z/VM and Tape Encryption

Eric Farman
IBM, z/VM I/O Development

10 August 2011
Session 9570

Trademarks

The following are trademarks of the International Business Machines Corporation in the United States, other countries, or both.

Not all common law marks used by IBM are listed on this page. Failure of a mark to appear does not mean that IBM does not use the mark nor does it mean that the product is not actively marketed or is not significant within its relevant market.

For a complete list of IBM Trademarks, see **www.ibm.com/legal/copytrade.shtml**

The following are trademarks or registered trademarks of other companies.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency, which is now part of the Office of Government Commerce.

* All other products may be trademarks or registered trademarks of their respective companies.

Notes:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon 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 throughput improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Agenda

- Terminology
- Overview
- z/VM Support
  - “Default Key” Encryption
  - “User Defined Key” Encryption
  - Tape Rekey

A PDF of this presentation is available at:
http://www.vm.ibm.com/devpages/farman

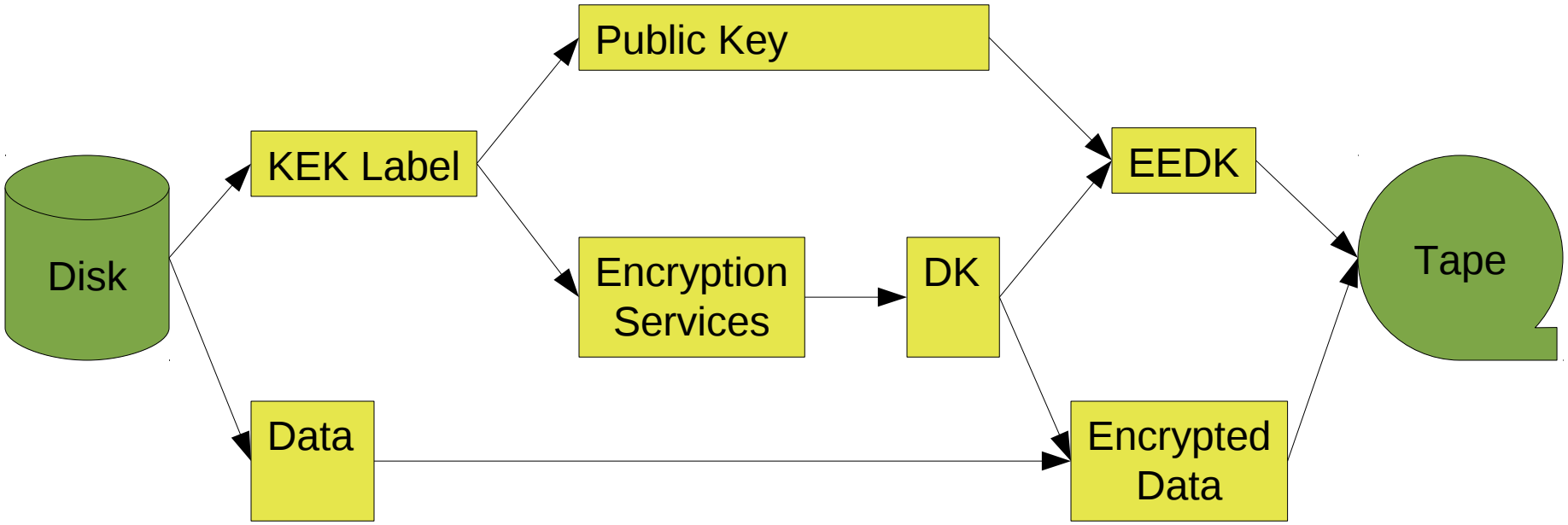
Terminology

- BOT – Beginning of Tape
- DK – Data Key
  - 256-bit AES symmetric key used to encrypt/decrypt data on tape
- EEDK – Externally Encrypted Data Key
  - DK encrypted with public key referenced by KEK Label
- EKM – Encryption Key Manager
  - Software that provides key management capabilities
- KEK – Key Encrypting Key
  - Public/private key pair used for encrypting/decrypting DK, respectively
- KEK Label – Key Encrypting Key Label
  - Human-readable representation of a KEK, defined in EKM

