Db2 zOS Security & Encryption Update

Francesco Borrello
IBM Cloud
Techinical Sales and Solutions

francesco.borrello@it.ibm.com

2018

False Myths and GDPR

- **Art. 34 GDPR: Communication of a personal data breach to the data subject**

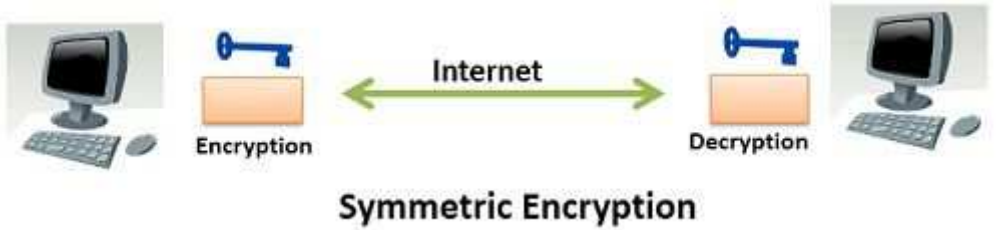
1) When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject **without undue delay**
2) The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal breach […]
3) The communication to the data subject referred to in paragraph 1 **shall not be required if any of the following conditions are met**:
   a) The controller has implemented appropriate **technical and organizational** protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular **those that render the personal data unintelligible to any person who is not authorized to access it, such as encryption**;
   b) The controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialize;
   c) It would have involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner

[…]

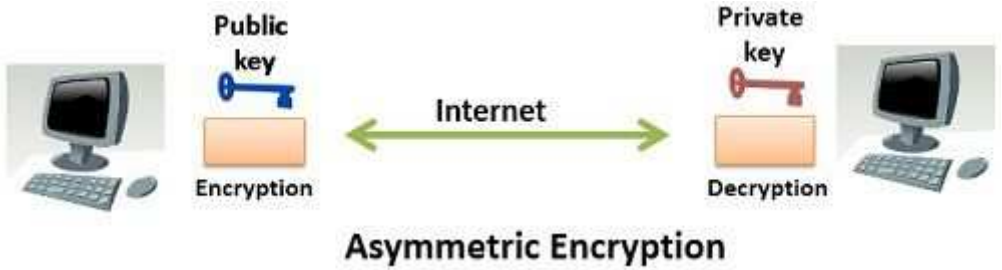
The good cryptographer's kit

- Encryption key

- Encryption Algorithm
  - Symmetric encryption: it always uses a single key for encryption and decryption of the message

