

# Pervasive Encryption on z/OS®

## NY Metro NaSPA

April, 2017

Mark Nelson, CISSP®, CSSLP®  
z/OS® Security Server Design and Development  
IBM®  
markan@us.ibm.com



# IBM z Systems Pervasive Encryption

*A Data Centric Approach to Information Security*

## *Data is the new perimeter*

*A transparent and consumable approach to enable extensive encryption of data **in-flight** and **at-rest** to substantially simplify & reduce the costs associated with protecting data & achieving compliance mandates.*

### Encryption Policy



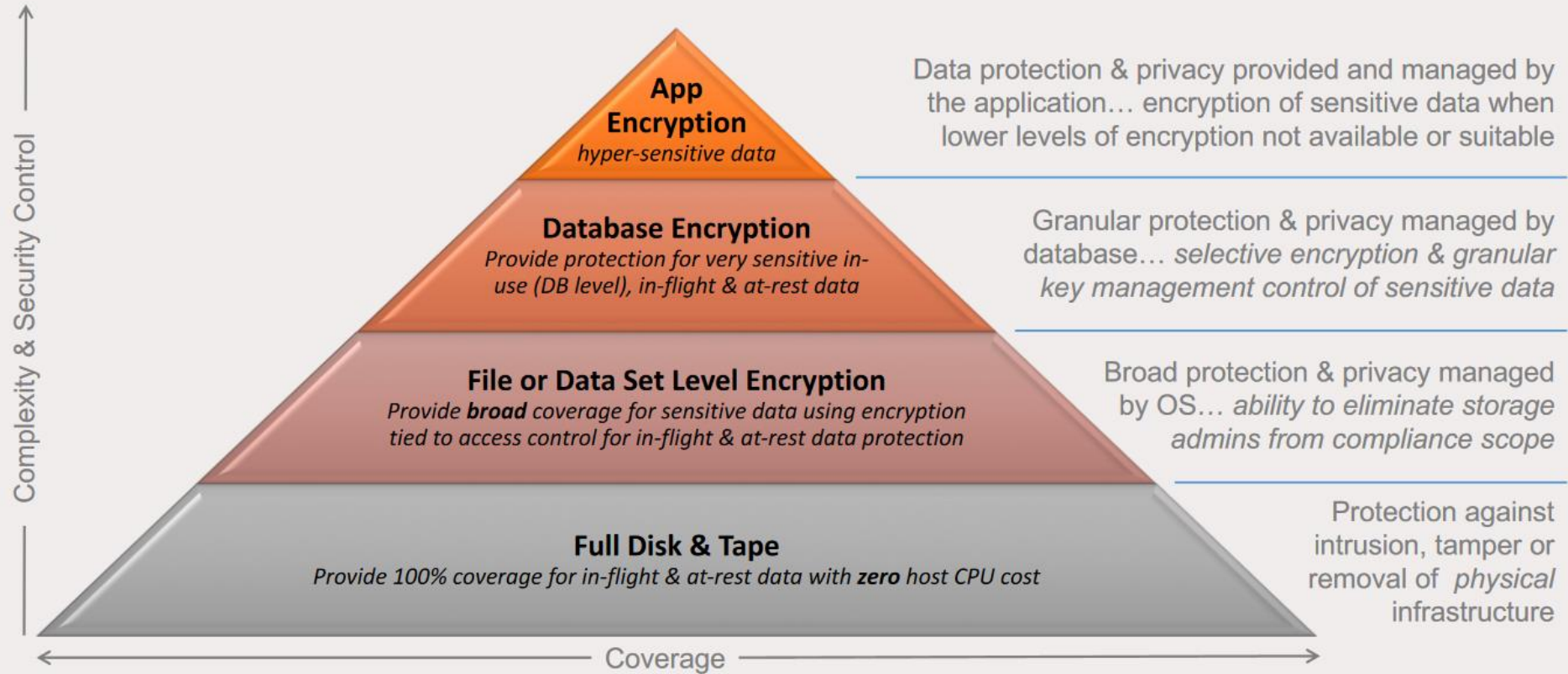
**In-Flight**

**At-Rest**



# Multiple layers of encryption for data at rest

## Robust data protection



## IBM US Software Announcement 216-392, 4 October 2016

- **IBM plans to deliver application transparent, policy-controlled dataset encryption in IBM z/OS. IBM DB2 for z/OS and IBM Information Management System (IMS) intend to exploit z/OS dataset encryption**

### IBM Statement of Direction:

IBM's statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM's sole discretion.

Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision.

The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract.

The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.



## IBM US Software Announcement 217-085, 21 February, 2017

- **z/OS 2.3 will be designed to provide policy-enabled data protection for z/OS data sets, zFS file systems, and Coupling Facility structures, giving users the ability to encrypt data to strengthen compliance and audit responsiveness and provide simplified security processes and protection for mission-critical data. These planned enhancements include:**
  - DFSMS provides new enhancements that are designed to give users the ability to encrypt their data sets, using either SAF or SMS policies, without changing their application programs. DFSMS intends to make use of the Central Processor Assist for Cryptographic Functions (CPACF) to encrypt and decrypt extended format (version 2 only) sequential BSAM and QSAM data sets and all types of extended format VSAM data sets as written to and read from disk. In addition, data set level encryption is planned to allow the data to remain encrypted during administrative functions such as backup/restore, migration/recall, and replication.
  - zFS plans to make use of the DFSMS data set encryption to support the encryption of individual files (file content), access control lists, security information, and symbolic link contents. The use of zFS encryption can be paired with compression to offset the overhead of encryption.



## Implementation Details: What's Supported and What's Not Supported

- **Encrypted data is transparent to the application when the application uses standard access method APIs. *No application changes are needed.***
- **Supported access methods**
  - BSAM/QSAM sequential data sets, extended format only (Version 2)
  - VSAM and VSAM/RLS (KSDS, ESDS, RRDS, VRRDS, LDS), extended format only
  - New option to allow access to data in the encrypted form
- **Restrictions**
  - System data sets (such as catalogs, HSM data sets, RACF data sets) must not be encrypted unless otherwise specified
  - Encrypted data sets are supported only on 3390 device types
  - Sequential (non-compressed) data sets with a BLKSIZE of less than 16 bytes cannot be encrypted as they cannot be extended format
  - Data sets used during IPL must not be encrypted



## Implementation Details: Hardware and Software Levels

- **All systems sharing the data must be at a minimum level of z/OS V2.1 or higher**
  - Coexistence only on V2.1 (with APARs)
  - Supported on V2.2 (with APARs)
  
- **Requires:**
  - Feature 3863, CP Assist for Cryptographic Functions (CPACF)
  - The minimum processor hardware is z196 or higher with CEX3 or later



## Implementation Details: RACF Setup – Access Checks

- **With this support, DFSMSdfp calls ICSF. User creating, updating, or accessing encrypted data will need access to certain ICSF services**
  - For example, CSNBKRR2 (CKDS Key Record Read2 service) in the CSFSERV class
- **The key to be used for the encryption is specified by its ICSF key-label. The user must be authorized to this key-label in the CSFKEYS class**
  - You can permit users and groups to the CSFKEYS class in the “traditional” manner:

```
PERMIT key-label CLASS(CSFKEYS) ID(...) ACCESS(READ)
```

- Alternatively, you can allow everyone to use the key, but only when using it for data set encryption/decryption using the CRITERIA specification on PERMIT:

```
PERMIT key-label CLASS(CSFKEYS) ID(*) ACCESS(READ)  
WHEN (CRITERIA (SMS (DSENCRYPTION) ) )
```

- **To allow the user to create encrypted data sets, the user must have at least READ authority to the resource STGADMIN.SMS.ALLOW.DATASET.ENCRYPT in the FACILITY class.**





## Implementation Details: RACF Setup – Defining the Key Label to DFP

- A sequential or VSAM data set would be defined as 'encrypted' when a key label is supplied on allocation of a new sequential or VSAM data set. The key label can be specified (in order of precedence):

- RACF data set profile

```
ALTDSDD 'PROJECT.DATA.*' UACC(NONE) DFP(DATAKEY(key-  
label))
```

- JCL, dynamic allocation, TSO allocate, IDCAMS

```
//DD1 DD DSN=A.B.C, DISP=(NEW, CATLG), DATACLA=DSN1DATA,  
// MGMTCLASS=DSN1MGMT, STORCLAS=DSN1STOR,  
// DSKEYLBL=' LABEL . FOR . DSN1 '
```

- SMS DATA CLASS



## Implementation Details: Other Things to Note

- When data set level compression is requested, the access methods handle the compression before the encryption
- Only AES-256 keys are supported
- LISTVTOC, LISTCAT, CSI (catalog search interface) all return encryption status of a data set
- SMF 14/15 (sequential data sets) and SMF 62 (VSAM data sets) has the encryption status of the data set as does DCOLLECT



# Questions?

