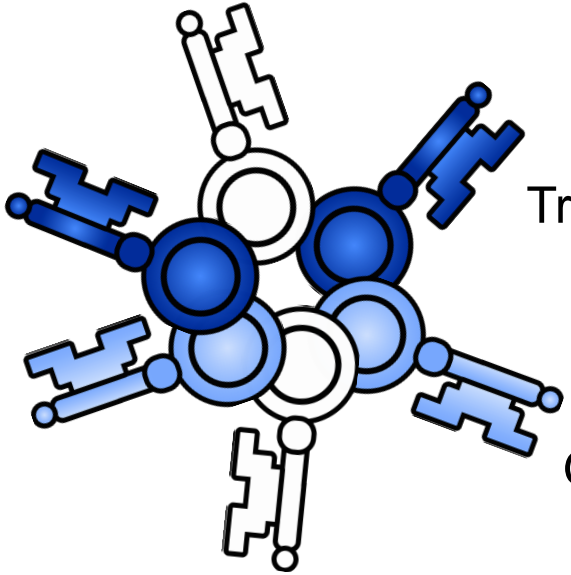
Types of keys

Key Type	Location	Purpose
clear key	host memory & key store	No encryption to protect the key. This is not recommended.
secure key	host memory & key store	Encrypted with a Master Key to best protect it in the key store.
protected key	host memory	Encrypted using CPACF wrapping key for hybrid security & performance.

Customized key management

Enterprise Key Management Foundation – Web Edition (EKMF Web)

Operational Keys

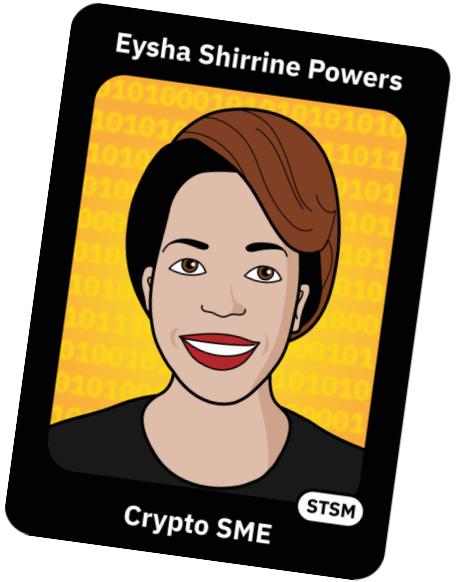


Trusted Key Entry (TKE) Workstation

Master Keys

Guardium Key Lifecycle Manager (GKLM)

Self-encrypting Device Keys



EKMF Web functionality

Pervasive Encryption

- Centralised key management for Pervasive Encryption
- Distribute keys across multiple Sysplexes and LPARs
- Key Monitoring and one-click recovery
- View dataset encryption status through dataset dashboard

Cloud Key Management

- AWS
- Azure
- IBM Key Protect & HPCS

ZKey Integration

- ZKey provides Volume encryption for LinuxOne

EKMF Web

- Creates and manages the volume encryption keys
- Enables sharing of keys between Linux systems

GKLM Integration

- GKLM Provides keys to Storage devices for data encryption

EKMF Web

- Enables GKLM to use a hardware protected master key
- Handles encryption and decryption of storage keys on demand

EKMF Web API

- Enables key management integration with business processes
- Interactive Swagger API Explorer interface for documentation and prototyping.
- Functionally equivalent to the EKMF Web UI.

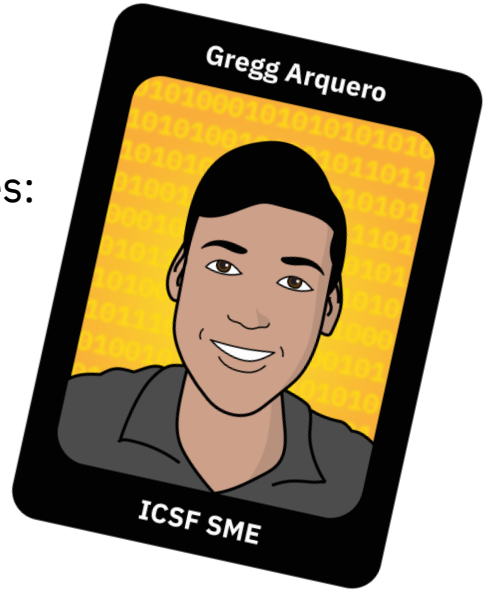
Master key distribution option (z/OS 3.1)

Master key entry via the ICSF panels has been enhanced to limit who can load each key part and reset the new master key registers.

