IBM z Systems

z/OS Pervasive Encryption
- Data Set Encryption

Agenda

- Pervasive Encryption: Role of z/OS data set encryption
- Db2 z/OS exploitation
- Considerations
- Implementation
- Resources

Data protection and compliance are business imperatives

"It's no longer a matter of if, but when …"

26%

Likelihood of an organization having a data breach in the next 24 months [1]

European Union General Data Protection Regulation (GDPR)

Payment Card Industry Data Security Standard (PCI-DSS)

Of the **9 Billion** records breached since 2013 only **4%** were encrypted [3]

$4M

Average cost of a data breach in 2016 [2]

Health Insurance Portability and Accountability Act (HIPAA)

1, 2 Source: 2016 Ponemon Cost of Data Breach Study: Global Analysis -- http://www.ibm.com/security/data-breach/
3 Source: Breach Level Index -- http://breachlevelindex.com/

z/OS Data Set Encryption

Statement of Direction

https://www.ibm.com/common/ssi/rep_ca/2/897/ENUS216-392/ENUS216-392.PDF

IBM z/OS V2R3 Preview

*"z/OS V2.3 plans to replace application development efforts with **transparent, policy-based data set encryption**:*

- ***Planning enhanced data protection for z/OS data sets**, zFS file systems, and Coupling Facility structures **to give users the ability to encrypt data without needing to make costly application program changes."***

Preview IBM z/OS V2R3 United States Software Announcement 217-085, dated February 21, 2017

IBM z/OS V2R3

IBM z/OS V2R3 Europe Software Announcement ZP17-0316, dated July 17, 2017

August 7, 2017 : z/OS V2.2 Data Set Encryption is now available!!

- **Provides full function on V2.2; Coexistence on z/OS V2.1**
  (Can access encrypted data sets, but cannot create new encrypted data sets)

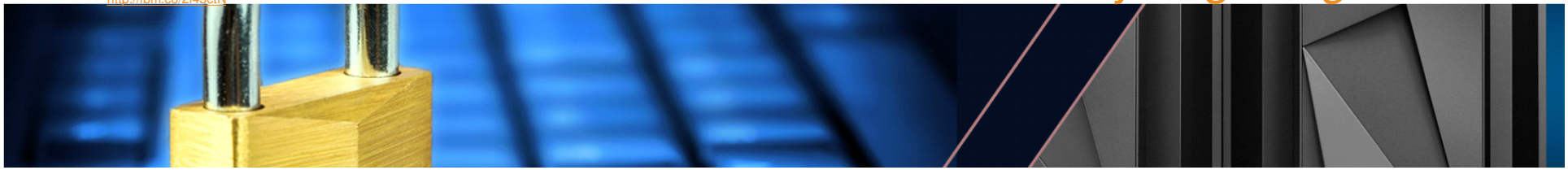
Pervasive Encryption with IBM z Systems

Enabled through full-stack platform integration

Integrated Crypto Hardware	Hardware accelerated encryption on every core – z14 CPACF performance improvements of up to 7x Next Gen Crypto Express6S – up to 2x faster than prior generation
Data at Rest	Broadly protect Linux® file systems and z/OS data sets[1] using policy controlled encryption that is transparent to applications and databases
Clustering	Protect z/OS Coupling Facility[2] data end-to-end, using encryption that's transparent to applications; requires z/OS V2.3
Network	Protect network traffic using standards based encryption from end to end, including encryption readiness technology[2] to ensure that z/OS V2.3 systems meet approved encryption criteria
Secure Service Container	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 Enterprise Key Management Foundation (EKMF) provides real-time, centralized secure management of keys and certificates with a variety of cryptographic devices and key stores.

