z/TPF EE V1.1
z/TPFDF V1.1
TPF Toolkit for WebSphere® Studio V3
TPF Operations Server V1.2

IBM Software Group

TPF Users Group Spring 2007

Tape Encryption

Name :John Tarby
Venue : SCP subcommittee

AIM Enterprise Platform Software

IBM z/Transaction Processing Facility Enterprise Edition 1.1.0

Any references to future plans are for planning purposes only. IBM reserves the right to change those plans at its discretion. Any reliance on such a disclosure is solely at your own risk. IBM makes no commitment to provide additional information in the future.

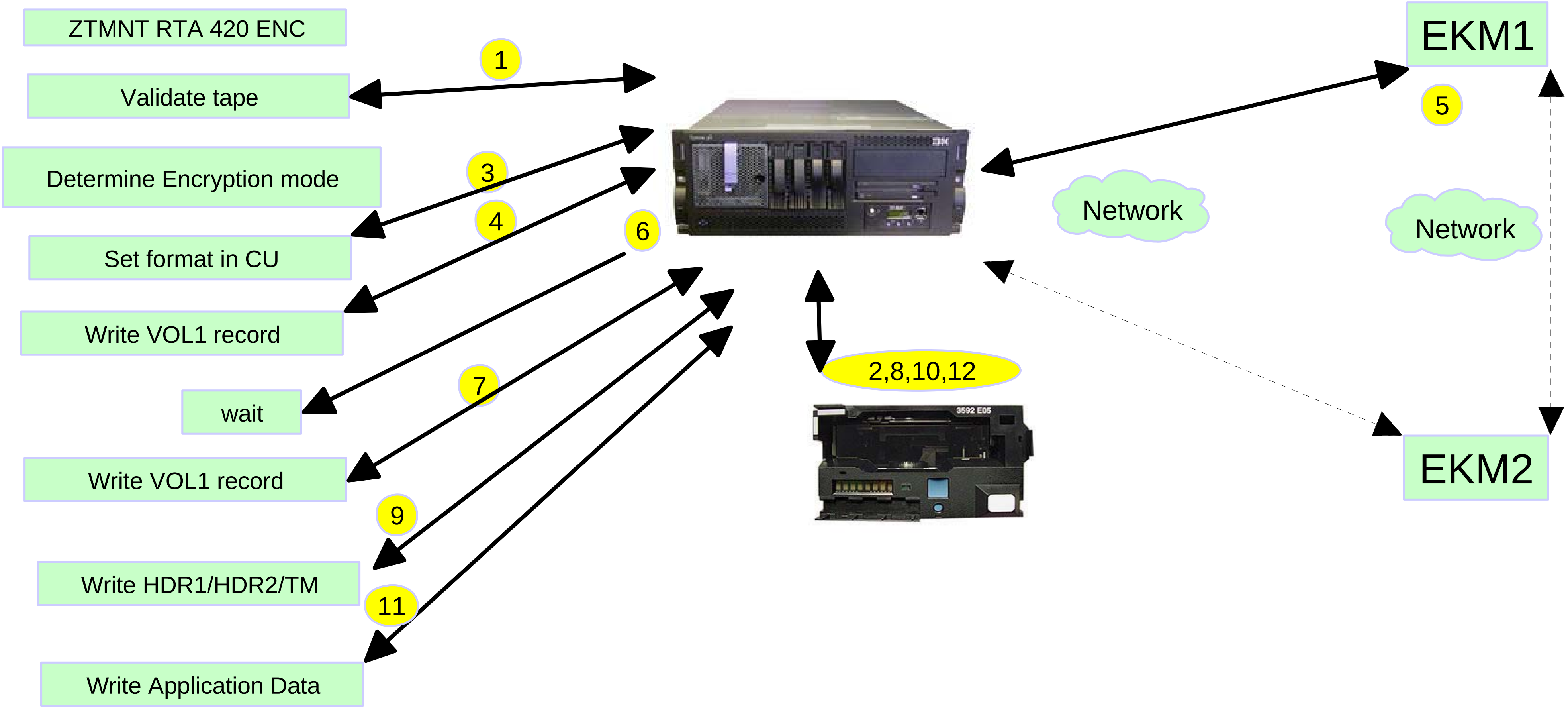
Tape Encryption and TS1120 (3592-E05 emulation) Support

- z/TPF apar PJ31479
- Adds support for TS1120 drives in E05 mode
  - Drives that are Encryption Enabled as well as Encryption Capable
  - 500 gig capacity with standard cartridges
  - 100 gig capacity for short cartridges
  - 700 gig capacity with extended cartridges
- In general
  - New format is F896TRK
  - ENC/NOENC terminology is used throughout z/TPF commands
  - Java based Encryption Key Manager (EKM) is required
  - z/TPF has no knowledge of keys used by the EKM for tape encryption.

