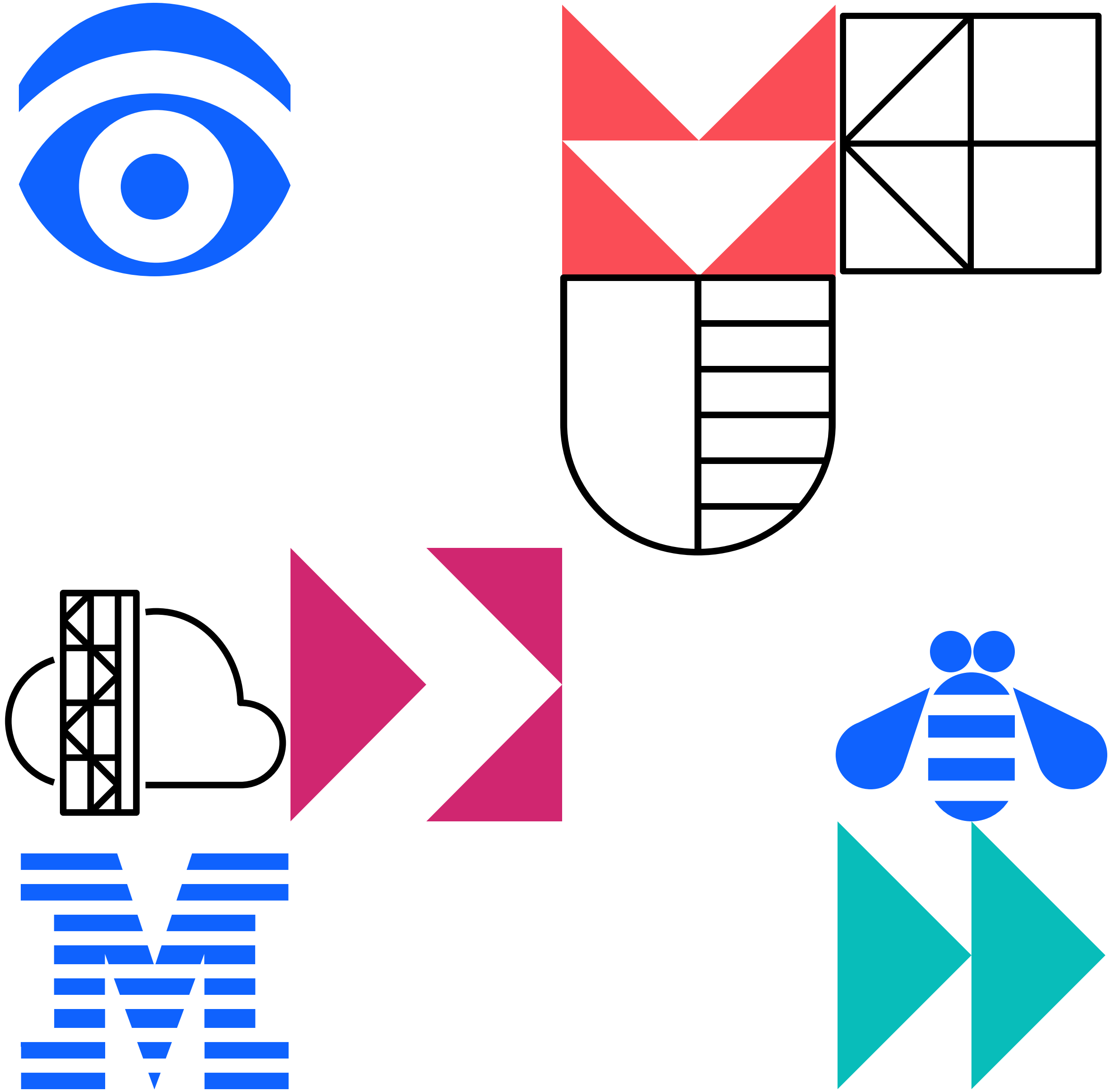
The Pervasive Encryption Journey: Data Security, Key Rotation, and Quantum Resilience



Gregg Arquero
IBM Software Engineer, Security
gmarquer@us.ibm.com

IBM

Cost of data breaches spikes in 2024

USD $4.88M

Global averages of data breach costs increased 10% from 2024, the largest jump seen in one year.

40%

Nearly half of breaches involved data distributed across multiple environments.

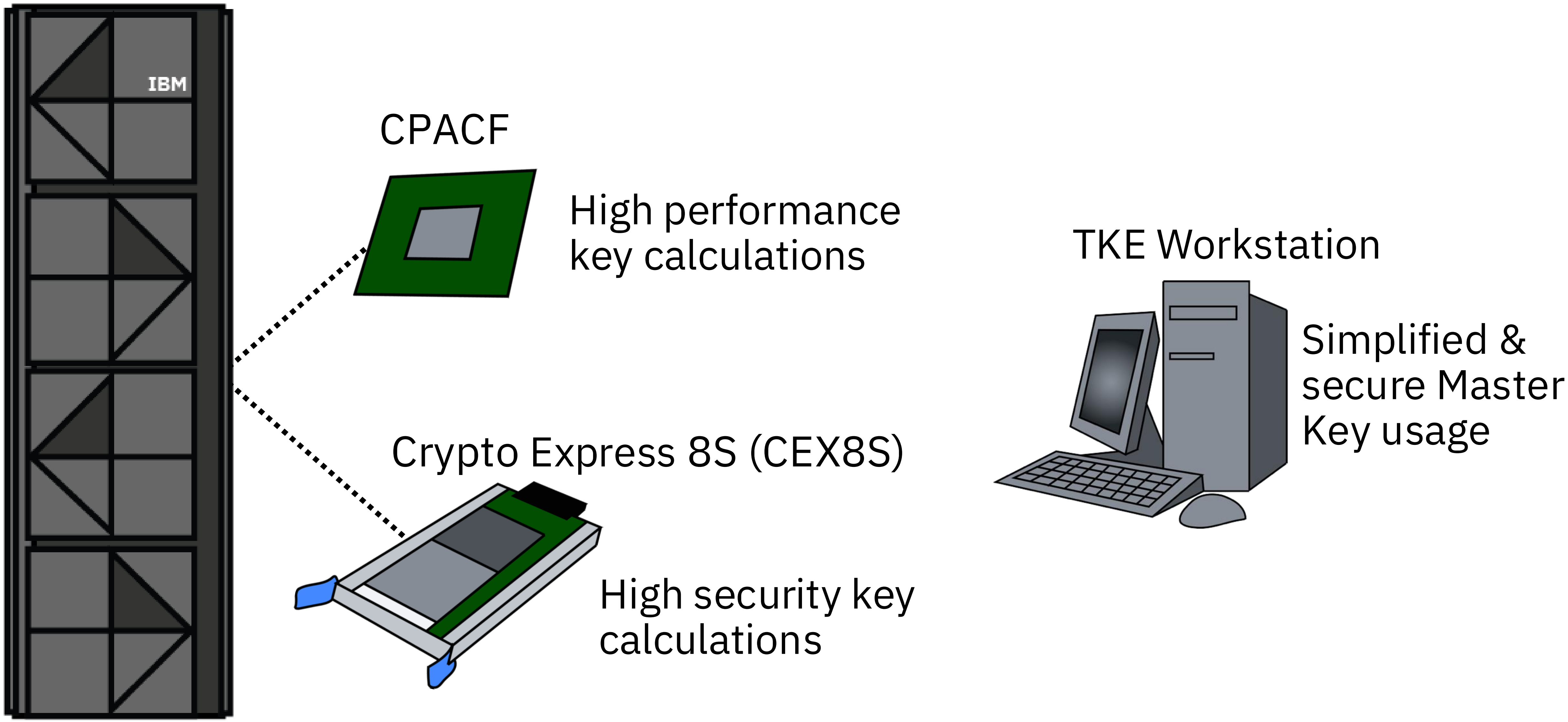
70%

A majority of organizations reported a significant or very significant disruption to business.