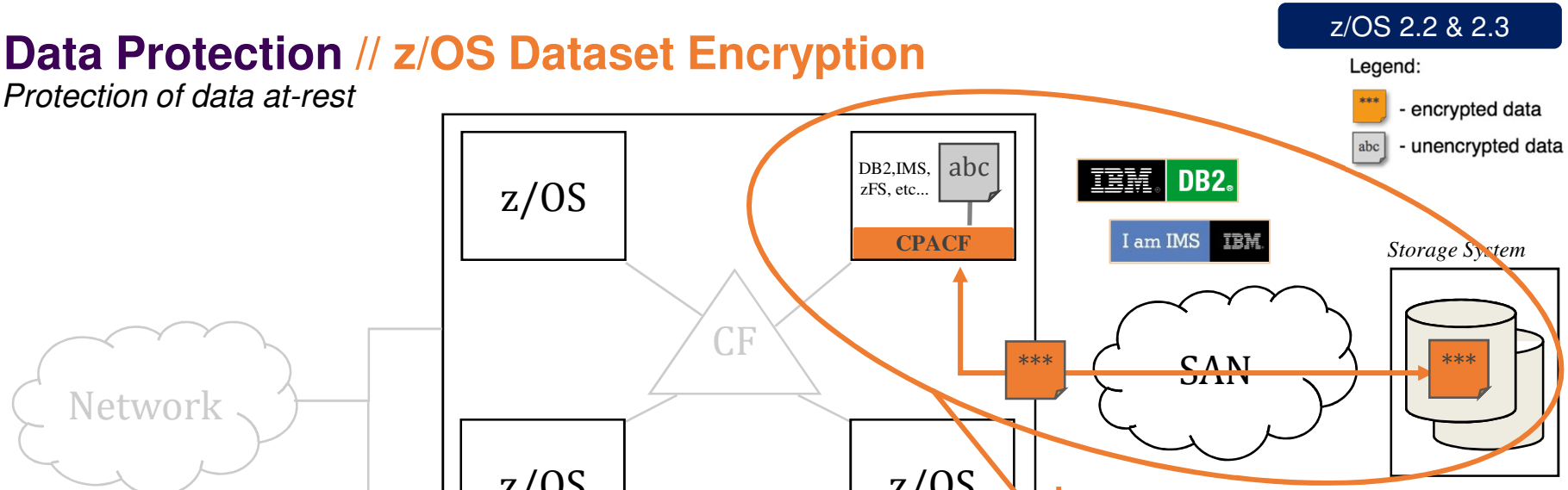
1 Statement of Direction* in the z/OS Announcement Letter (10/4/2016) - http://ibm.co/2ldwKoC
2 IBM z/OS Version 2 Release 3 Preview Announcement Letter (2/21/2017) - http://ibm.co/2l43ctN

And we're just getting started …



Data Protection // z/OS Dataset Encryption

Protection of data at-rest



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

z/OS Dataset Encryption:

- Application transparent & enabled by policy
- Encryption tied to fine grained access control
- Host encryption via CPACF as data written-to or read-from disk.
- Supports ext. format sequential & VSAM
- Includes HSM & DSS migration/backup of encrypted data sets
- Replicated data remains encrypted
- Supports: CICS®, DB2, IMS, Logger, & zFS

In-memory system or application data buffers will not be encrypted

z/OS Data Set Encryption – Customer Value

*Clients who are required to protect customer data can leverage the z Systems hardware encryption for **data at rest** through existing **policy management**… **without application changes.***

1. – **No application changes required**
2. – **Data set level granularity**
3. – **Supports separation of access control for data set and encryption key label**
4. – **Enabled through RACF and / or SMS policy and / or Db2 V12 DDL**
5. – **Audit readiness**

Key label: *64-byte label of an existing key in the ICSF CKDS used for access method encryption/decryption.*
Encryption type: *AES-256 bit key (XTS, protected key). Note: AES-256 key must be generated as a secure key (i.e. protected by crypto express AES Master Key)*

Designed to take advantage of the processing power of the z14

Application transparency via access methods

Supported access methods/data set types

Covers DB2, IMS, zFS, Middleware, Logs, Batch, & ISV Solutions[1]

- **BSAM/QSAM**
  - **Sequential data sets**
    - Extended format only
      - **Data class DSNTYPE=EXTR or EXTP; JCL DSNTYPE=EXTREQ or EXTPREF**
- **VSAM and VSAM/RLS**
  - **KSDS, ESDS, RRDS, VRRDS, LDS**
    - Extended format only
      - **Data class DSNTYPE=EXTR or EXTP; JCL DSNTYPE=EXTREQ or EXTPREF**

No application changes or awareness that sequential or VSAM data is encrypted when accessed using the standard access method APIs.

Data encrypted/decrypted only when accessed via supported access methods.

- *Data encryption/decryption as data is written to or read from disk …centralized within Media Manager*
- *In-memory system or application data buffers remain in the clear*
- *Data remains encrypted during backup/recover, migration/recall, and replication*

1 Any applications or middleware making use of VSAM, QSAM, BSAM access methods. Refer to individual product documentation to confirm support of z/OS data set encryption.

For those applications that use the licensed Media Manager services, changes to Media Manager interfaces required to access encrypted data sets.

Resources: Sample execs, JCL

IBM z Systems

Developed by Eysha Powers

IBM

You are in: IBM Crypto Education Wiki > Pervasive Encryption - zOS Data Set Encryption

Pervasive Encryption - zOS Data Set Encryption

| Updated yesterday at 9:56 AM by Eysha Shirrine | Tags: aes, aes_mk, cex5s, ckds, dataset, dfsms, icsf, pervasive_encryption, racf, saf, secure

Page Actions

z/OS Data Set Encryption

Hardware and Operating System Support

Product/Feature	Required Level	Description
Hardware		
Minimum HW	z196 CPACF	Minimum HW for AES-XTS (MSA-4)
	Crypto Express3	Minimum HW for Secure-key/Protected-key CPACF[1]
Recommended HW	z14 CPACF	AES-XTS CPACF performance improvements
	z14 Crypto Express6s	Crypto express performance improvements
Operating System – Base Support		
DFSMS	z/OS 2.3	Full support
	z/OS 2.2 + OA50569 PTFs	
	z/OS 2.1 + OA50569 PTFs	*Toleration only –read/write, cannot create encrypted data sets.*
RACF	z/OS 2.3	DFP segment key label and conditional access checking
	z/OS 2.1, 2.2 + OA50512 PTFs	
ICSF	HCR77C0 or HCR77C1	Protected-Key Read
	HCR77A0–B1 + OA50450 PTFs	