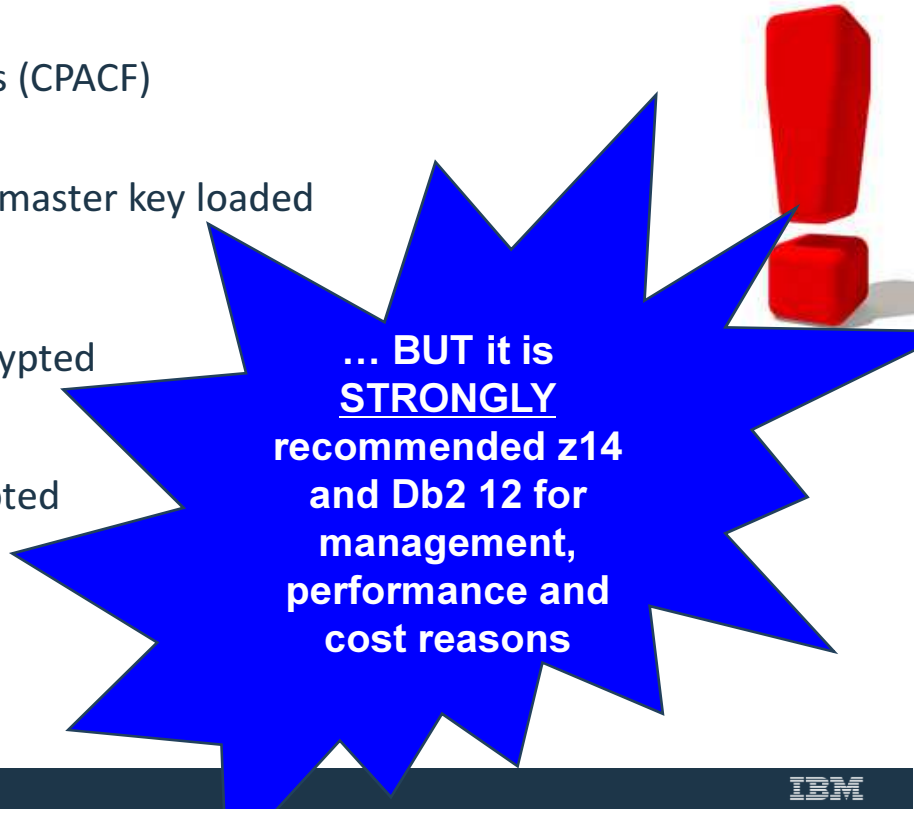


  - Asymmetric encryption: it uses a pair of keys. One key is used for encryption (generally referred to as public key) and the other one is used for decryption of the message (generally referred to as private key)



Prerequisites

- Hardware requirements
  - Data set encryption requires IBM Enterprise z196 or later as well as the following cryptographic hardware features:
    - Crypto Express3 Coprocessor or later
    - Feature 3863, CP Assist for Cryptographic Functions (CPACF)
- Operating System requirements
  - ICSF is installed and configured with a CKDS and AES master key loaded
- Coexistence requirements
  - On a z/OS V2R3 or z/OS V2R2 with OA50569, you can create encrypted data sets as well as access encrypted data sets
  - On a z/OS V2R1 with OA50569, you cannot create encrypted data sets. However, you can access encrypted data sets
- Db2 for zOS Base Encryption Support
  - Db2 V11 APAR – PI81900
  - Db2 V12 APAR – PI81907 (for M100 level)



z14 Integrated Cryptographic Hardware

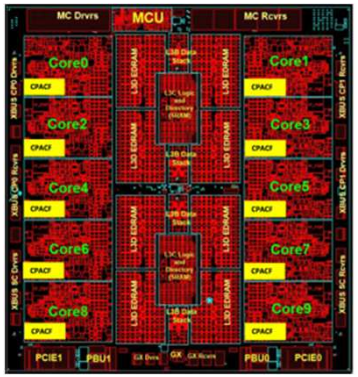
Hardware innovation

CP Assist for Cryptographic Functions (CPACF)

- Hardware accelerated encryption on every microprocessor core
- Performance improvements of up to 7x for selective encryption modes

Crypto Express6S

- Next generation PCIe Hardware Security Module (HSM)
- Performance improvements up to 2x
- Industry leading FIPS 140-2 Level 4 Certification Design



Why is it valuable:

- More performance = lower latency + less CPU overhead for encryption operations
- Highest level of protection available for encryption keys
- Industry exclusive “protected key” encryption