To enable, the **CSF.MASTER.KEY.ENTRY.BY.PART** XFACILIT control must be enabled.

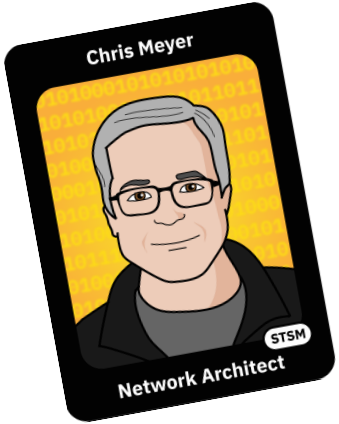
To load key parts, users must have READ access to the key part profiles:

- CSF.MKE.LOAD.FIRST.PART
- CSF.MKE.LOAD.MIDDLE.PART
- CSF.MKE.LOAD.FINAL.PART
- CSF.MKE.RESET.NMK

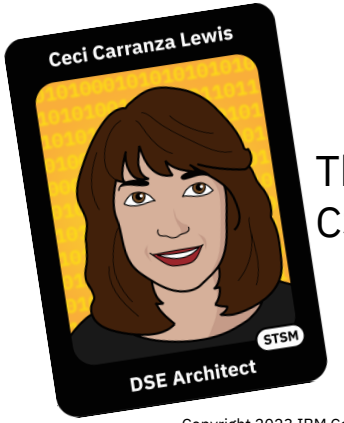


Master key distribution example

First key officer
CSF.MKE.LOAD.FIRST.PART



Second key officer
CSF.MKE.LOAD.MIDDLE.PART



Third key officer
CSF.MKE.LOAD.FINAL.PART

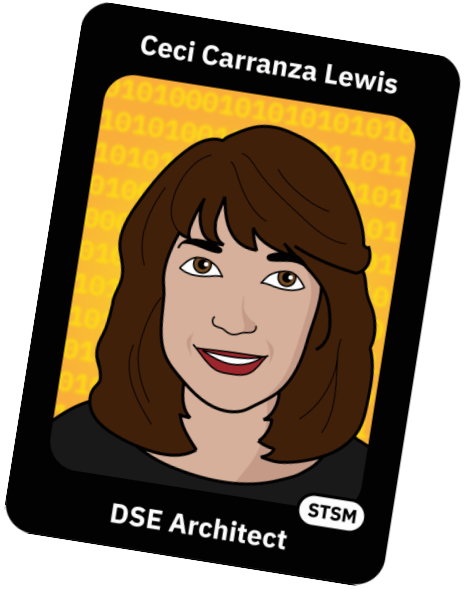
Key Parts are
XORed together

1DA6CCD7...
CB4D6ED4...
3F48395AC...

E9A39B59D...

Initial encryption format support

- Extended Format Encryption
  - SMS-managed only
  - Sequential extended format data sets
    - Accessed through BSAM and QSAM
  - VSAM extended format data sets
    - (KSDS, ESDS, RRDS, VRRDS, LDS) that are accessed through base VSAM and VSAM/RLS)



Basic and large format encryption (z/OS 2.4)

- Basic and Large Format Encryption (non-extended format DASD data sets)
  - Access using BSAM and QSAM APIs
    - Transparent to application except for DASD space calculations (due to new 8-byte block prefix)
  - Access using EXCP
    - Application changes required
      - » The EXCP program must account for 8 byte prefix on each block
      - » The EXCP program must encrypt the data before writing and decrypt after reading
      - » New macro, IGGENC provided for encryption/decryption

This enables vendors' custom data base software to support data set encryption

JES spool encryption (z/OS 2.4)