Source: Cost of a Data Breach Report 2024

IBM Z Pervasive Encryption

IBM z16 crypto hardware components



IBM Z Pervasive Encryption

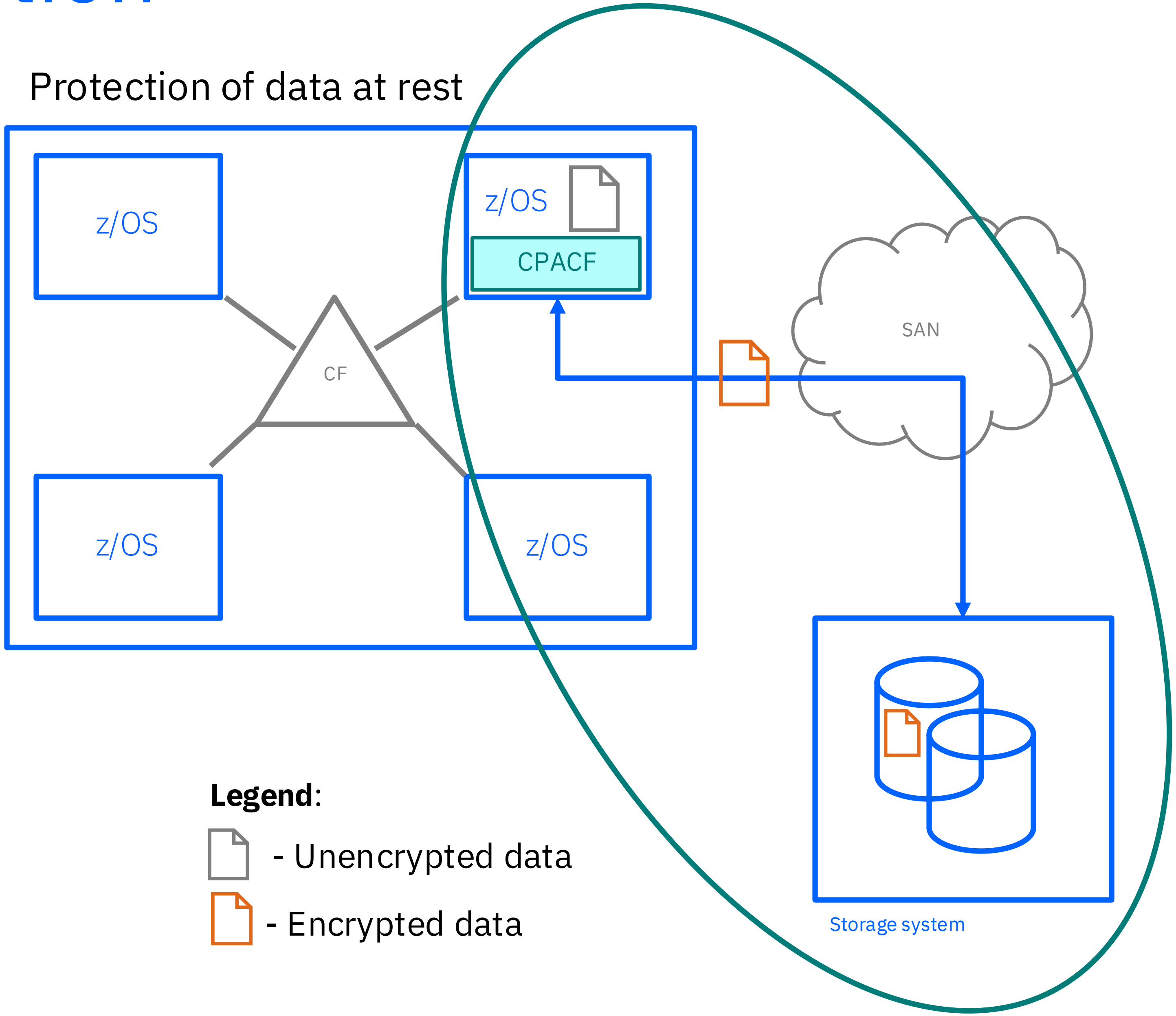
Enabled through full-stack platform integration

Integrated Crypto Hardware	Hardware accelerated encryption on every core – CPACF performance improvements of up to 7x Next Gen Crypto Express8S – up to 2x faster than prior generation
Data at Rest	Broadly protect Linux volumes and z/OS data sets using policy-controlled encryption that is transparent to applications and databases
Clustering	Protect z/OS Coupling Facility data end-to-end, using encryption that's transparent to applications
Network	Protect network traffic using standards-based encryption from end to end, including encryption readiness technology to ensure that z/OS systems meet approved encryption criteria
Hyper Protect Virtual Servers	Secure deployment of software appliances including tamper protection during installation and runtime, restricted administrator access, and encryption of data and code in-flight and at-rest
Key Management	The IBM Unified Key Orchestrator for z/OS (UKO for z/OS) provides real-time, centralized secure management of keys and certificates with a variety of cryptographic devices and key stores.

z/OS Data Set Encryption

- Application transparent & enabled by policy
- Host encryption via CPACF as data is written to or read from disk
- Supports Seq ext fmt, VSAM ext fmt, PDSE, JES2 spool, Db2, CICS, & IMS
- Includes HSM & DSS migration and backup of encrypted data sets
- Replicated data remains encrypted

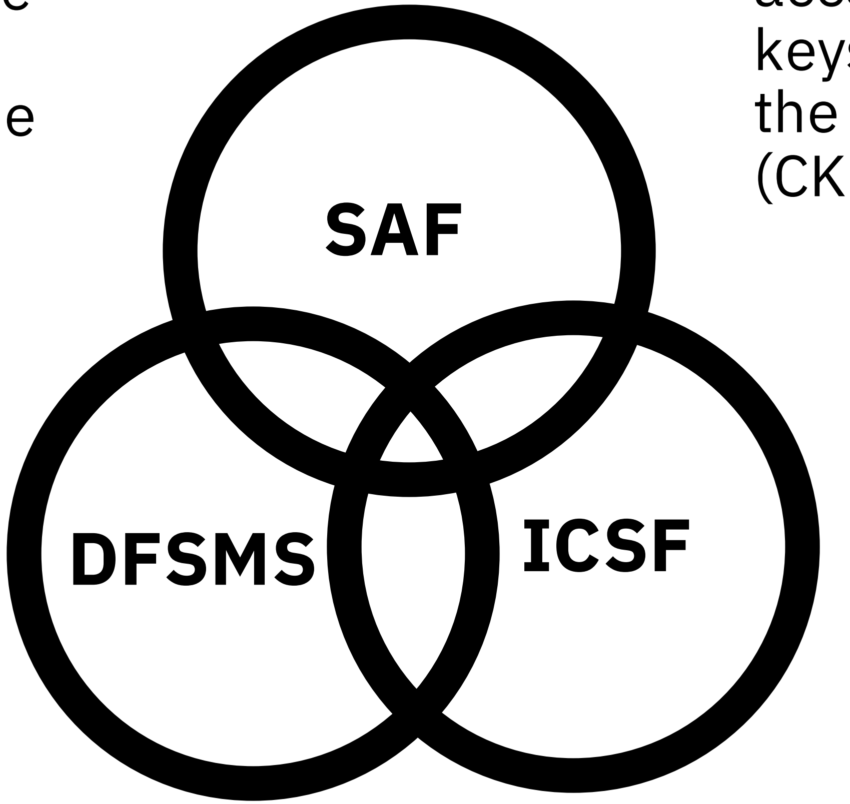
Protection of data at rest



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).