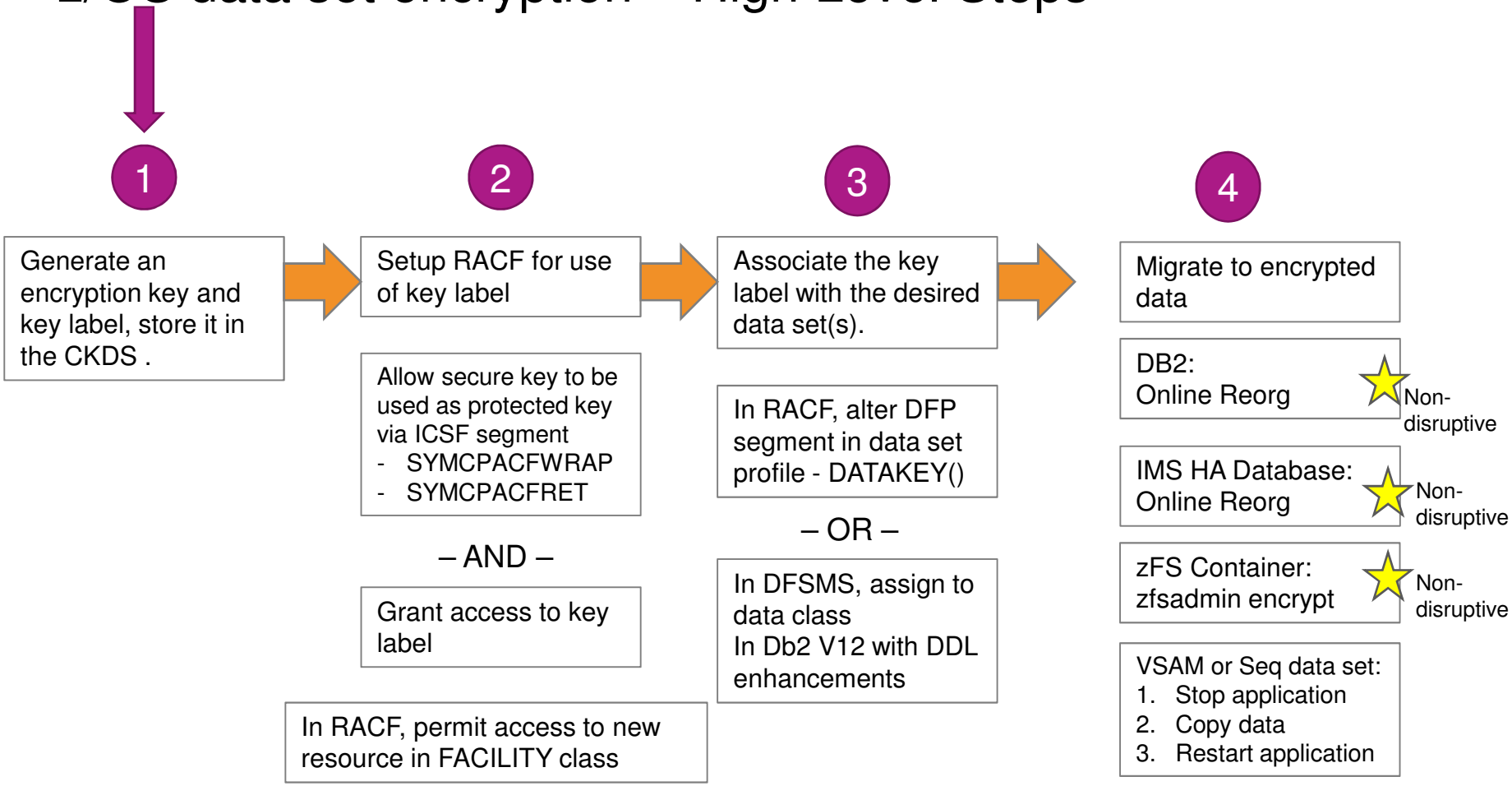
[1] – *Secure-key is STRONGLY RECOMMENDED for production environments. Clear-key may be used for dev/test.*

z/OS Data Set Encryption

Exploitation

Product/Feature	Required Level	Description
	Software Exploitation	
DB2	DB2 v12 + PI81907	Base exploitation + database administration enablement for V12@FL50x
	DB2 v11 + PI81900	Base exploitation
IMS	IMS v14	FF VSAM DB & OLDS - *test only no code changes expected*
	IMS v15	FP DEDB VSAM & WADS enablement support
CICS	*Supported CICS versions*	Test-only for user, CICS TS, and TD data sets
MQ	*NA*	*Recommendation for MQ - Advanced Message Security*
zSecure	zSecure 2.3	zSecure Audit & Admin support for z/OS data set encryption
zBNA	zBNA x.y.z	zBatch Network Analyzer support for z/OS data set encryption
	z/OS Exploitation	
zFS	z/OS 2.3	User Interface & data conversion support
System Logger	z/OS 2.3 w/RB 2.2 & 2.1	Media Manager enablement for logger data sets

z/OS data set encryption – High Level Steps



https://www.youtube.com/watch?v=g4A6zaq1HNQ

2a Prepare for access method access to ICSF CKDS Key provisioning service

Setup security policy for key provisioning

- **Security Admin** must update the ICSF segment of the covering profile
  - Set SYMCPACFWRAP(YES), SYMCPACFRET (YES)