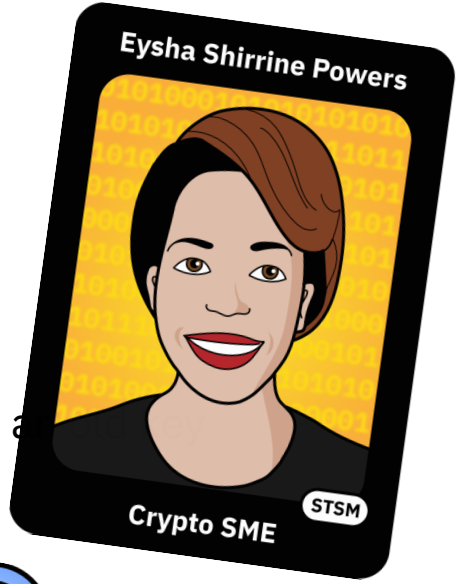
- Security Administrators required to protect sensitive data on SPOOL can leverage the z Systems hardware encryption through existing policy management without application changes.
- Similar to DFSMS, this involves defining a record in the CKDS data set which can be identified and accessed via a 64-character key label.
- Use of this key label is secured via SAF/RACF profiles.
- JCL parameter DSKEYLBL or JESJOBS class profiles can be used to identify SYSOUT and instream data sets to be encrypted.
- Data to be encrypted will first be compressed providing storage efficiency.
- New COMPRESS= option on OUTCLASS(x) statement allows SYSOUT data sets to be compressed (even if not encrypting the data)

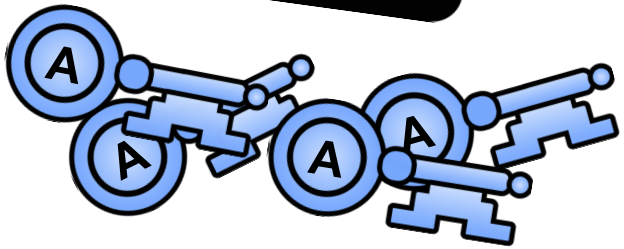
Enhancement to Archived Keys (z/OS 2.5)

- General insight: ”Never throw away a key”
  - Ensures data is not lost if key rotation is incomplete
  - Migrated data may become out of scope
  - Archive keys instead

- New decrypt-only configuration option for Archived Keys
  - Supported by ICSF and by z/OS data set encryption in 2021
  - Mitigates risk of a “moving target” of data sets encrypted with a
  - Facilitates key rotation

XFACILIT profile ‘CSF.KDS.KEY.ARCHIVE.DATA.DECRYPT’





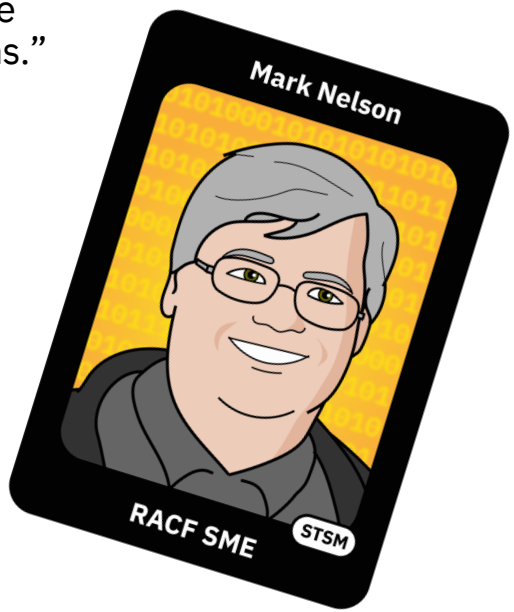
RACF statement of direction realized!