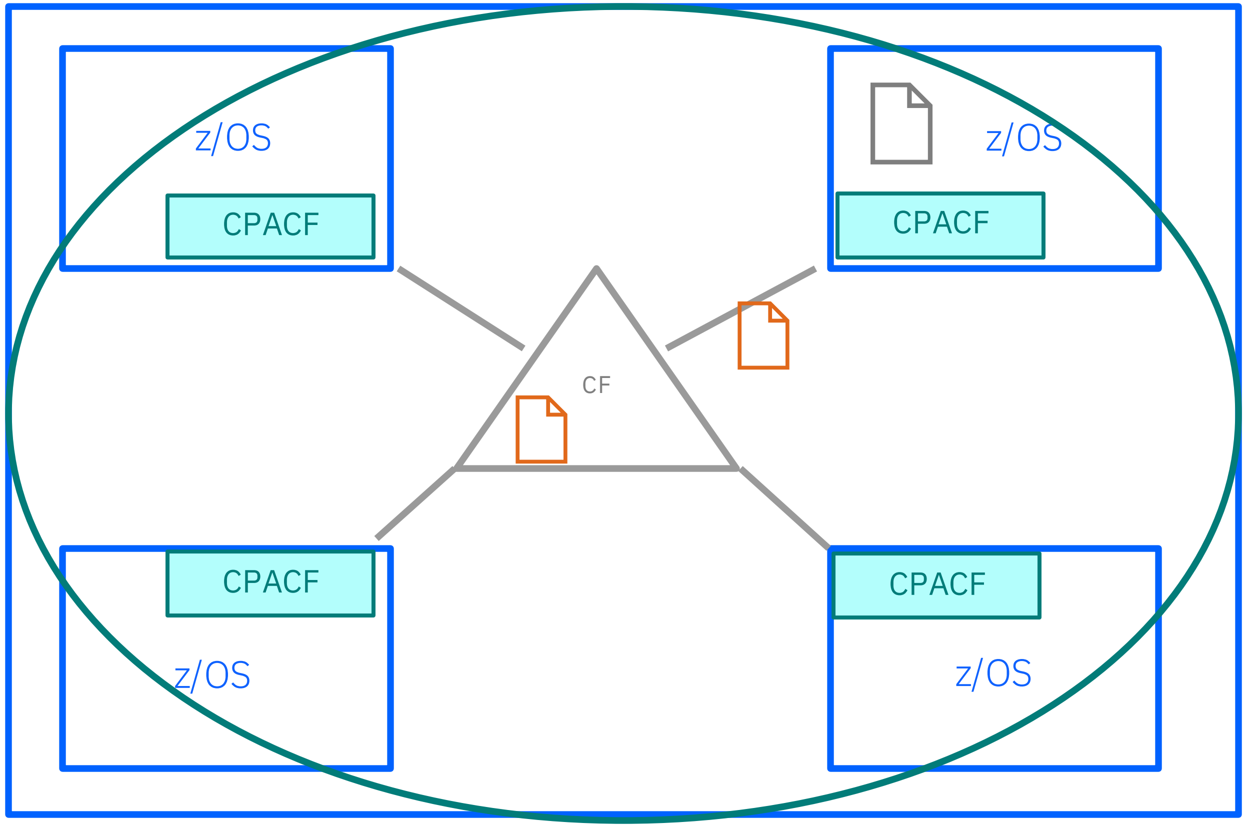
DFSMS will respond to the presence of the **key label**, check the user's access to **CSFKEYS**, and interact with ICSF for the associated protected key.

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

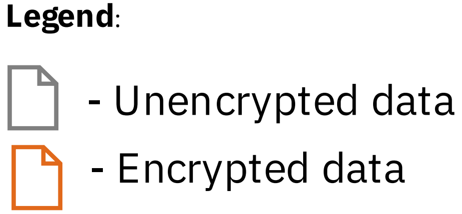
Coupling Facility Encryption

- Host encryption via CPACF as data is written to or read from disk
- Data encrypted in the host and remains encrypted until decrypted by the host
- List & Cache structures only
- No application enablement required

Protection of data in-flight and in-use

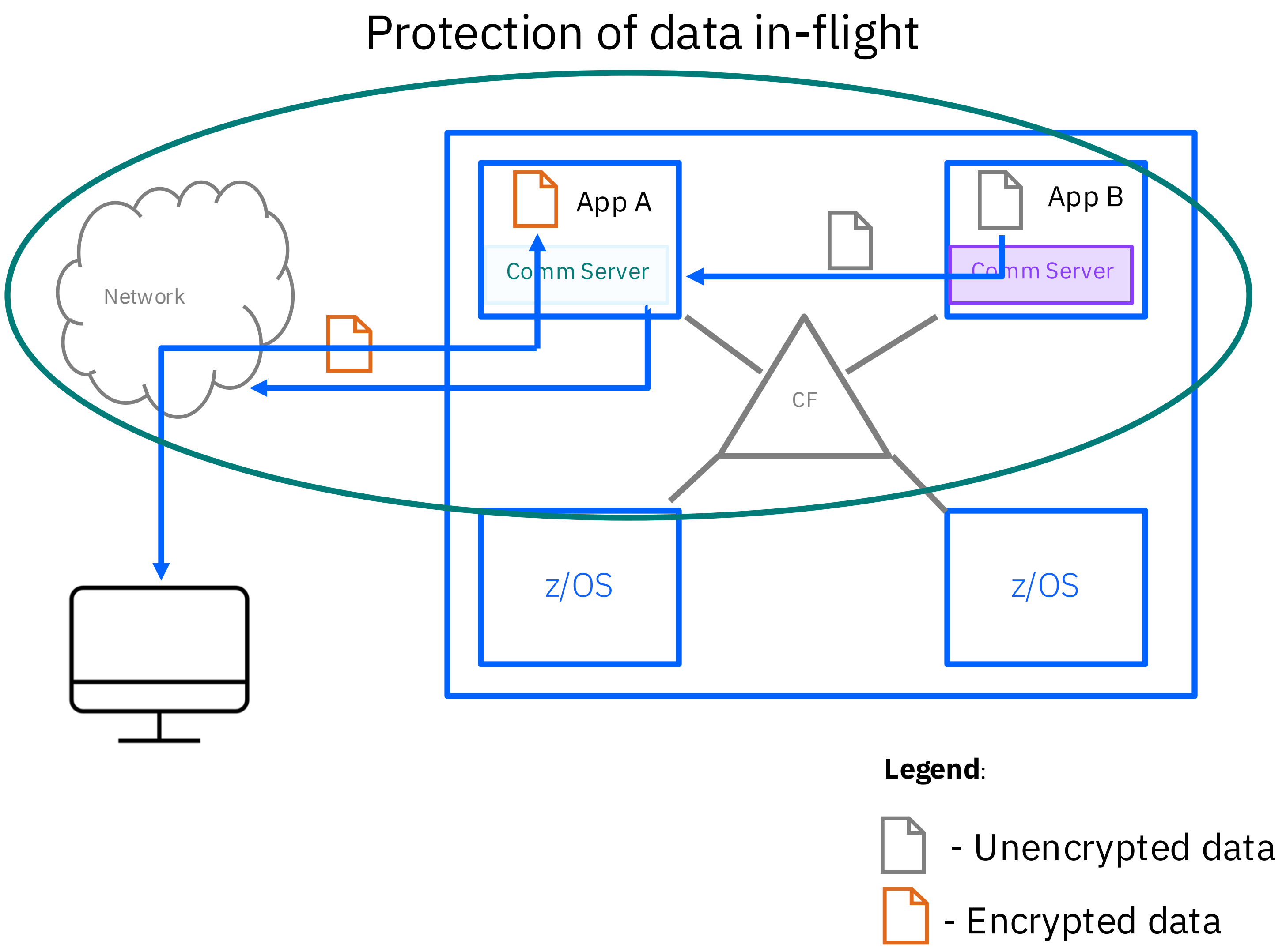


z/OS Parallel Sysplex cluster



z/OS Network Security

z/OS Encryption Readiness Technology (zERT) can help determine when network traffic meets specified policy with discovery and reporting capabilities.



zERT features

zERT Discovery

- SMF 119 subtype 11 "zERT Connection Detail" records
- These records describe the complete cryptographic protection history of each TCP and EE connection
- At least one record is written for each connection - and each describes all cryptographic protection for that connection
- Well suited for real-time monitoring applications
- Depending on your z/OS network traffic, these could be generated in very high volumes

zERT Network Analyzer

- Web-based (z/OSMF) UI to query and analyze zERT Summary (subtype 12) records
- The latest network analyzer PTF always contains an up-to-date fresh install image
- Intended for z/OS network security administrators (typically systems programmers)
- Comes with Communications Server at no extra charge, but relies on Db2 for z/OS

zERT Aggregation

- SMF 119 subtype 12 "zERT Summary" records
- These records describe the repeated use of security sessions over time
- Writes one zERT Summary record at the end of each recording interval for each
  security session active during the interval
- Well suited for reporting and analysis
- Can greatly reduce the volume of SMF records (over Discovery) while providing the same level of cryptographic detail

zERT Policy-Based Enforcement

- Real-time monitoring based on user-written policy rules
- Directs the TCP/IP stack to take specific actions when a user-defined security policy is or is not met for a new TCP connection
- Notification and defensive actions supported

z/OS Data Set Encryption Enhancements

Available Function

Data Set Type	Availability	Description
VSAM extended format data set encryption	3Q 2017	Support VSAM (KSDS, ESDS, RRDS, VRRDS, LDS) extended format Support transparent VSAM and VSAM/RLS access KSDS may be compressed format
Sequential extended format data set encryption	3Q 2017	Support sequential extended format Support transparent BSAM/QSAM access May be compressed format (Generic, Tailored, zEDC)
zFS encryption	3Q 2017	Support for zFS file system data as encrypted and compressed.
PDSE encryption	3Q 2019	Support data PDSEs (data members only) Support transparent BSAM/QSAM/BPAM access Data pages and directory pages are encrypted Must be SMS-managed New resource in FACILITY class to allow support
JES2 spool	2Q 2020	Support the encryption of instream and SYSOUT data sets on SPOOL.
Basic and Large format sequential data set encryption	4Q 2020	Support DASD data sets that cannot be extended format Support transparent BSAM/QSAM access Support EXCP access, requiring changes to application. New API for EXCP callers. Must be SMS-managed New resource in FACILITY class to allow support