Setup SAF resources

- **Security Admin** sets up access to the ICSF **CKDS Key Record Read2** (CSNBKRR2) service
  - Define the RACF profile such that no one has access to the ICSF services. Examples:
    - **RDEFINE CSFSERV * UACC(NONE)**
    - **RDEFINE CSFSERV CSFKRR2 UACC(NONE)**
  - Allow everyone to have access to the callable service CSNBKRR2
    - **PERMIT CSFKRR2 CLASS(CSFSERV) ID(*) ACCESS(READ)**

The above are examples intended to show how an installation might set up CSFSERV profiles.

2b Prepare system to allow data set encryption

Set up SAF resource to enable data set encryption based on key label specification

- **Security Admin** must consider whether migration action should allow data set encryption
  - *Ensure **all systems** that may need to **access the data** have the **CKDS** with key material required to decrypt the data sets **AND** are at the **correct HW/SW levels.***
    - **All systems in the sysplex, remote sites, fall-back systems**, …

- To allow the system to create encrypted data sets when the key label is specified via a method outside of the DFP segment in the RACF data set profile, the user must have at least **READ authority** to the following **new resource in the FACILITY class:**

  STGADMIN.SMS.ALLOW.DATASET.ENCRYPT
  - The system checks the authority to this facility class when the data set is first allocated (created).
    - The system does not require the user to have authority to this resource. when the key label is specified in the **DFP segment in the RACF data set profile**.

Note: For years, IBM has recommended, and continues to recommend, that STGADMIN.* be defined with UACC(NONE)

2c

Setup access to key labels

Setup SAF resources for key-label

- **Security Admin** sets up profiles in the CSFKEYS general resource class based on installation requirements. Any user that must access data in the clear must have access to the key label
- The following are examples.
  - **Define the RACF CSFKEYS profile such that no one has access to any key label**
    - **RDEFINE CSFKEYS * UACC(NONE)**
  - **Define the RACF profile such that no one has access to key-label**
    - **RDEFINE CSFKEYS key-label UACC(NONE)**
  - **To allow key label to be used by JOHN when accessed by any application**
    - **PERMIT key-label CLASS(CSFKEYS) ID(JOHN) ACCESS(READ)**
  - **To allow key label to be used by MIKE only when accessed by DFSMS**
    - **PERMIT key-label CLASS(CSFKEYS) ID(MIKE) ACCESS(READ) WHEN(CRITERIA(SMS(DSENCRYPTION)))**
  - **To allow key label to be used by any user only when accessed by DFSMS**
    - **PERMIT key-label CLASS(CSFKEYS) ID(*) ACCESS(READ) WHEN(CRITERIA(SMS(DSENCRYPTION)))**
  - **To allow key label to be used by Db2 MSTR and DBM1 userid**

The above are examples intended to show how an installation might set up CSFKEYS profiles based on access requirements. Designed to support separation of access: data owner vs data manager.

3 Creating encrypted data sets – supplying key labels

A data set is defined as 'encrypted' when a **key label** is supplied on allocation of a ***new*** sequential or VSAM extended format data set

A **key label** supplied via new keywords in any of the following sources (using ***order of precedence*** as follows):

- **RACF Data set profile DFP segment**
- **JCL, Dynamic Allocation, TSO Allocate, IDCAMS DEFINE**
- **Db2 V12 only: System keylabel and data keylabel for user tables and stogroups using V12@FL50x**
- **SMS Construct: Data Class**

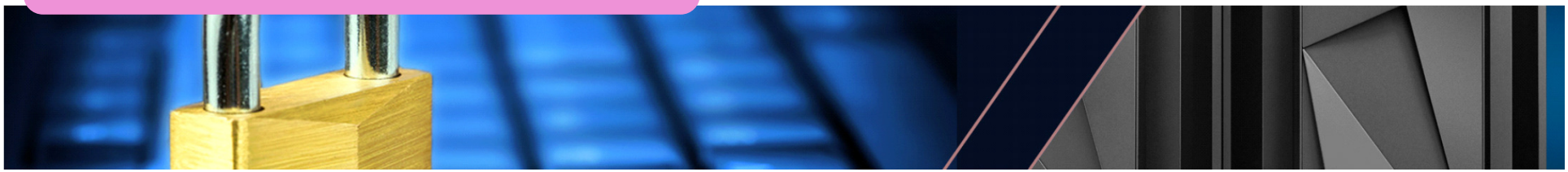
DFP segment in RACF data set profile

- Label of an existing key in the ICSF CKDS used by access methods for encrypting/decrypting sequential and VSAM data
- Provides granularity for different key labels to be used based on RACF profiles

```
ALTDSD 'PROJECTA.DATA.*' UACC(NONE) DFP(RESOWNER(iduser1))
                        DATAKEY(Key-Label))
```