Pervasive Encryption with IBM z Systems

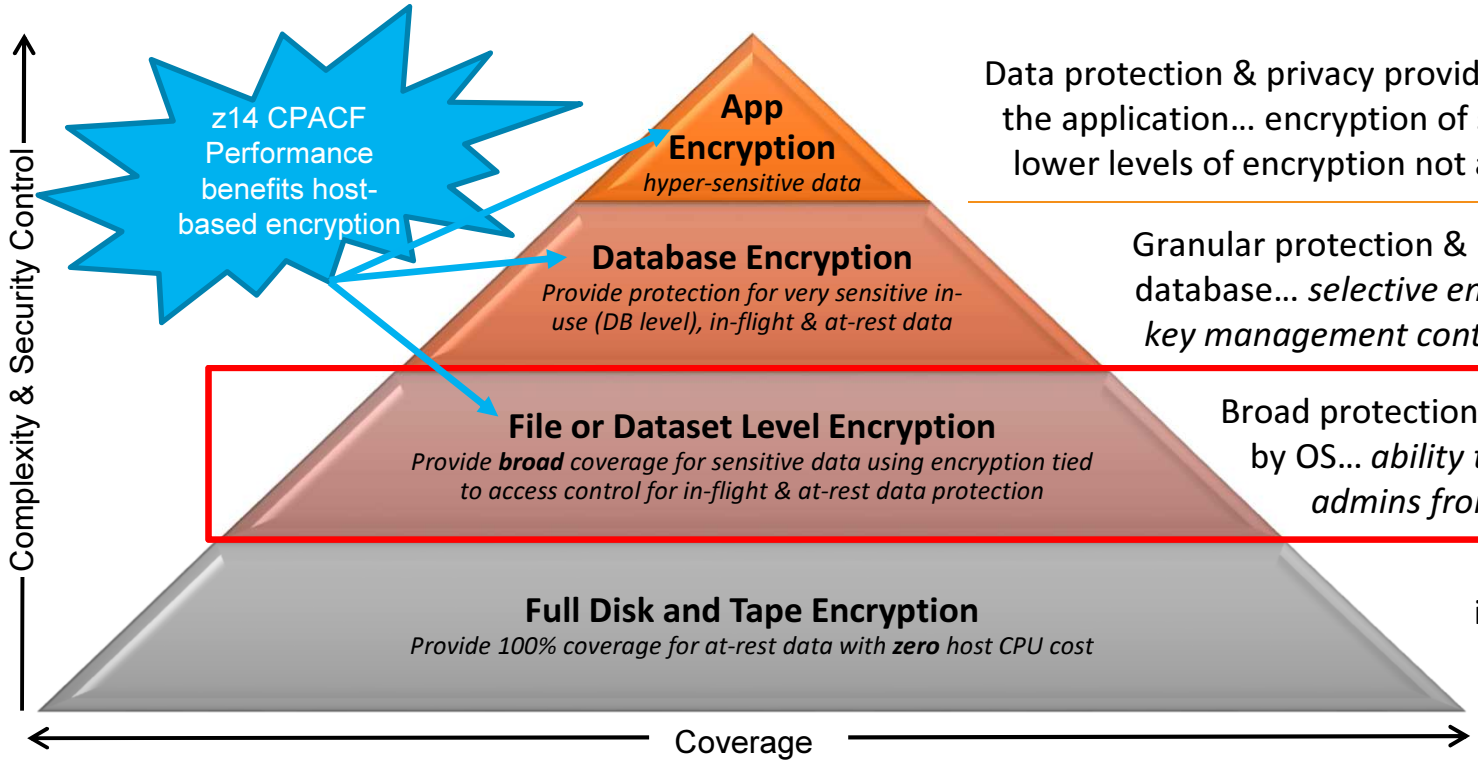
Enabled through full-stack platform integration

Integrated Crypto Hardware		Hardware accelerated encryption on every core – CPACF performance improvements of up to 7x Next Gen Crypto Express6S – up to 2x faster than prior generation
Data at Rest		Broadly protect Linux file systems and z/OS data sets 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
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
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.

And we're just getting started …

Multiple Layers of Encryption

Robust protection for at-rest data



Data protection & privacy provided and managed by the application… encryption of sensitive data when lower levels of encryption not available or suitable

Granular protection & privacy managed by database… *selective encryption & granular key management control of sensitive data*