z/OS Data Set Encryption Enhancements

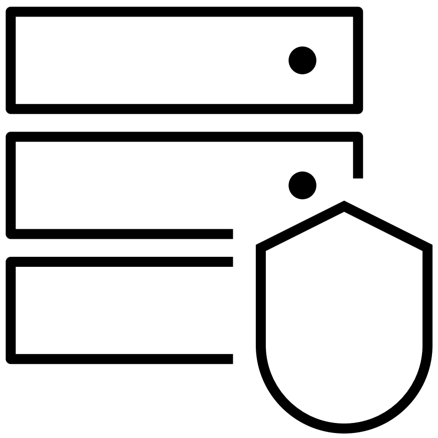
Available Function - continued

Supported Data Set Types / Functions	Availability	Description
PDSE zEDC compression	3Q 2021 [V2.5 w/ rollback to V2.3, V2.4]	Allow encrypted PDSEs to be compressed by access methods
ICSF Archived Key	3Q 2021 [V2.5]	Support archived keys designated as decrypt only Supported for VSAM and sequential extended format, PDSE, Basic and large format
RACF DB Encryption	2Q 2022 [V2.5]	Support for Encrypted VSAM DB in RACF
ICSF AES CIPHER Key panels	3Q 2023 [3.1 only]	Allows simplified generation of new AES CIPHER keys for use in Data Set Encryption

Statement of Direction: Tape Data Set Encryption

“IBM intends to enhance pervasive encryption to perform encryption within the access methods for **tape data sets**. It is expected to be transparent to the application program unless it uses EXCP. This new data set encryption support is intended to be independent of any encryption that occurs in the tape subsystem.”

https://www.ibm.com/docs/en/announcements/zos-v25-2q-2022-enhancements?region=US#sodx__title__1



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

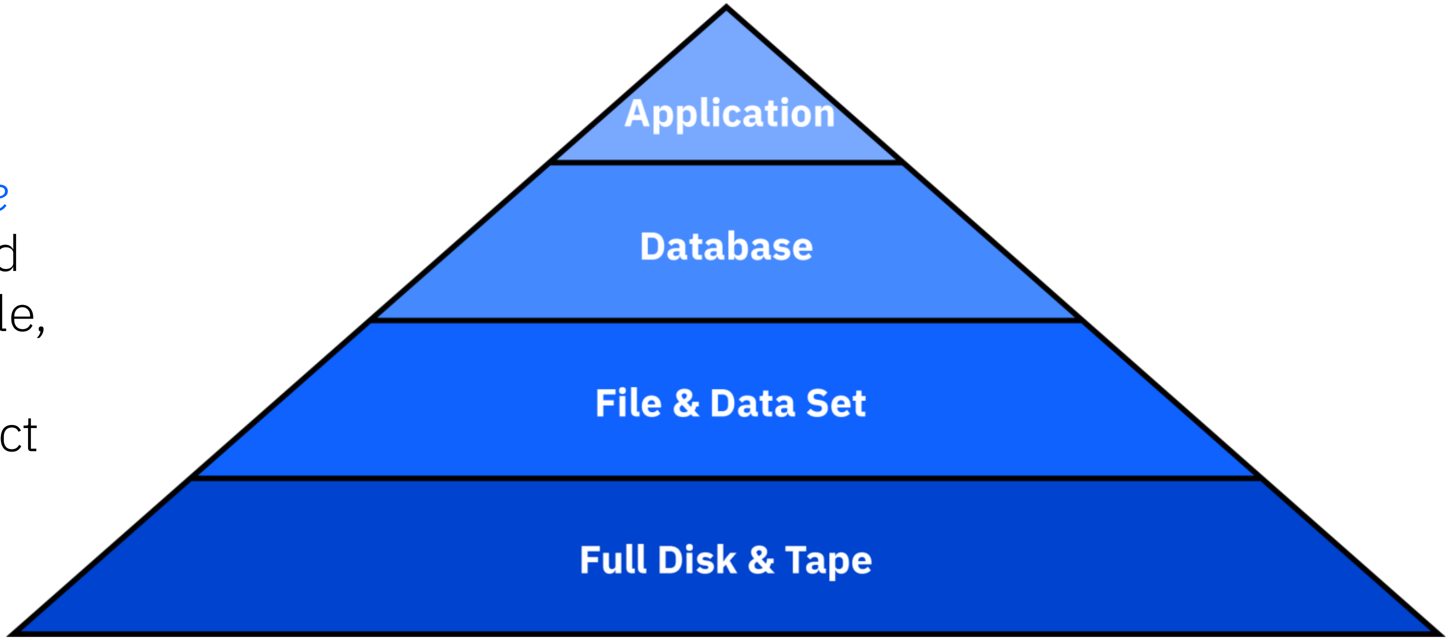
This Quantum-Safe journey is a natural continuation of Pervasive Encryption

Payment Card Industry Data Security Standard

Version 4.0, Requirement 3.5.1.2

Is disk encryption enough?

"While disk encryption may still be present on these types of devices, it *cannot be the only mechanism used to protect PAN stored on those systems*. Any stored PAN must also be rendered unreadable per Requirement 3.5.1—for example, through truncation or a data-level encryption mechanism. Full disk encryption helps to protect data in the event of physical loss of a disk and therefore its use is appropriate only for removable electronic media storage devices."

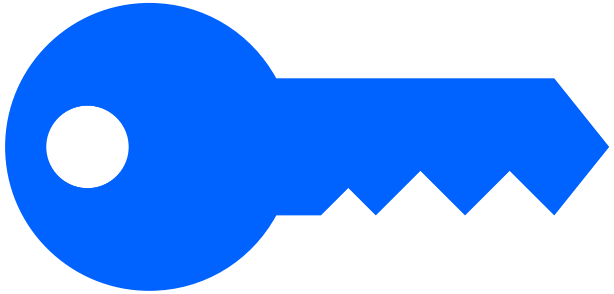


"This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment."

Master vs Operational keys

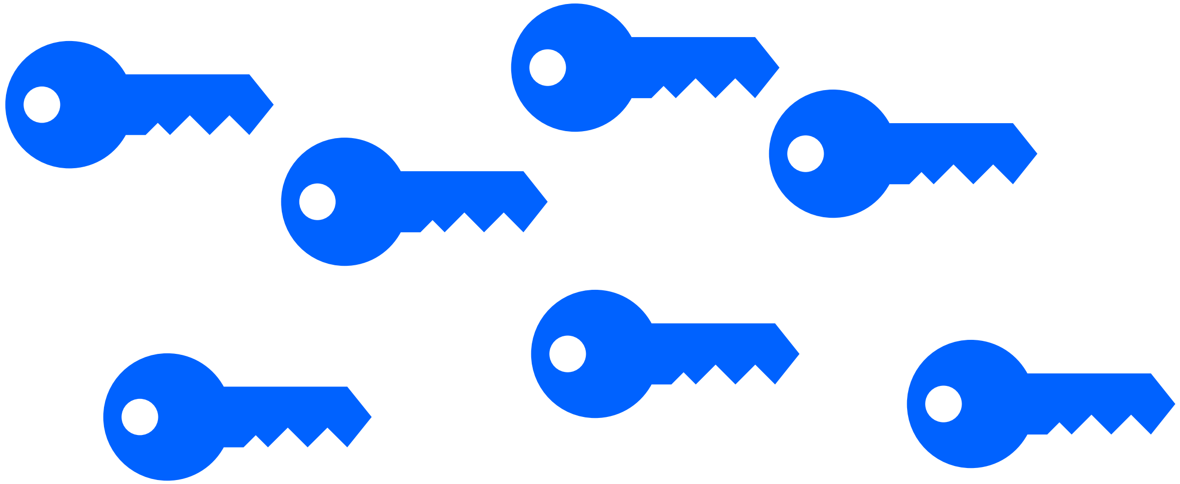
Master Keys

- Master keys are used only to encipher and decipher keys
- Master keys are stored in secure, tamper responding hardware
- Master keys should be changed periodically