Overview

- Hardware-based encryption support introduced with the 3592 Model E05 tape drives (and C06 Control Unit)
- Data is sent between Operating System and Control Unit as plain text data
- CU and EKM handle key processing at the point of the first read/write I/O issued to a mounted tape cartridge
  - Communication path must be configured as “out-of-band” (TCP/IP) for z/VM
- One or two public keys can be used for a cartridge
  - Presumption is one key would be for the creator of the tape
  - A second key would be for the intended recipient of the tape

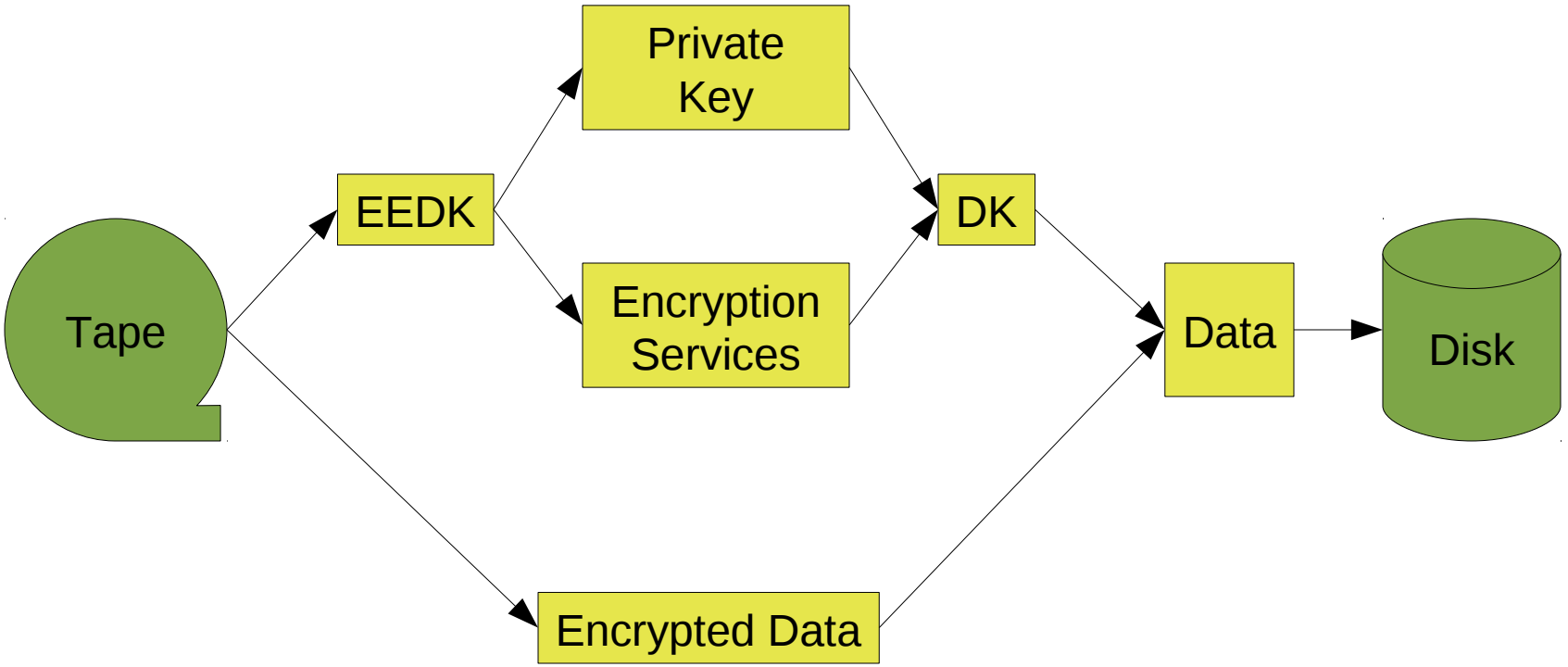
Overview – Encrypted Write to Tape (from BOT)