Command Keyword	Meaning
DATAKEY(Key-Label)	Identifies the KEY LABEL in ICSF CKDS used to encrypt/decrypt the data
NODATAKEY	Removes a key label if defined to the RACF DPF segment

Key label only used for new data set create
Any subsequent change to RACF Data set profile will not affect existing data sets



JCL, Dynamic Allocation and TSO Allocate

- New keyword to be used for DASD data sets
  - **DSKEYLBL=key-label**
    - Key label of an existing key in ICSF CKDS used by access methods for encrypting/decrypting sequential and VSAM data
    - Userid executing **Db2 utilities** like REORG, UNLOAD, COPY ... require keylabel authority for **input/output datasets** if data is/should be encrypted outside of Db2
      - Sort datasets cannot be encrypted
      - TEMPLATE utility with new DSKEYLBL option planned for V12@FL50x

```
//DD1    DD    DSN=DSN1,DISP=(NEW,CATLG),DATACLAS=DSN1DATA,MGMTCLAS=DSN1MGMT,
//               STORCLAS=DSN1STOR,DSKEYLBL='LABEL.FOR.DSN1'
```

DSKEYLBL is effective only if the new data set is on DASD. It is ignored for device types other than DASD, including DUMMY.

Key label only used for new data set create

Creating a new VSAM data set via IDCAMS

- New parameter on DEFINE for CLUSTER
  - **KEYLABEL=key-label**
    - Key label of an existing key in ICSF CKDS used by access methods for encrypting/decrypting sequential and VSAM data
    - Used for both cluster and any alternate index

```
DEFINE CLUSTER -
(NAME(DSN1.EXAMPLE.ESDS1) -
RECORDS(100 500) -
RECORDSIZE(250 250) -
KEYLABEL (LABEL.FOR.DSN1) -
NONINDEXED )
```

More considerations concerning Db2

- **Complete encryption solution** for all Db2 data including user tables, indexes, LOBs/XML, active/archive logs, catalog/directory
- **V11/V12 base enhancements** provided by APAR PI81900/PI81907 supports RACF dataset profile and SMS dataclass definition for z/OS V2.2+ dataset encryption

- New V12@FL50x **zPARM** system keylabel parameter planned for **catalog/directory and archive logs**
  - SET SYSPARM command by installed SYSADM and SECADM
- New V12@FL50x database administration capabilities planned
  - Issue a **CREATE or ALTER TABLE** to add a key label for individual tables and associated indexes, LOB, XML, clone ts that need to be encrypted at rest
  - Issue a **CREATE or ALTER STOGROUP** to add a key label for tables in a storage group that need to be encrypted at rest
  - New **KEYLABEL column** is added to **Db2 catalog tables**
    - CATMAINT UPDATE LEVEL V12R1M50x has to be executed to add new KEYLABEL column before new function level activation

More considerations concerning Db2

- Execute REORG utility
  - Utility job must specify a user ID which has access to any encrypted input or output data sets
  - Utility job uses Db2 authority to access Db2 data

SMS Construct: Data Class

Data Class identifies key label to be used when creating a new data set.

- Key label of an existing key in ICSF CKDS used by access methods for encrypting/decrypting sequential and VSAM data

```
                                DATA CLASS ALTER                    Page 5 of 6
Command ===>

SCDS Name . . . : IBMUSER.ENCSCDS
Data Class Name : ENCRLS64

To ALTER Data Class, Specify:

  Tape Encryption Management
    Key Label 1 . . .      (1 to 64 characters or blank)

    Key Label 2 . . .

    Encoding for Key Label 1  . . . . .              (L, H or blank)
    Encoding for Key Label 2  . . . . .              (L, H or blank)

  DASD Data Set Level Encryption Management
    Data Set Key Label . . .  (1 to 64 characters or blank)
    PROTKEY.AES.SECURE.KEY.32BYTE

Use ENTER to Perform Verification; Use UP/DOWN Command to View other Panels;
Use HELP Command for Help; Use END Command to Save and Exit; CANCEL to Exit.
```