Encrypted VSAM data set support in RACF

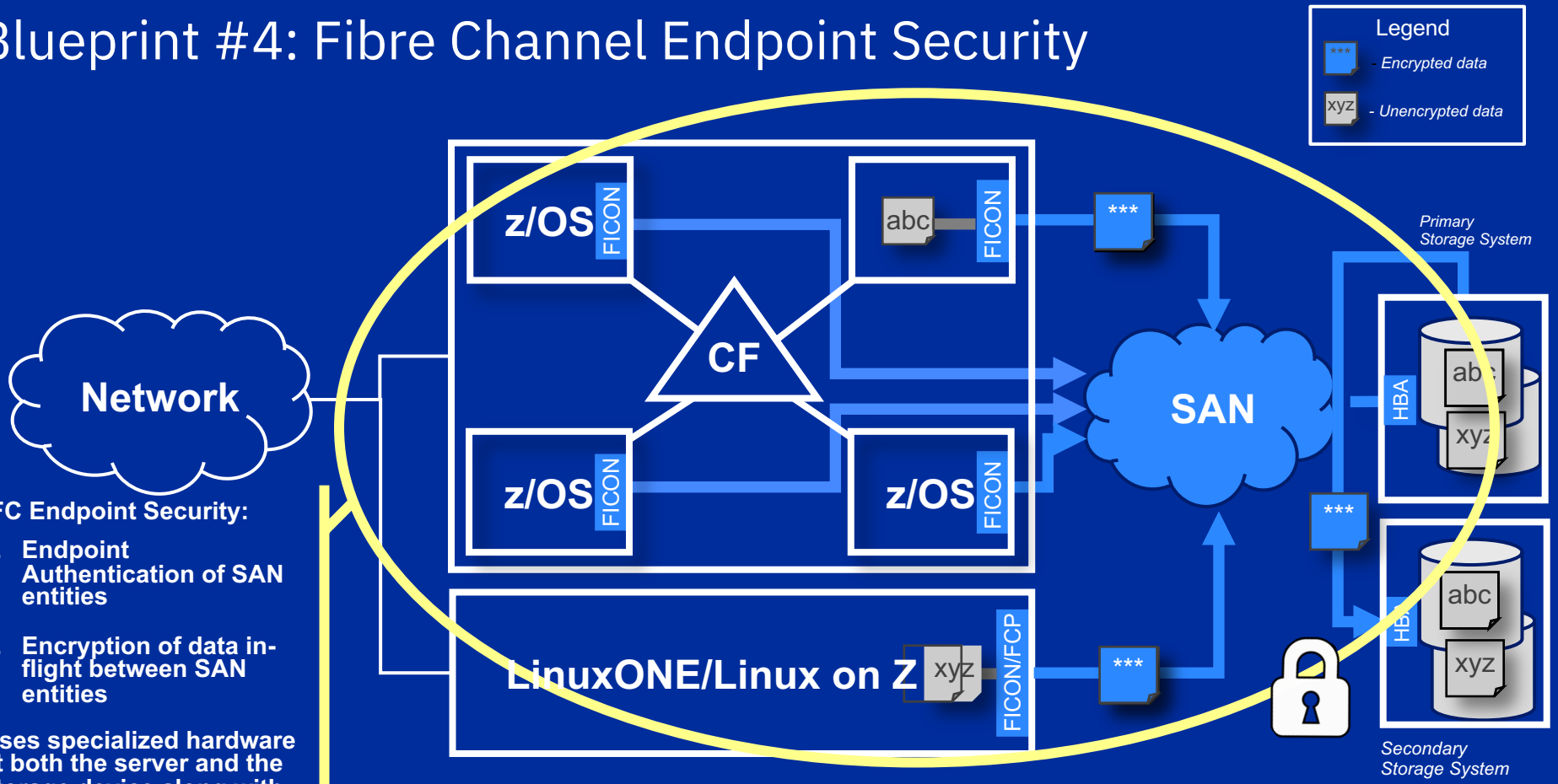
"IBM intends to enhance pervasive encryption through RACF support for the use of an encrypted VSAM data set as its data base in specific configurations."

Why VSAM?

- Enables data set encryption
- Integrates well with RACF's existing serialization
- Consistent with RACF's current database architecture
- Provides the ability to utilize existing diagnostics
- Leverages standard z/OS skills
- Leverages current and future I/O infrastructure improvements