Overview – Encrypted Write to Tape

- OS specifies KEK Label(s) to use
  - CU and EKM negotiate with key store and cryptographic services
  - Retrieve public key(s) referenced by KEK Label(s)
  - Generate random DK
  - Use public key to encrypt DK into an EEDK
  - Store EEDK(s) on tape cartridge
- Data is encrypted with DK as it gets written to tape
  - It is written as the OS specified, if writing from BOT
  - It is written in the existing format, if the tape cartridge is moved beyond BOT before writing

Overview – Encrypted Read from Tape



Overview – Encrypted Read from Tape

- EEDK(s) are retrieved from tape cartridge
  - CU and EKM negotiate with key store and cryptographic services
  - No OS operands need to be specified
  - Private key is located to decrypt the DK within EEDK
    - If not found, tape I/O fails with error
- Data is decrypted with DK as it gets read from tape
- Additional data that is appended to the tape is encrypted with DK

z/VM Support

- Enables dedicated device support for any guest OS that supports tape encryption (e.g., z/OS, Linux)
- Provides mechanism for z/VM to enable encryption on behalf of those guests that do not support tape encryption (e.g., CMS) or want it managed by hypervisor
- Also used by facilities of z/VM itself, such as with SPXTAPE or DDR
- DFSMS/VM FL221 supports locating encryption-capable drives in an ATL

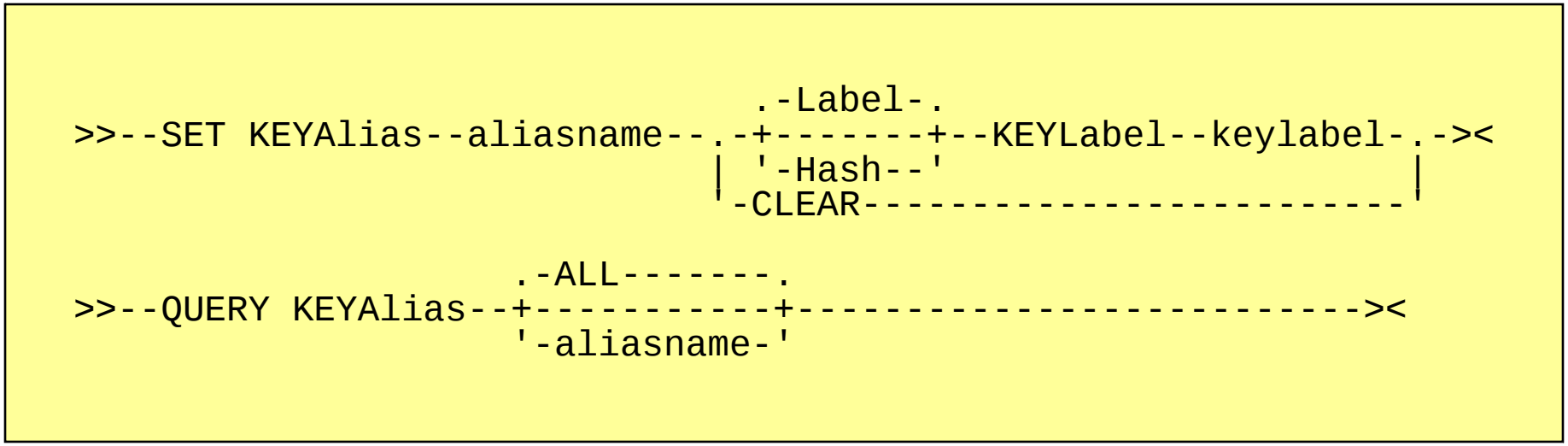
z/VM Support

- When z/VM is preparing a tape drive for use by itself or for unaware guests, encryption information needs to be provided to the drive
  - Commands permit the use of a set of “default” keys defined by the EKM
  - Alternatively, one or two key labels can be specified to use specific key pairs
    - Will also necessitate specification of an encoding mechanism
    - Expectation is one label will be owned by creator of tape, optional second label for a separate reader
- A z/VM “key alias” can be used to specify KEK Label(s) other than the EKM Default on ATTACH or SET RDEVice commands
  - Generated by the SET KEYalias command
  - Contains a KEK Label and an encoding mechanism
- KEK Label support also added to DDR
  - Since DDR can run standalone, uses a new control statement