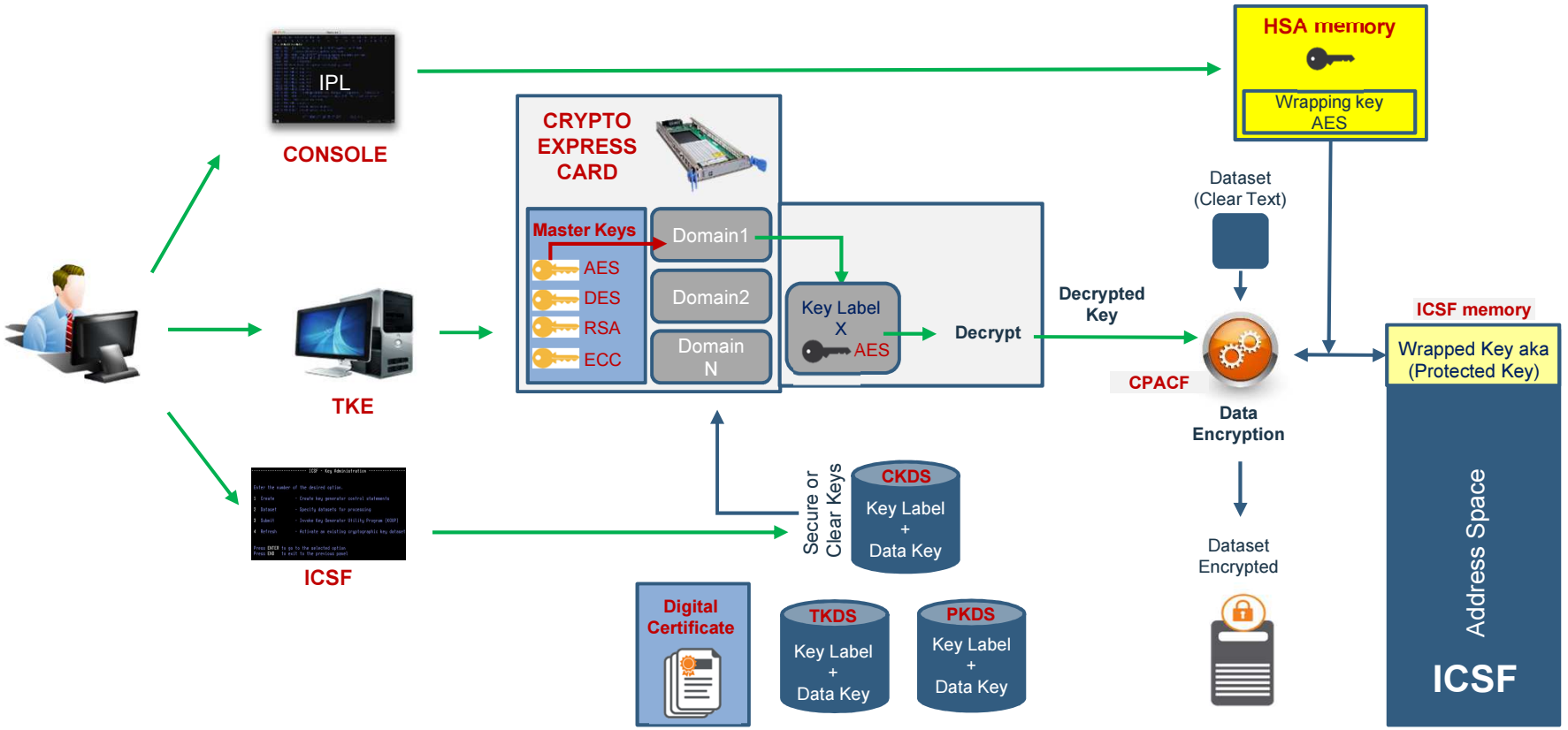
Broad protection & privacy managed by OS… *ability to eliminate storage admins from compliance scope*

Protection against intrusion, tamper or removal of *physical* infrastructure

DFSMS Dataset Encryption - Overview

- DFSMS encrypts/decrypts records when written to or read from disk
- DFSMS managed data sets that supported encryption of data at rest:
  - BSAM / QSAM
    - Sequential – Extended format only
  - VSAM and VSAM/RLS
    - KSDS, LDS, ESDS, RRDS, VRRDS – Extended format only
- Encryption type – AES 256 bit key
- Key Label – A 64-byte label of the key in the ICSF CKDS that is used for encryption/decryption of the data set

Dataset Encryption: How does it work?



Db2 Support of z/OS Dataset Encryption

- Db2 can now transparently encrypt data at rest without database downtime or requiring administrator to redefine objects which could cause disruption to operations. No application changes required.
  - Encrypt active and archive log datasets
  - Encrypt catalog and directory table spaces
  - Encrypt user table spaces
- Utilizes new z/OS DFSMS data set encryption support delivered in z/OS 2.3 and z/OS 2.2
- Db2 12 adds additional controls to set up encryption policies using Db2 interfaces

Steps to enable encryption

1

ICSF Admin

Generates an encryption key and key label.
Stores it in the ICSF CKDS

2

Security Admin

Sets up RACF for use of key label

Allows secure key to be used as protected key via ICSF segment
- SYMCPACFWRAP
- SYMCPACFRET

– AND –

Permits Db2 use of the key label

In RACF, permit access to new resource in FACILITY class

3

Security / Database / Storage Admin

Associate the key label with the desired data set.