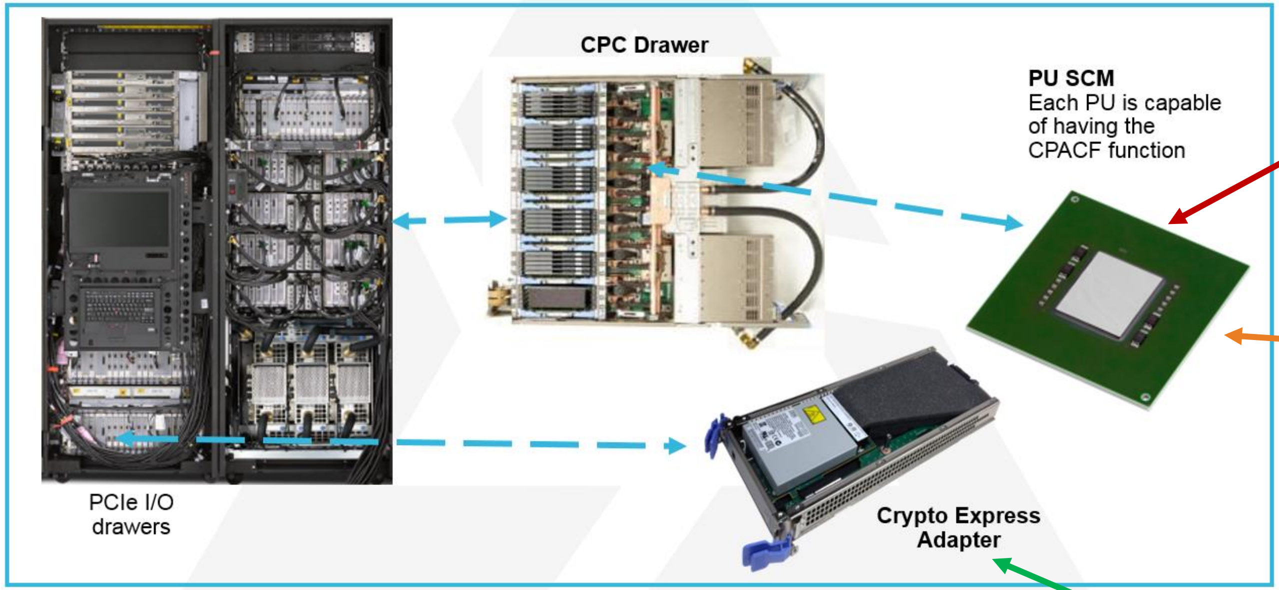
Operational Keys

- Operational keys are used in various cryptographic operations (e.g. encryption).
- Operational keys may be stored in a key store (e.g. data set, file, database) or returned back to the calling application.
- Operational keys encrypted by a master key are considered secure keys



Protecting Operational Keys: Using Secure & Protected Keys

Operational keys should not be stored in the clear in the host environment. Secure keys are strongly recommended for persistent key storage (e.g. key data sets). Protected keys are recommended for storing keys in address space memory (e.g. Db2, DFSMS).



High speed

Clear Key

Key values are not encrypted. Crypto operations may be performed in CPACF or on a Crypto Express adapter

Speed & Security Hybrid

Protected Key

Key values are encrypted under a CPACF wrapping key. Crypto operations are performed only using CPACF

High security

Secure Key

Key values are encrypted under a Master Key. Crypto operations are performed only on a Crypto Express adapter

Note: With z/OS data set encryption, protected keys are implicitly created from secure keys.

Only protected keys created from secure keys should be used for Pervasive Encryption.

IBM Z Operational Keys: Explaining Clear, Protected, Secure

- Clear Keys are not encrypted. **Crypto operations may be performed in CPACF or on a Crypto Express adapter**
- Protected keys are encrypted under a CPACF wrapping key. **Crypto operations are performed only using CPACF**
- Secure keys have key values that are encrypted by a Master Key on a tamper-responding **Crypto Express adapter.**

Key Type	**Located In…**	**Protected by…**
Clear Key	Guest Memory or key store	Security Policy only

Key Type	**Located In…**	**Protected by…**
Protected Key	Guest memory, encrypted	An LPAR-specific key, and machine instructions

Key Type	**Located On…**	**Protected by…**
Secure Key	Guest memory or Key store, encrypted	A Master Key in a Hardware Security Module (HSM) on your Crypto Express Adapter

Key Rotation

Master Key Rotation

Master key rotation involves re-enciphering secure, operational keys that reside in Key Data Sets. Re-encipherment occurs in the secure boundary of the Crypto Express adapter. ICSF synchronizes the changes across members of the sysplex sharing the same Key Data Set (when applicable).

For each secure key:

- The operational key value is decrypted from under the current Master Key
- The operational key value is encrypted with the new Master Key

After all secure keys have been re-enciphered:

- The current Master Key becomes the old Master Key
- The new Master Key becomes the current Master Key

Using Coordinated Change MK, the master key rotation is non-disruptive. Master keys can be rotated while crypto workloads are running.

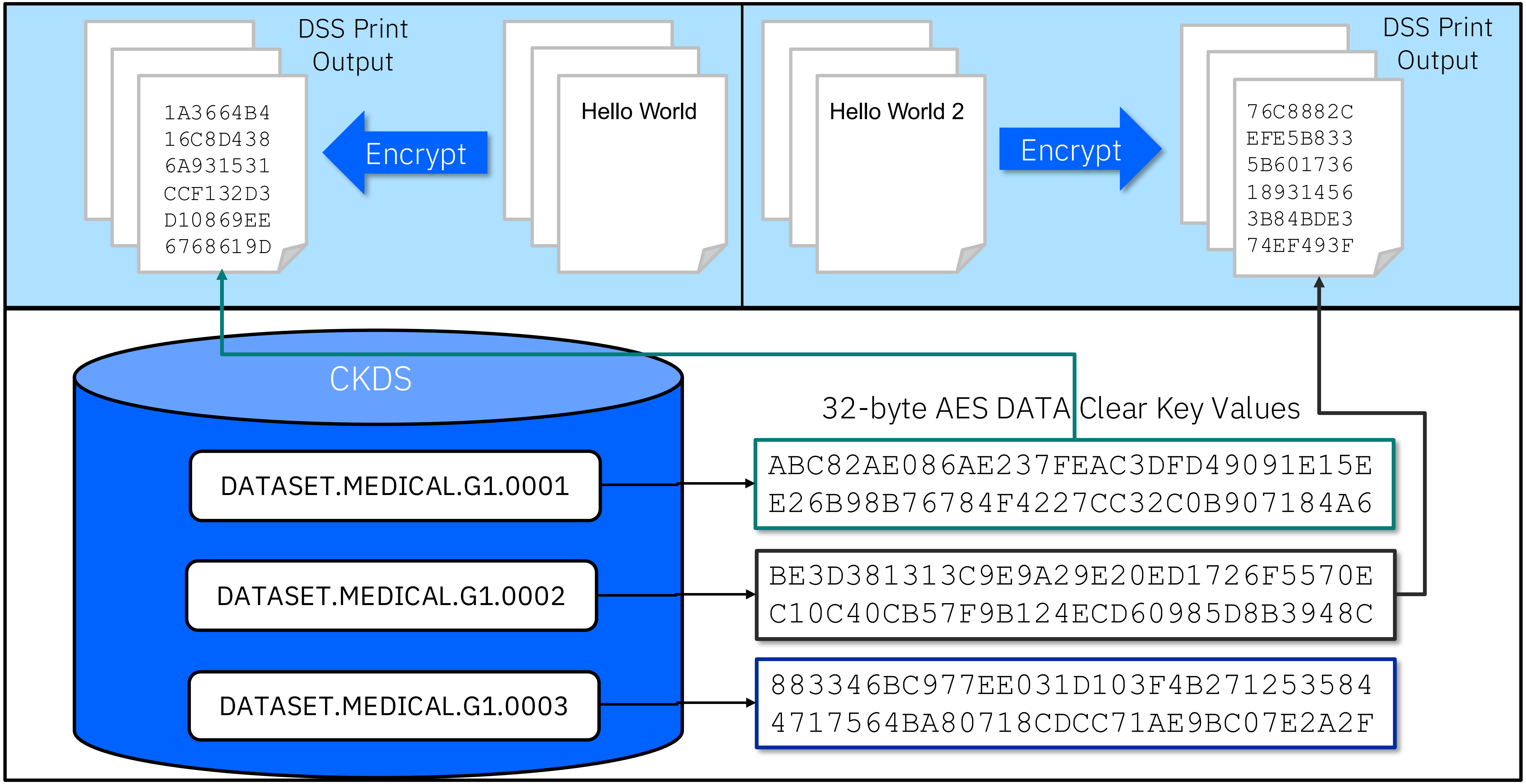
Note: The TKE is the most secure method for managing master keys