Encoding Mechanisms

- Method of identifying which private key would be required to decrypt a given EEDK
  - “LABEL” uses the KEK Label directly, such that the recipient must have the same KEK Label tagging the public/private key
  - “HASH” uses a hash of the public key, such that the recipient’s KEK Label need not match that of the originator
- In either case, the private key that corresponds to the public key used for encryption must be present in the key store
  - Does not provide a mechanism for fabricating the private key

z/VM Support – SET/Query KEYAlias command



z/VM Support – SET/Query KEYAlias command

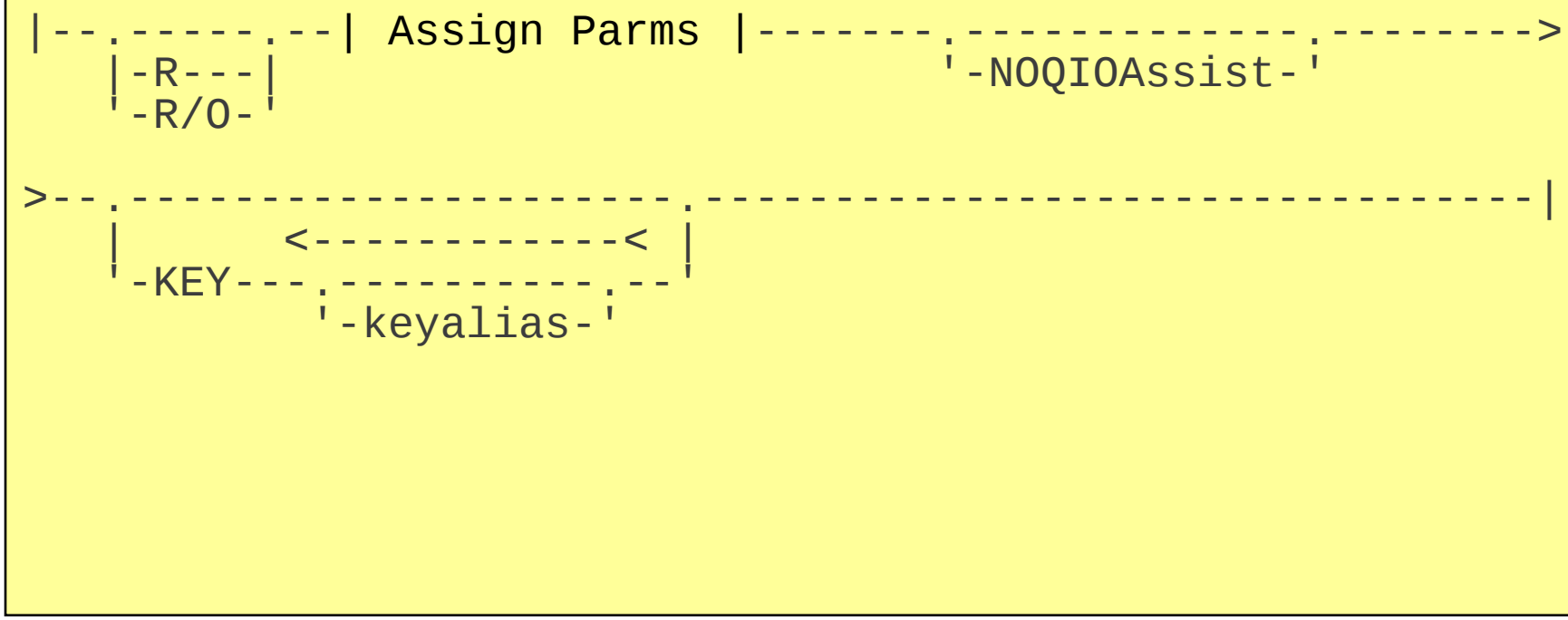
```
SET KEYA 1K1L LABEL KEYL tape_sol_tst_shr_pvt_1024_lbl_01
Ready; T=0.01/0.01 16:14:21
SET KEYA 1K1H HASH  KEYL 'tape sol tst shr pvt 1024 lbl 01'
Ready; T=0.01/0.01 16:14:28
q keya 1k1l
KEYALIAS: (L) 1K1L
        = TAPE_SOL_TST_SHR_PVT_1024_LBL_01
Ready; T=0.01/0.01 16:14:33
q keya
KEYALIAS: (L) 1K1L
        = TAPE_SOL_TST_SHR_PVT_1024_LBL_01
KEYALIAS: (H) 1K1H
        = TAPE SOL TST SHR PVT 1024 LBL 01
Ready; T=0.01/0.01 16:14:39
```