Key label only used for new data set create

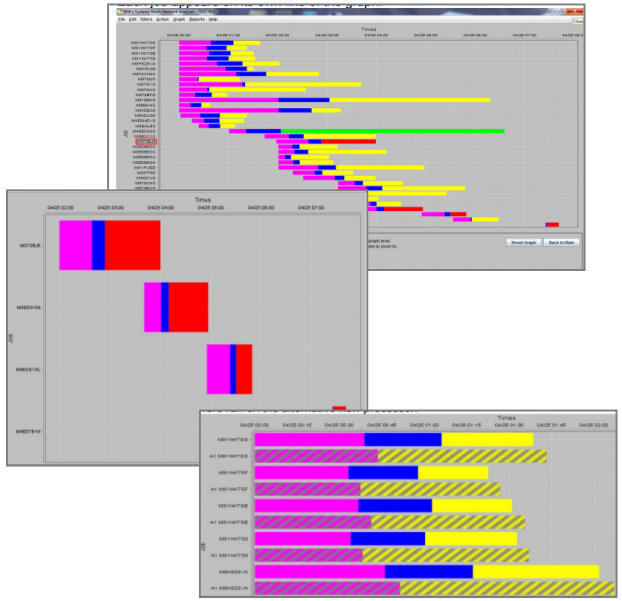
4b How can I be sure the data is encrypted?

- Encryption attributes displayed in various system interfaces
  - SMF records, DCOLLECT records
  - LISTCAT, IEHLIST LISTVTOC
- Db2 V12@FL50x planned enhancements
  - DISPLAY GROUP to show system keylabel (zPARM)
  - REPORT TABLESPACESET utility to display keylabel info for the table spaces used by each table
  - DISPLAY LOG / DISPLAY ARCHIVE show keylabel info for active and archive logs
- IBM Security zSecure suite V2.3 helps administer and audit data set encryption capabilities

z Systems Batch Network Analyzer (zBNA) Tool

Estimating Resources and Technology Options using z Batch Network Analyzer (zBNA)

- zBNA is a no charge, as-is PC-based analysis tool originally designed to analyze batch windows
- Uses SMF workload data and generates graphical and text based reports
- Previously enhanced for zEDC to identify & evaluate BSAM / QSAM compression candidates
- **Enhanced for Encryption**
  - To help clients estimate the CPU impact of enabling encryption
  - zBNA V1.8.1



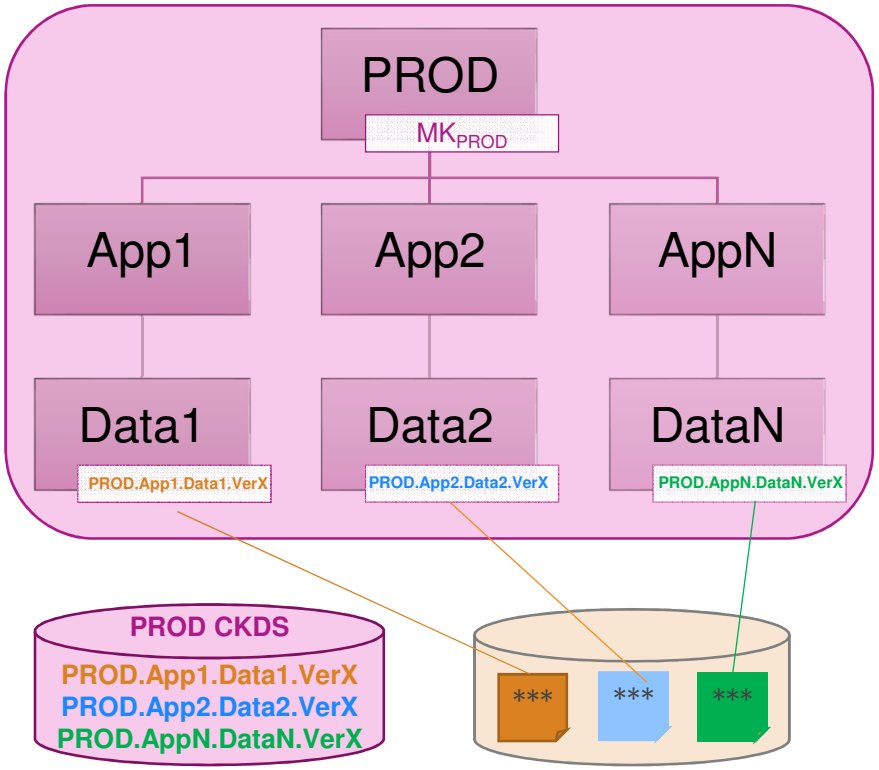
NEW! Support planned for z/OS data set encryption and coupling facility encryption

Available on techdocs for customers, business partners, and IBMers
http://www.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/PRS5132

Note: z/OS Capacity Planning tool zCP3000 also updated to provide encryption estimates
http://w3-03.ibm.com/support/americas/wsc/cpsproducts.html

Naming Conventions & Granular Access Control

Leveraging naming conventions & z Security to enforce separation across application instances



- Naming conventions can be used to segment applications, data, and keys, e.g.
  - Environment: PROD, QA, TEST, DEV
  - Application: App1, App2,…, AppN
  - Data-Type: Account, Payroll, Log
  - Version: Ver1, Ver2,…,Verx
- Application resources (data sets, encryption keys) can be assigned names based on naming conventions, e.g.
  - PROD.APP2.LOG.VER10
  - PROD.APP1.PAYROLL.KEY.VER7
- Security rules can be used to enforce separation with granular access control for application resources and encryption keys