Considerations For Rotating Operational Keys

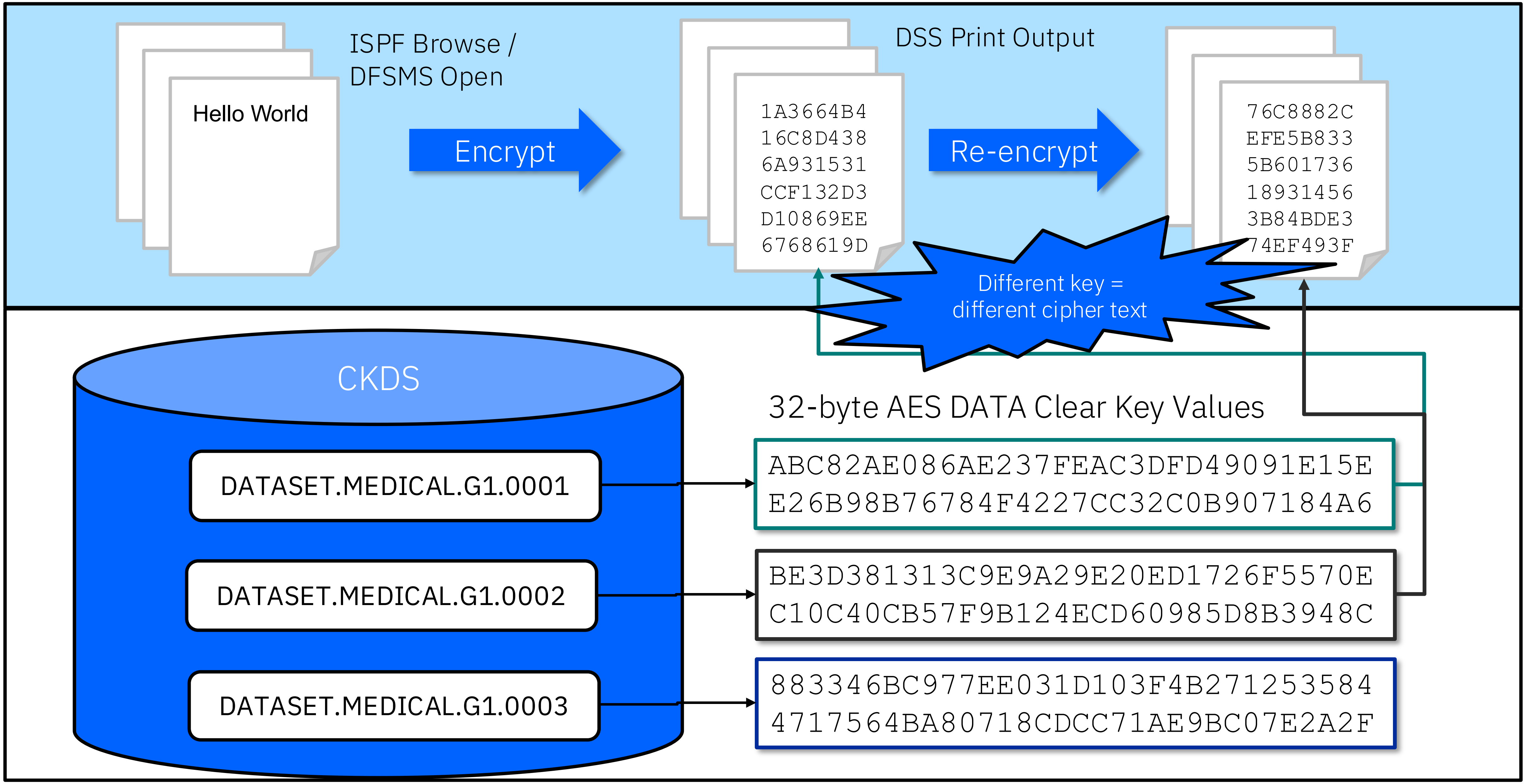
- Aging Out encrypts new data with new keys after a pre-defined period of time
  - Pros: Non-disruptive
  - Cons: More keys to manage, not sufficient when a key is compromised, only affects new data
- Re-encryption encrypts all data with new keys after a pre-defined period of time or an operational key compromise
  - Pros: Effective when a key is compromised, affects new and old data
  - Cons: Disruptive (except Db2 online reorg), must identify all data encrypted with the old key

Note: Key versioning is recommended. Old keys should be deactivated (or archived) rather than deleted.

Aging Out encrypts new data with new keys



Re-encryption encrypts all data with new keys



Naming convention example

Key label example:

DATASET.<data_set_resource>.ENCRKEY.<seqno>

CSFKEYS profile:

RDEFINE CSFKEYS DATASET. <data_set_resource>.ENCRKEY.* UACC(NONE)

The sequence number at the end facilitates key rotation

- A new key will be provisioned, requiring a new key label
- Generics used in the CSFKEYS profile means that profile doesn't change
- The DATASET profile(s) are updated with that new key label for future allocations

Why perform key rotation?

What is a Cryptoperiod?

Payment Card Industry Data Security Standard

Version 4.0, Requirement 3.7.4

- A cryptoperiod is the time span during which a cryptographic key can be used for its defined purpose.
- Cryptoperiods are often defined in terms of the period for which the key is active and/or the amount of cipher-text that has been produced by the key.
- Considerations for defining the cryptoperiod include, but are not limited to, the strength of the underlying algorithm, size or length of the key, risk of key compromise, and the sensitivity of the data being encrypted.

U.S. National Institute of Standards & Technology

Special Publication 800-57, Revision 5, Section 5.3

A cryptoperiod is the time span during which a specific key is authorized for use by legitimate entities or the keys for a given system will remain in effect.

The consequences of exposure are measured by:

- Sensitivity of the information
- Criticality of the processes protected by the cryptography
- Cost of recovery from the compromise of the information or processes

Sensitivity refers to:

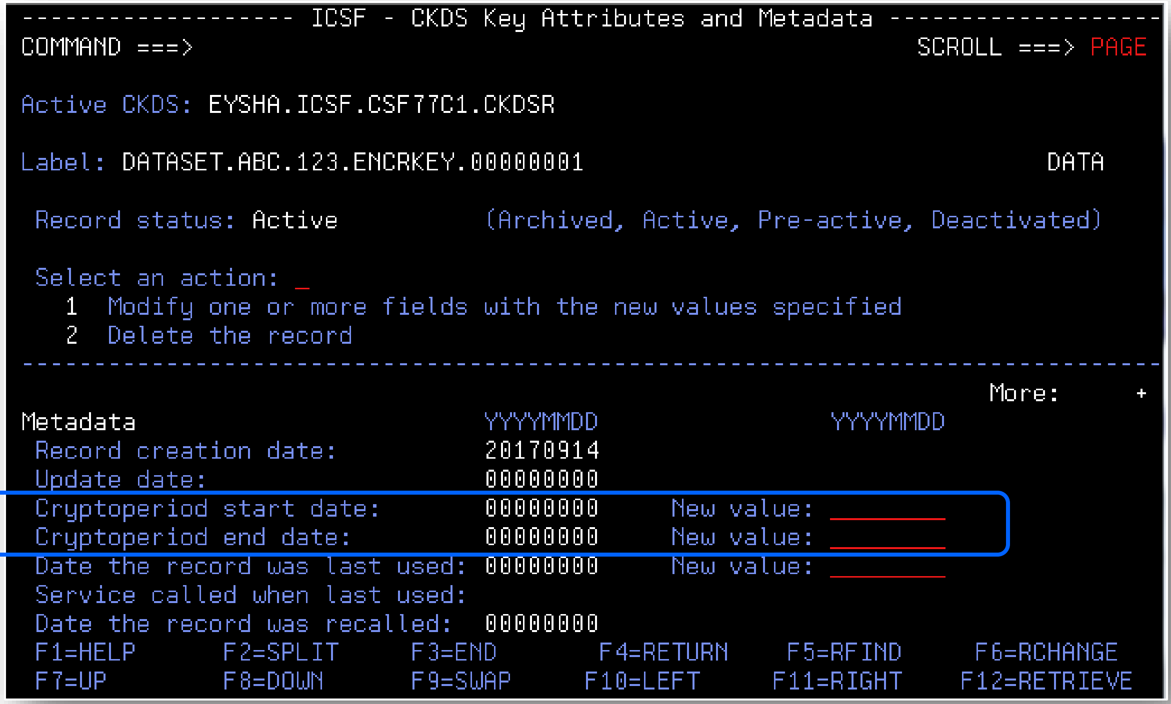
- Lifespan of the information being protected (e.g., 10 minutes, 10 days, or 10 years) and
- Potential consequences of a loss of protection for that information (e.g., the disclosure of the information to unauthorized entities).