z/VM Support – Enable Encryption

- ATTACH Command (Class B)
  - Defines the encryption settings to be used for a guest that is unaware of tape encryption
  - An unmodified ATTACH will inherit any encryption settings already associated with the tape drive
    - e.g., ATTACH MULTIUSER, DETACH LEAVE
  - Can be used with shared tape, provided each guest uses the same encryption settings
  - Drive must not contain a tape cartridge, or the mounted cartridge must be positioned at BOT
    - Ensures all data on a cartridge is consistent

ATTACH Command Syntax

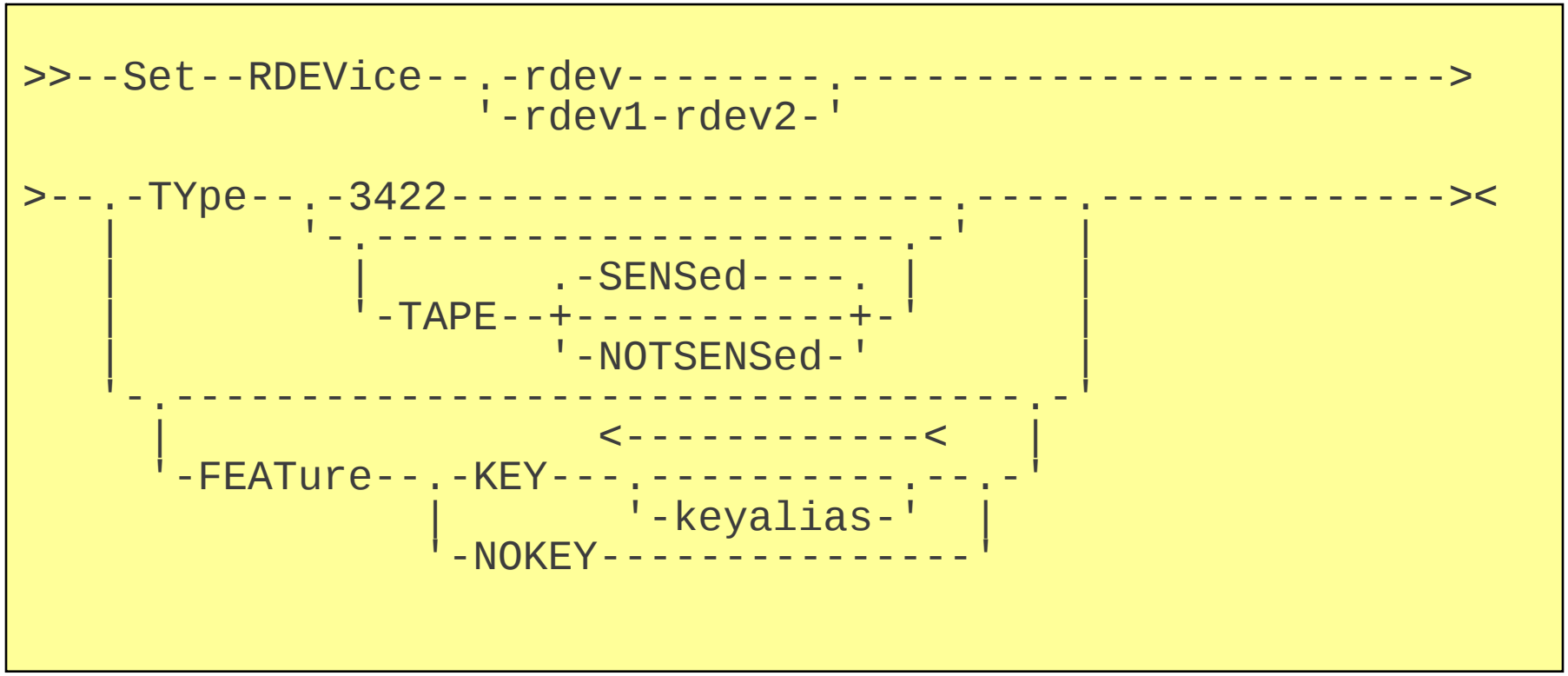
Options for Shared/Dedicated Tape Device:



z/VM Support – Enable Encryption

- SET RDEVice Command (Class B)
  - Defines the encryption settings to be used for a guest that is unaware of tape encryption, while permitting ATTACH to be issued without any changes
    - Will be superseded by encryption options on the ATTACH command, if any are specified
  - Target RDEV must be free and online
    - This differs from the existing SET RDEVice command, which expects the specified rdevice(s) to be varied offline

SET RDEVice Command Syntax



z/VM Support – Disable Encryption

- DETACH Command
  - Cleans up encryption settings on a device
  - SET RDEVice encryption settings are not affected
    - Rather, they are removed by a SET RDEVice command with the NOKEY option
  - If DETACH is issued with the LEAVE option, the encryption settings will not be removed since the cartridge is not being ejected from the drive
    - Subsequent ATTACH should not specify any encryption settings

z/VM Support – Query Encryption

- DIAGNOSE x210
  - The Virtual/Real Device Characteristics block that is returned on a Diagnose x210 code has been updated to return a new underlying device type, x13, that indicates a 3592 Model E05 drive that has been enabled for encryption

```
d210 181
DEVNUM =>0181<
VRDCBLOK =>0181005F 08830100 08831008 13000000
           35920635 90100190 4EDC0000 B4D7FD5C
           69E00000 00000000 35920635 92140013
           0E001001 00000100 46838000 04000000
           04000011 22C00000 00000000 00000000
           00000000 00000000 00000000 000000<
Good Condition code from diagnose
Ready; T=0.01/0.01 17:14:12
```

z/VM Support – Query Encryption

- Query TAPe DETails Command (Class B)
  - Displays encryption capability
  - Shows active (ATTACH) and/or inactive (SET RDEVICE) KEK Label information
    - “DEFAULT” is displayed if encryption was enabled but no KEK Labels were specified
- Query Virtual Commands (Class G)
  - Query Virtual TApes displays encryption capability
  - Query Virtual <device> DETAILS displays active (ATTACH) and/or inactive (SET RDEVICE) KEK Label information
    - “DEFAULT” is displayed if encryption was enabled but no KEK Labels were specified

z/VM Support – Query Encryption

- “DETAILS” commands have been updated
  - ACTIVE heading now shows what is currently being used on the tape drive, regardless of what was specified on ATTACH
  - New ATTACHED heading will display that information, if different
  - Provides information about encryption environment
    - When tape is not written immediately after initial mount, or
    - When tape is rekeyed