Blueprint #4: Fibre Channel Endpoint Security

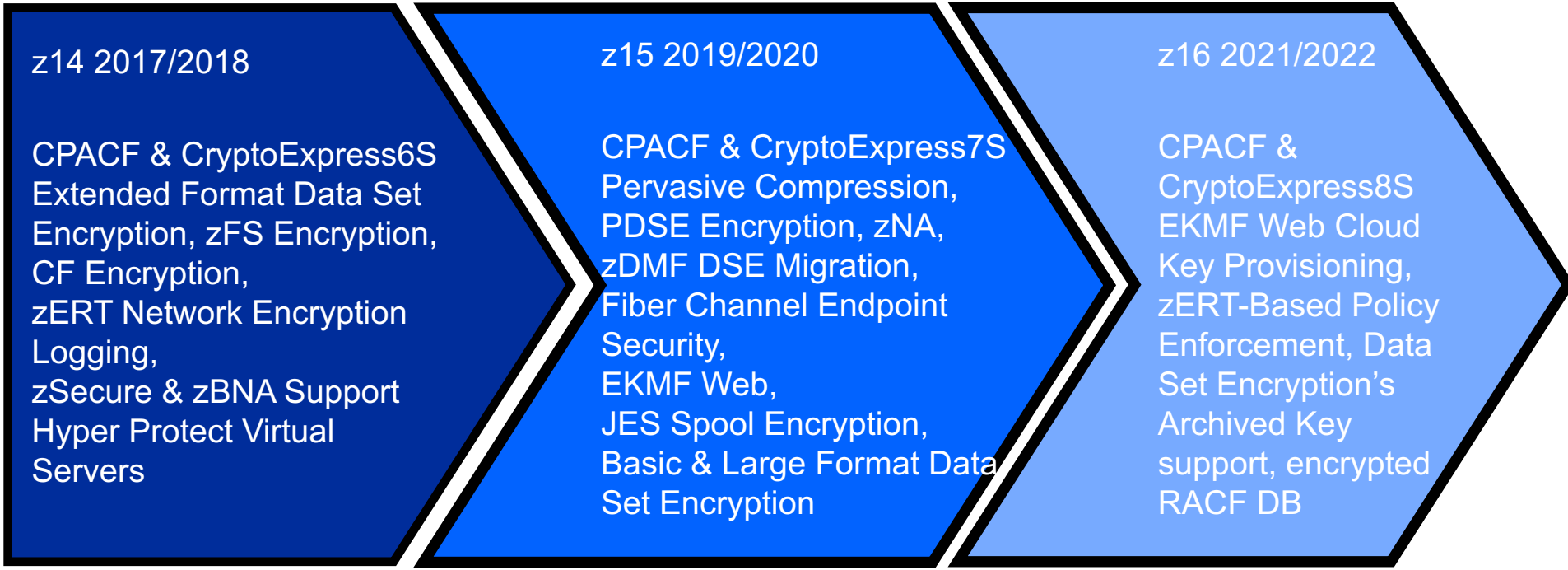


FC Endpoint Security:

1. **Endpoint Authentication of SAN entities**
2. **Encryption of data in-flight between SAN entities**

Uses specialized hardware at both the server and the storage device along with GKLM

Pervasive Roadmap so far



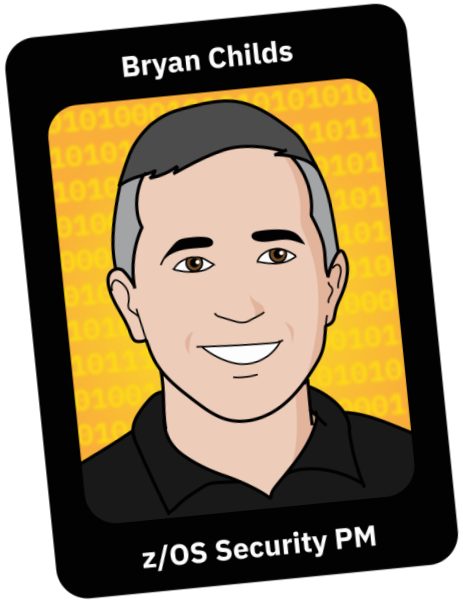
Redbook assistance

”Transitioning to Quantum-Safe Cryptography on IBM Z”
https://www.redbooks.ibm.com/abstracts/sg248525.html

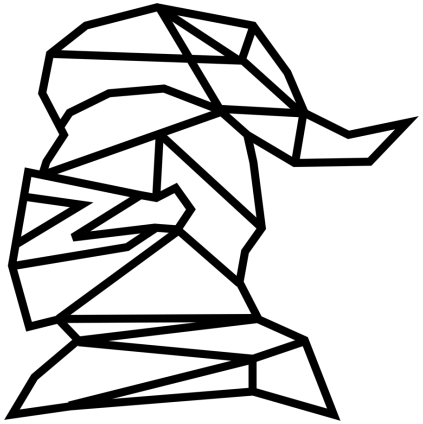
“Getting Started with Data Set Encryption”
https://www.redbooks.ibm.com/abstracts/sg248410.html

Redbooks

Gratitude



THANK YOU!



Trademarks

See URL: **http://www.ibm.com/legal/copytrade** for a list of trademarks.