Enforcing Cryptoperiods

z/OS ICSF supports the ability to specify a cryptoperiod for a key stored in a Key Data Set in KDSR or KDSRL common record format. The ICSF administrator can specify the crypto-period start and end dates and ICSF will allow only the key material to be used by applications within those dates.

1. Key validity start and end dates can be set using the CKDS KEYS panel utility (for ICSF releases HCR77C1 or later) or programmatically using the Metadata Write (CSFKDMW) callable service.
   - The date cannot be set to a date in the past
2. When an application attempts to use an inactive key
   - ICSF writes an SMF type 82 record indicating attempted key use
   - ICSF fails the request

To reactivate an expired key, the key validity date must be set to a future date.



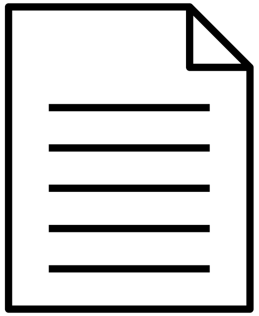
U.S. National Institute of Standards & Technology

Special Publication 800-57, Revision 5, Section 5.3

Among the factors affecting the length of a cryptoperiod are:

1. The strength of the cryptographic mechanisms (e.g., the algorithm, key length, block size, and mode of operation);
2. Personnel turnover (e.g., of system administrators and CA system personnel);
3. The threat to the information from new and disruptive technologies (e.g., quantum computers).
4. The security life of the data.
5. The number of copies of a key and the distribution of those copies;

And many more.....



https://doi.org/10.6028/NIST.SP.800-57pt1r5

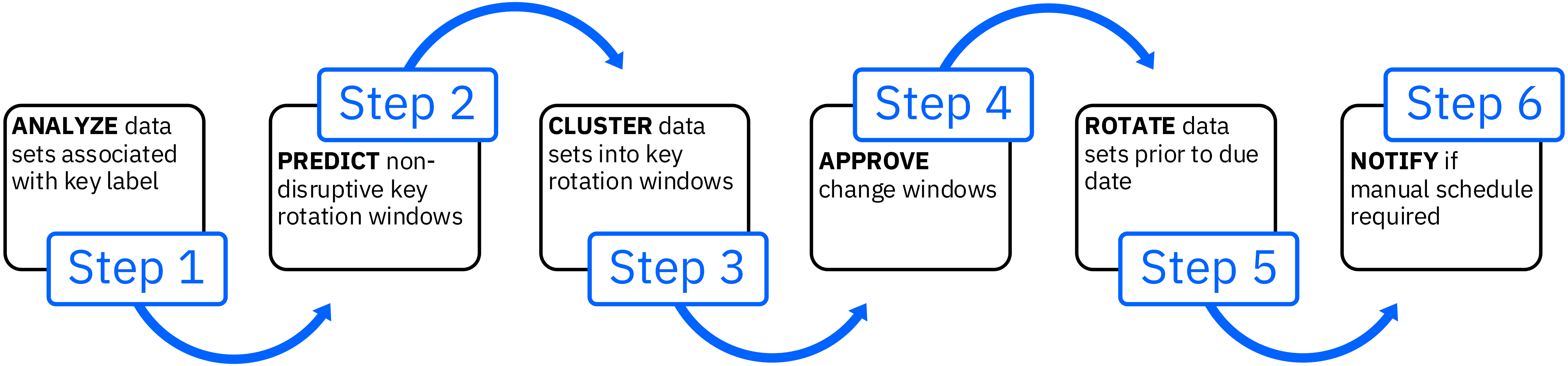
Data set key rotation simplification

As-Is Scenario
Summary

- Pain Point 1: z/OS data set key rotation requires a scheduled outage for most applications.
- Pain Point 2: It can be difficult to determine data sets' associations with applications.
- Pain Point 3: z/OS data set key rotation is largely a manual effort.

To-be Scenario: Data Set Key Rotation

powered by data set analytics



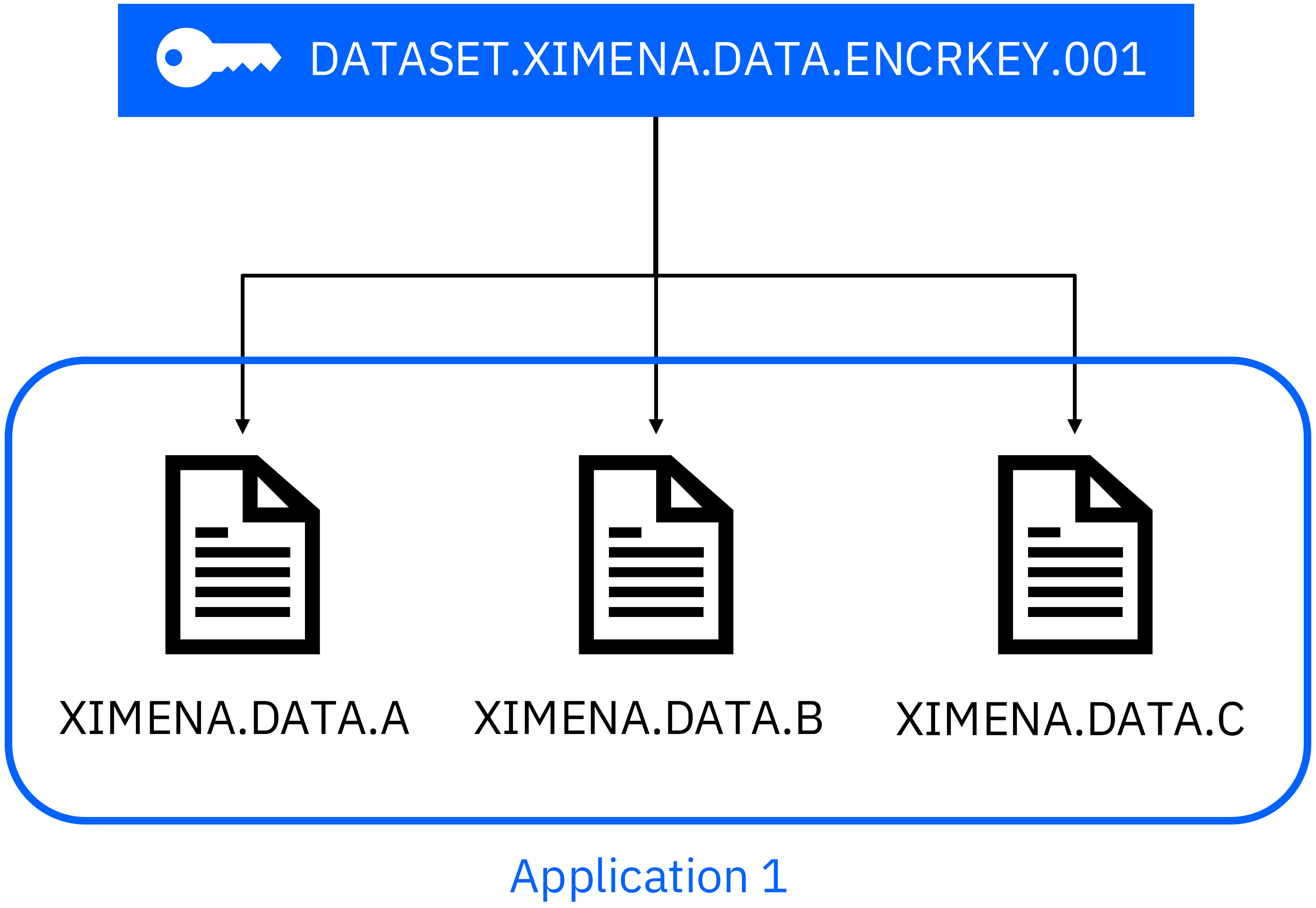
Analyze Data Sets

Pattern 1: Single key, single application

Every encrypted data set has an associated key label.