z/VM Support – Query Encryption

```
q tape details 7e2
TAPE 07E2 SEQUENCE NUMBER E0010 LIBPORT 1 ENCRYPTION CAPABLE
  ACTIVE KEY LABEL(S):
    (H) Erics Public Key
    (L) MAHNA MAHNA
  INACTIVE KEY LABEL(S): DEFAULT
Ready; T=0.01/0.01 01:32:41
q v tapes
TAPE 0181 ON DEV  07E2 3590 R/W SUBCHANNEL = 0008 ENCRYPTION CAPABLE
Ready; T=0.01/0.01 01:43:28
q v 181 details
TAPE 0181 ON DEV  07E2 3590 R/W SUBCHANNEL = 0008 ENCRYPTION CAPABLE
  ACTIVE KEY LABEL(S):
    (H) Erics Public Key
    (L) MAHNA MAHNA
  INACTIVE KEY LABEL(S): DEFAULT
Ready; T=0.01/0.01 01:44:09
```

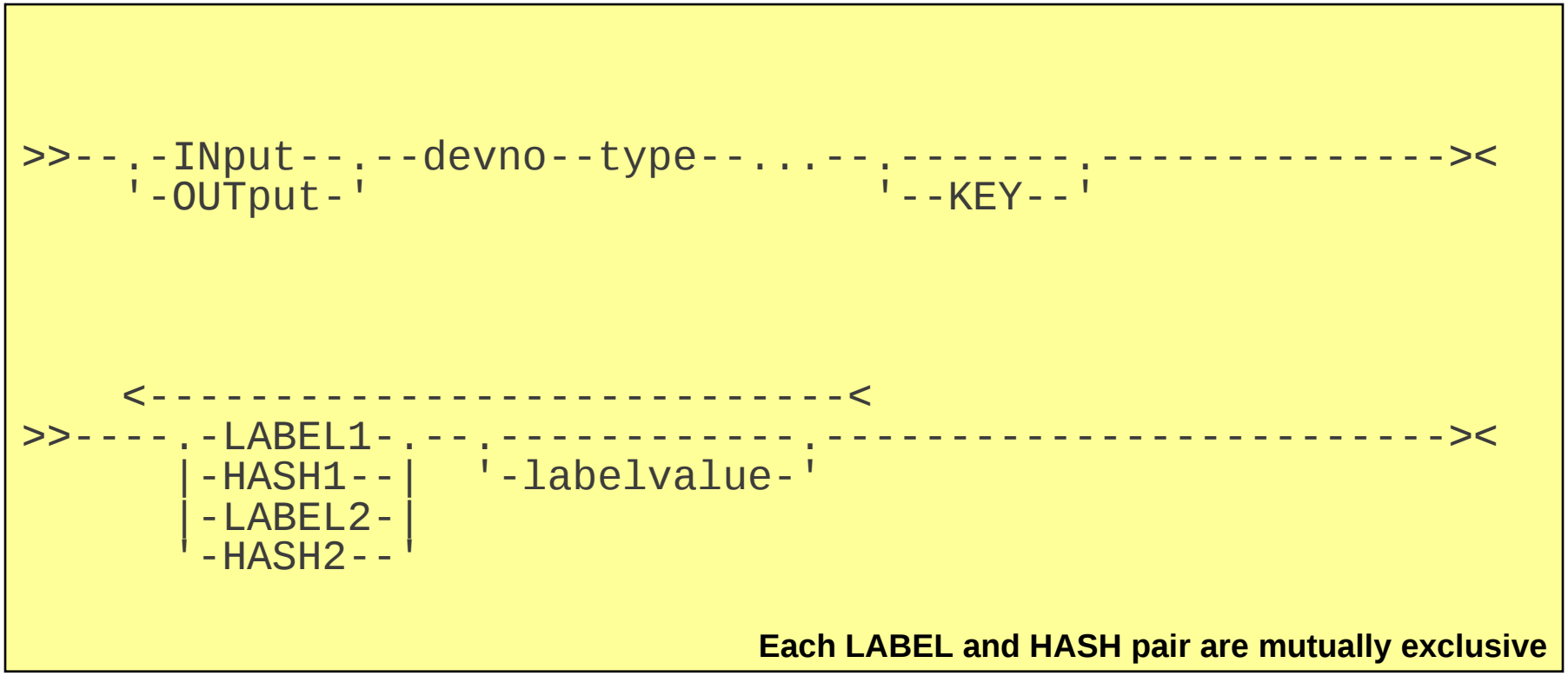
z/VM Support – Query Encryption (alternate keys)

```
q tape details 7e2
TAPE 07E2 SEQUENCE NUMBER E0010 LIBPORT 1 ENCRYPTION CAPABLE
  ACTIVE KEY LABEL(S):
    (H) Erics Public Key
    (H) Temporary Public Key
  ATTACHED KEY LABEL(S):
    (H) Erics Public Key
    (L) MAHNA MAHNA
  INACTIVE KEY LABEL(S): DEFAULT
Ready; T=0.01/0.01 04:17:22
```