Enterprise Key Management

Encryption of data at enterprise scale requires robust key management

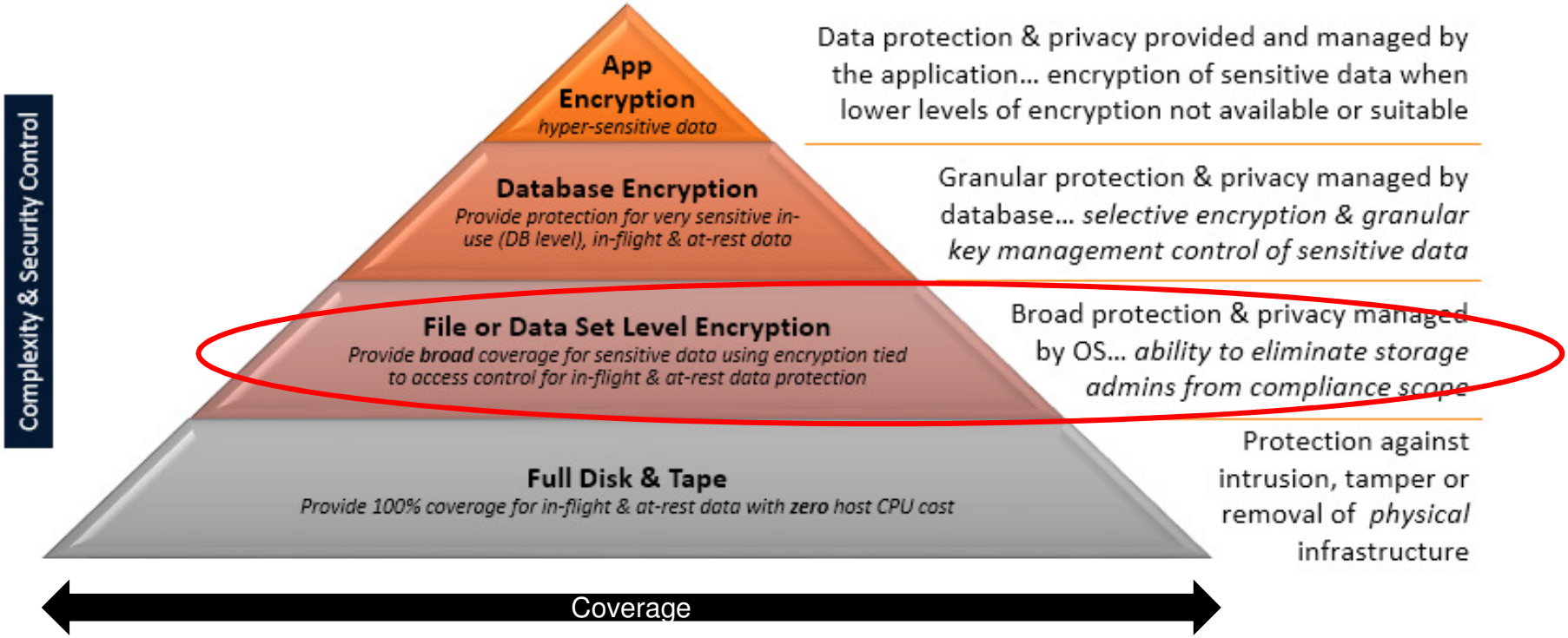
- The current key management landscape can be characterized by clients who have …
  - … already deployed an enterprise key management solution
  - … developed a self-built key management solution
  - … not deployed an enterprise key management solution

Key management for pervasive encryption must provide …

- Policy based key generation
- Policy based key rotation
- Key usage tracking
- Key backup & recovery

EKMF The IBM Enterprise Key Management Foundation (EKMF) provides real-time, centralized secure management of keys and certificates in an enterprise with a variety of cryptographic devices and key stores.