The analytics engine:

- locates all data sets matching the specified key label
- analyzes data set availability over time determining when data sets are typically open or closed



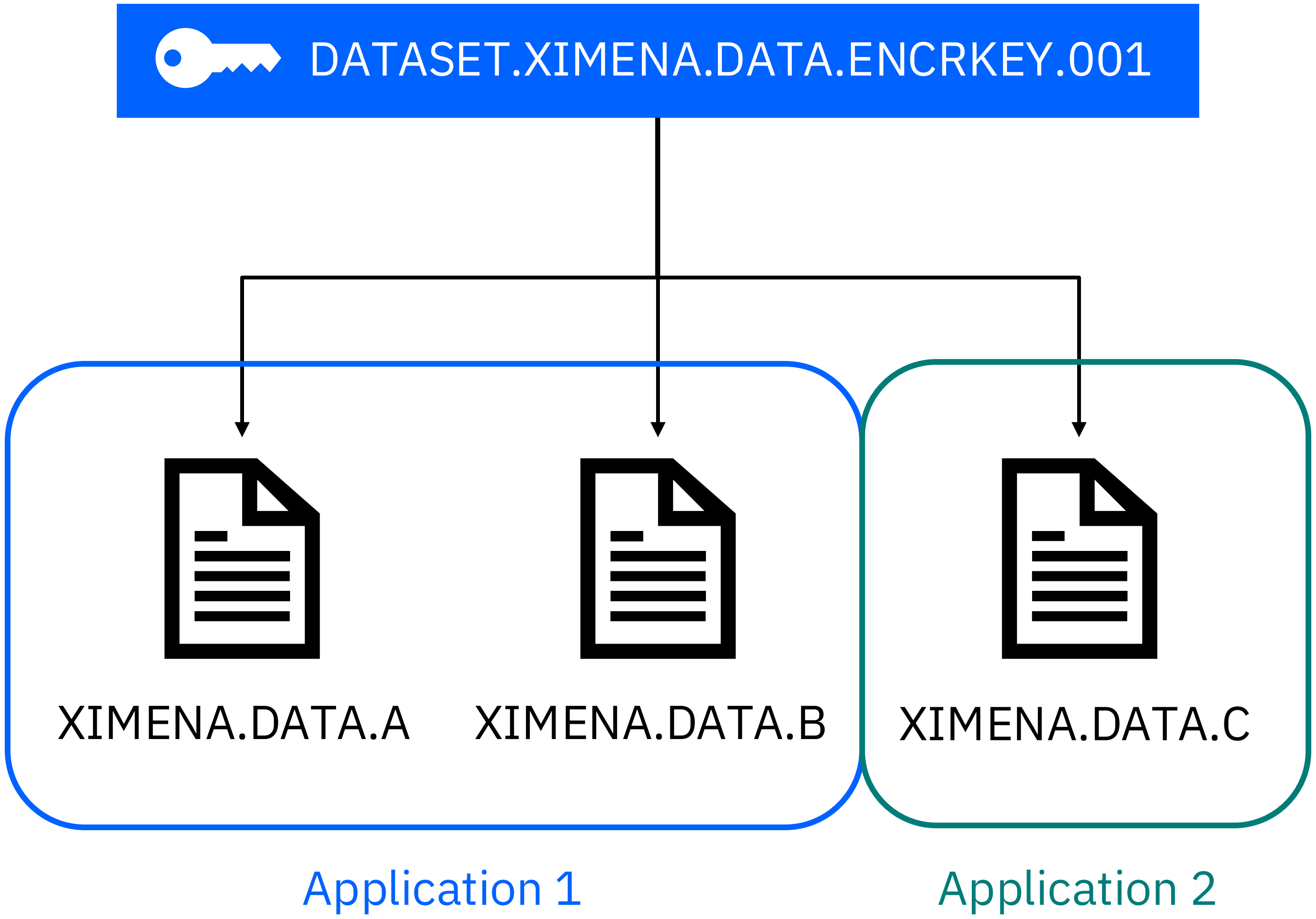
Analyze Data Sets

Pattern 2: Single key, multiple applications

Every encrypted data set has an associated key label.

The analytics engine:

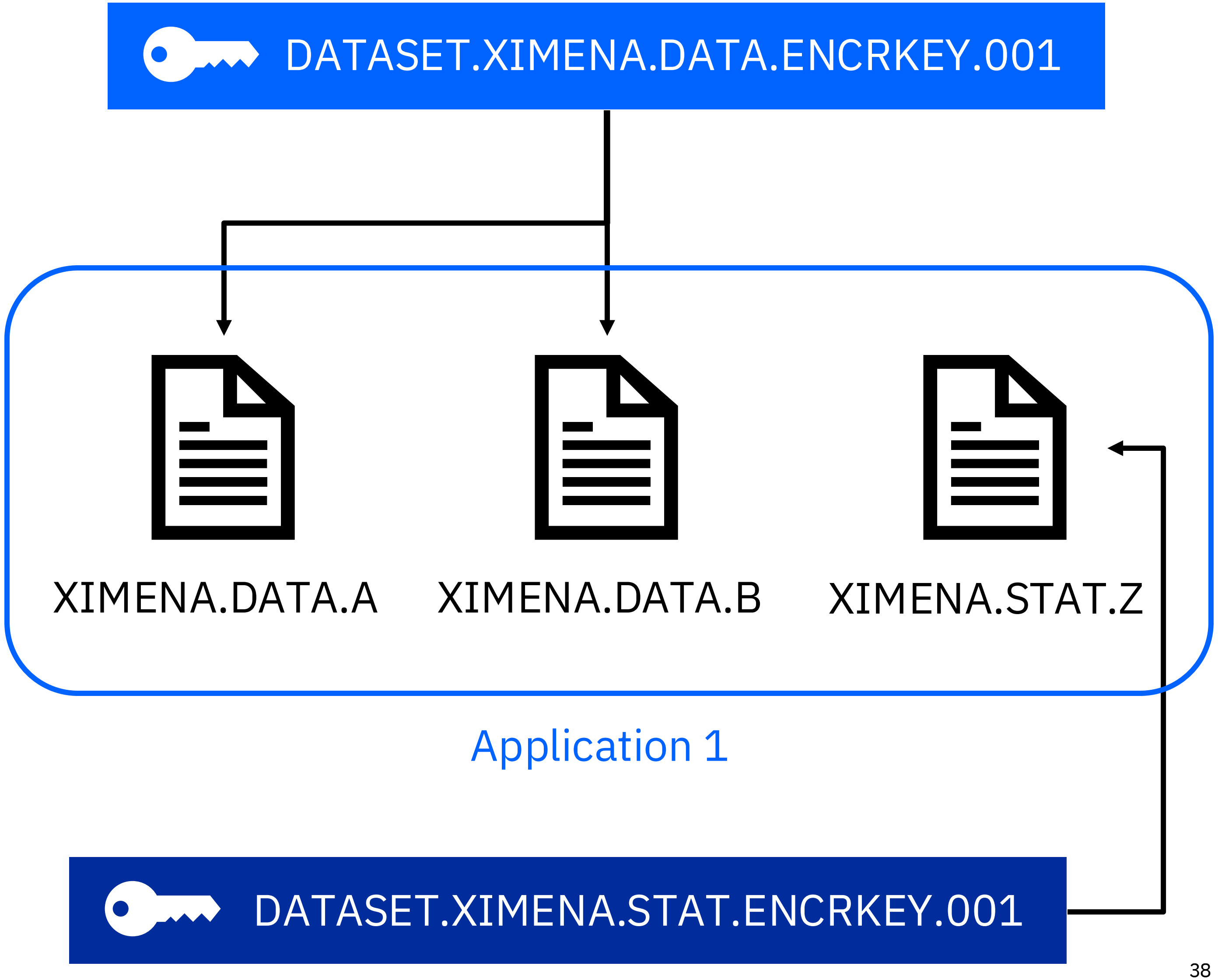
- locates all data sets matching the specified key label
- analyzes data set availability over time determining when data sets are typically open or closed



Analyze Data Sets

Pattern 3: Single application, multiple keys

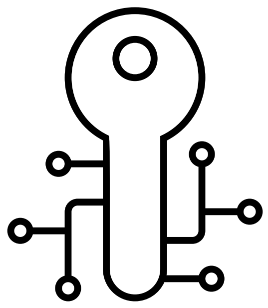
Every encrypted data set has an associated key label.



Statement of Direction: Data Set Key Rotation

IBM also plans to provide a software solution that **simplifies z/OS data set encryption**, encrypting and re-encrypting data at scale for both key rotation and initial encryption, and leveraging analytics to **minimize application downtime.** This is designed to simplify adherence to expanded compliance regulations such as PCI DSS v4.0.

https://www.ibm.com/docs/en/announcements/statement-direction-security-zos



Resources

”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/redbooks/pdfs/sg248410.pdf

Redbooks

Questions?

Thank You