In RACF, alter DFP segment in data set profile - DATAKEY()

– OR –

(V12 only) In Db2, set key label for system objects and user objects

– OR –

In DFSMS, assign to data class

4

Database Admin

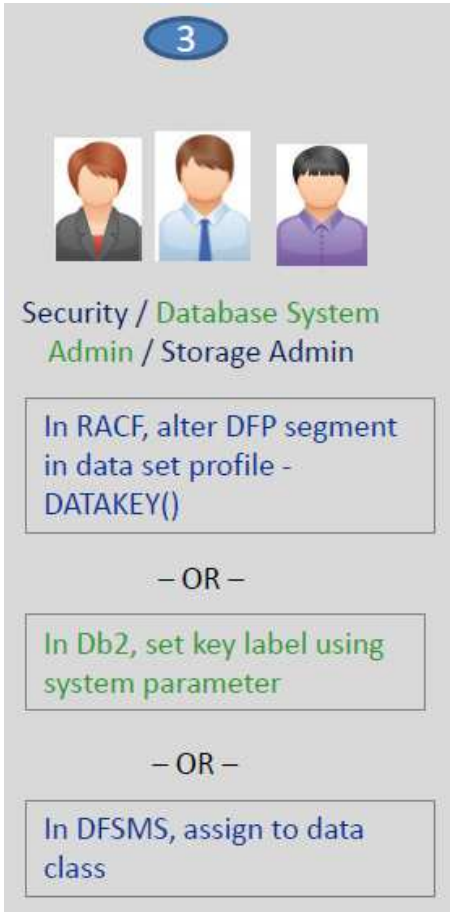
Migrate to encrypted data

Online REORG

Non-disruptive

Encrypting Db2 System Objects

- The options to define a key label used by Db2 (Precedence order):
  - Security Admin can set a key label in the DFP segment of RACF data set profile using the new DATAKEY keyword
  - Database System Admin can set a key label using ENCRYPTION_KEYLABEL system parameter (V12R1M502 only)
    - -SET SYSPARM command is required for zParm value to take effect
    - Group scope: Takes effect on all the members of a data sharing group immediately
    - Security related parameter: Requires installation SYSADM or SECADM authority to set the zParm
    - Db2 DBM1 and MSTR address spaced IDs must be permitted access to the key label
  - Storage Admin can set a key label using IDCAMS DEFINE for active logs
  - Storage Admin can set a key label in the DFSMS dataclass



Encrypting Db2 System Objects

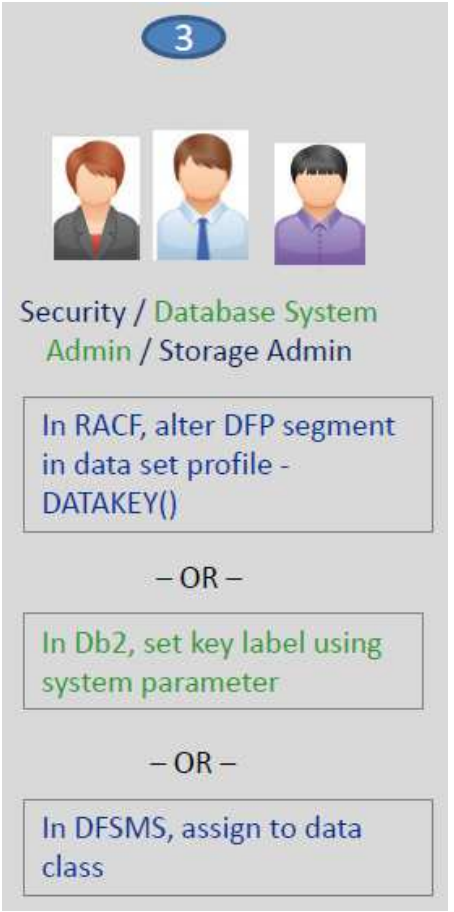
- Active logs
  - Encrypt new active logs
    - Define active log data set as encrypted and issue the SET LOG command NEWLOG option to add the newly defined active log data set to the active log inventory without stopping Db2
    - Encrypt all active logs
      - Stop Db2. Copy the contents of the active log data set to an encrypted data set. Restart Db2.
- Archive logs:
  - New archive logs automatically encrypted based on the key label setting
- Catalog and directory table spaces
  - Execute REORG TABLESPACE utility to encrypt table spaces and index spaces in DSNDB06 and DSNDB01
  - Encrypt DSNDB01.SYSUTILX – Execute RECOVER utility followed by REBUILD INDEX(ALL)