Multiple layers of encryption for data at rest



Resources: Publications

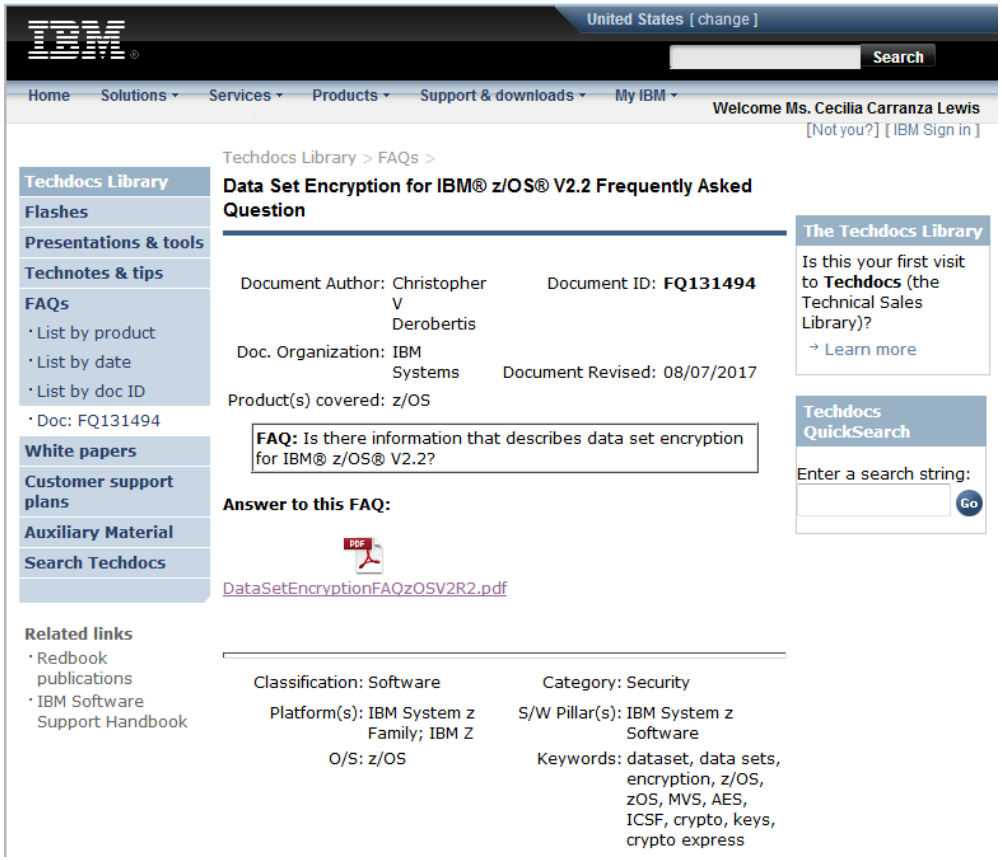
- ***z/OS DFSMS Using the New Functions – Data Set encryption implementation information***
- ***z/OS DFSMS Using Data Sets – Data Set encryption implementation information***
- *z/OS DFSMS Introduction*
- *z/OS DFSMSdfp Storage Administration*
- *z/OS DFSMS Managing Catalogs*
- *z/OS DFSMS Access Method Services Command Reference*
- *z/OS DFSMS Macro Instructions for Data Sets*
- *z/OS DFSMSdfp Advanced Services*
- *z/OS DFSMSdfp Diagnosis*
- *z/OS DFSMSdss Storage Administration Reference*
- *z/OS DFSMShsm Data Areas*
- *z/OS DFSMS Installation Exits*
- *z/OS MVS Initialization and Tuning Reference*
- *z/OS MVS System Commands*
- *z/OS MVS JCL Reference*
- *z/OS MVS System Management Facility (SMF)*
- *z/OS MVS System Messages Volume 1, 2, 6, 7 and 8*
- *z/OS MVS Programming: Authorized Assembler Services Guide*
- *z/OS Summary of Message and Interface Changes*
- *z/OS Migration*

28

Resources: Technote for z/OS V2.2

Techdoc contains

- Support provided in V2.2
- Complete list of maintenance
- HW/SW requirements
- Restrictions
- Exploiter support
  - DB2, IMS, CICS, MQ, zFS, zSecure



www-03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/FQ131494

Technote continued

Are there plans for IBM DB2 to support z/OS data set encryption?

Yes, IBM DB2 is designed to transparently encrypt data at rest without database downtime or requiring the administrator to redefine objects, which could cause disruption to operations. This includes the ability to transparently encrypt its logs, catalog, directory, tables and indices including all data types such as large binary objects transparently. In addition, for maximum availability, rekeying of data keys can be performed non-disruptively without taking DB2 databases offline.

IBM DB2 for z/OS v11 for z/OS and IBM DB2 v12 for z/OS (at M100 level) plan to support z/OS V2.2 data set encryption when the following DB2 service becomes available:

- DB2 V11 APAR - PI81900
- DB2 v12 APAR - PI81907 (for M100 level)

Are there plans for IBM IMS to support z/OS data set encryption?

Yes, Information Management System (IMS) V13 and V14 support z/OS V2.2 data set encryption.

IMS V13 and V14 do not require IMS product APARs or PTFs to support data set encryption.

The following information summarizes IMS data sets that do and do not support data set encryption.

Are there plans for IBM MQ to support z/OS data set encryption?

Yes, IBM MQ versions 8.0.0 and 9.0.0 (Long Term Support and Continuous Delivery Release) supports z/OS V2.2 data set encryption.

MQ versions 8.0.0 and 9.0.0 (LTS and CDR) do not require MQ product APARs or PTFs to support data set encryption.

The following information summarizes MQ data sets that do and do not support data set encryption.

Are there plans for IBM CICS Transaction Server to support z/OS data set encryption?

Yes, all in-service releases of CICS Transaction Server for z/OS (CICS TS) will support data set encryption, and do not require CICS product APARs or PTFs to support data set encryption.