z/VM Support – DASD Dump Restore

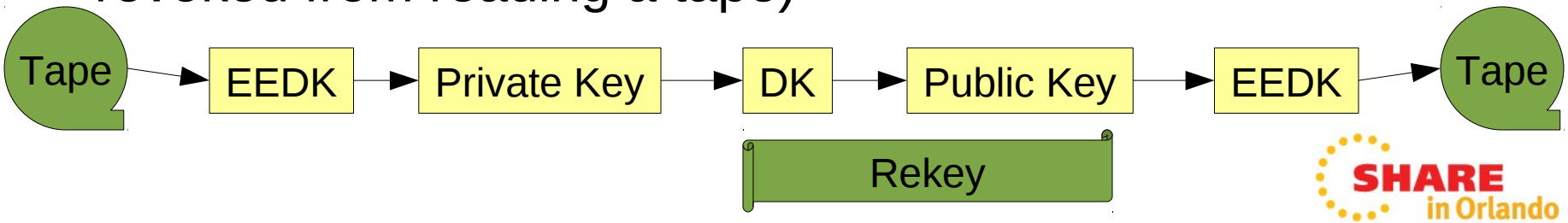
- DDR, used for backing up volumes to tape, has been updated to encrypt data via new control statements
  - If being run from within CMS virtual machine, can take advantage of same ATTACH parameters as any other guest, without changing the control statements that are issued
- INPUT/OUTPUT control statement has a “KEY” option to enable encryption with the use of the EKM “default”
  - “KEY” option is only valid on OUTPUT statement when target device is an encryption-capable tape drive

z/VM Support – DASD Dump Restore syntax



z/VM Support – Rekey operation

- Provides the ability to re-encrypt (“rekey”) a given tape cartridge with a different set of KEK Labels, without having to duplicate the tape
  - Requires hardware microcode to use this function
- Eases management of encrypted tapes if the KEK certificates expire after a given time period, or have been compromised
- Tapes originally destined for one user can be made readable by third-parties (conversely, users can be revoked from reading a tape)



z/VM Support – Initiate Rekey

- SET TAPE Command (Class B)
  - Defines the encryption settings that are to replace those defined on the specified tape device's mounted cartridge
  - Target RDEV must be mounted with an encrypted tape cartridge

```
>>--Set--TAPE--.-rdev--------.--REKEY--keyalias1--.-----------.--><
               '-rdev1-rdev2-'                     '-keyalias2-'
```

FIN

Backup Charts

You don't have to take my word for it

- Additional information
  - Redbook “IBM System Storage TS1120 Tape Encryption: Planning, Implementation, and Usage Guide”
    - Order Number SG24-7320
  - “IBM Encryption Key Manager component for the Java platform Introduction, Planning, and User's Guide”
    - Order Number GA76-0418

Other z/VM stuff that changed

- SPXTAPE, GIVE
  - No changes to code, but will honor encryption settings associated with the affected device
- Monitor
  - MRMTRDEV (Monitor Domain: Device Configuration Data)
    - New bit in MTRDEV_CALFLAGS
  - MRIODVON (I/O Domain: Vary On Device)
    - New bit in IODVON_CALFLAGS
  - MRIODDEV (I/O Domain: Device Activity)
    - New bit in IODDEV_CALFLAG1