Database Admin

Online REORG

Encrypting User Objects

- The options to define a key label for user objects encryption (Precedence order):
  - Security Admin can set a key label in the DFP segment of RACF data set profile using the new DATAKEY keyword
  - Application Database Admin can set a key label using SQL interfaces, CREATE / ALTER TABLE / STOGROUP (V12R1M502 only)
    - Enabled with APPLCOMPAT V12R1M502
  - Storage Admin can set a key label in the DFSMS dataclass



Encrypting User Objects

- Execute the REORG utility to encrypt existing table spaces
- New table spaces or partitions defined are encrypted using the key label based on the hierarchy

Database Admin

Online REORG to encrypt existing user objects

Encrypting Db2 Objects: Monitoring

- Display encryption key label using DFSMS interfaces, SMF records
- Run REPORT TABLESPACESET utility to display key label associated for each catalog and directory table spaces using the new SHOWKEYLABEL option (V12R1M502 only)
- Issue – DISPLAY LOG command to obtain current key label information for current active log data sets (V12R1M502 only)
- Issue – DISPLAY ARCHIVE command to obtain current key label information for archive log data sets that are in use (V12R1M502 only)

Utilities Consideration

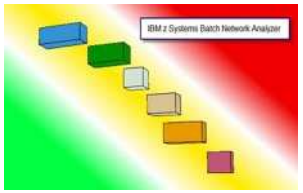
- All online utilities support table spaces and indexes whose underlying VSAM data sets are encrypted

- Input / Output data sets
  - Key label can also be specified using
    - JCL DSKEYLBL option
  - Authorization ID of the job requires access to the key label for any encrypted input or output data sets

Estimating CPU Cost of Data Protection

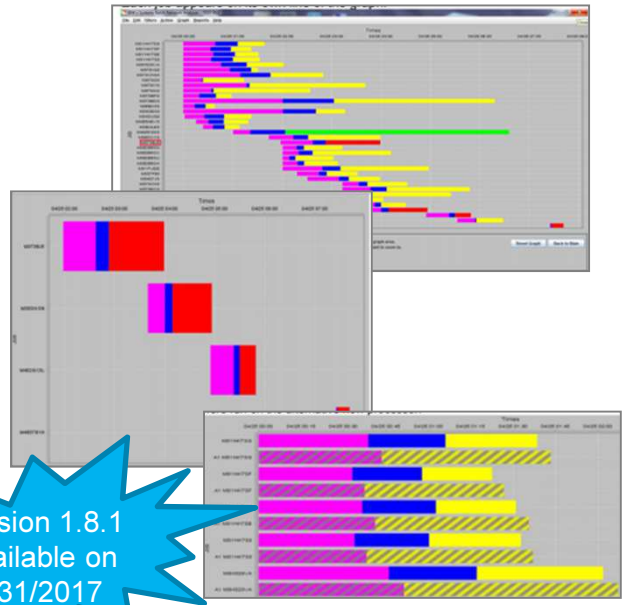
z Batch Network Analyzer (zBNA)

zBNA 1.8.1



zBNA Background:

- A no charge, “as is” tool originally designed to analyze batch windows
- PC based, and provides graphical and text reports
- Available on techdocs for customers, business partners, and IBMers
  http://www-03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/PRS5132
- Previously enhanced for zEDC to identify & evaluate compression candidates



zBNA Encryption Enhancements:

- zBNA will be further enhanced to help clients estimate encryption CPU overhead based on actual client workload SMF data
- Ability to select z13 or z14 as target machine
- Support will be provided for
  - z/OS data set encryption
  - Coupling Facility encryption

Version 1.8.1
Available on
8/31/2017


THANK YOU