Tape Encryption concepts

- EKM resides outside of z/TPF
  - Key negotiation handled between the tape control unit and the EKM over a TCP/IP connection.
  - Runs on a java machine with TCP connectivity to the CU
  - Control unit supports connectivity to two key managers at different IP addresses for redundancy.
    - Key stores must be kept in sync if two EKMs are used
- The decision to encrypt a tape is made at ZTMNT or automount time, it is not controlled by the application.
  - Entire tape is encrypted (aside from the labels)
- Encryption characteristics must match between active and ALT tape for tape switch
  - Standby tapes are always mounted with the same encryption setting as the active.

The picture that's worth 1000 words



What controls the tapes that are encrypted?

- ZTLBL sets attributes for a given tape name
  - Output only
    - Input tapes inherit the attribute of the volume being mounted
    - Just like compaction
  - Existing tapes are NOENC unless altered
  - New tapes are also NOENC unless specified
- ZTMNT can override what is set in the tape label
  - ZTMNT RTA 420 ENC or
  - ZTMNT RTA 420 NOENC
- TOPNC has no control over tape encryption settings
  - Applications do not need to be updated
- If application data is already encrypted then it can be written to any tape
  - The drive does not have to support encryption
  - Data would need to be decrypted by the application when read

How will I know that a tape is encrypted?

- Tape messages will indicate ENC/NOENC to identify the encryption attribute

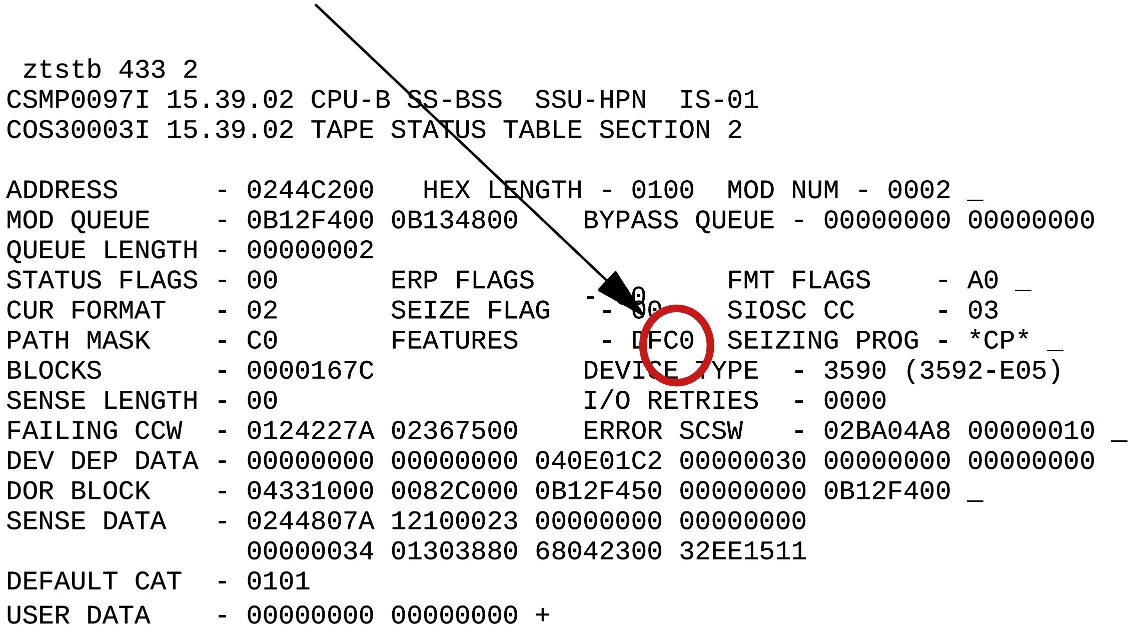
```
COTM0310I 14.50.42 TMNT BSS    TAPE RTL MOUNTED ON DEVICE 0433
          VSN TPF509 G0002 S0001 F896TRK SL B128             2 NOCOMP NOENC
```

- Tape status table section 1, tertiary indicator has a bit that says the current tape is mounted as encrypted
  - Valid for input and output, including ALT
  - bit CT3ENC x'02'

```
COTE0002I 15.39.02 DTAP      - TAPE STATUS

ADDRESS   NAME   SSU    STATUS   TPIND     VOLSER  FORMAT      #BLOCKS LDR

0420      RTA    BSS      AO    00 01 20   A00186   38K2             6 YES
0433      RTL    BSS      AO    22 01 22   TPF509  896TRK         5756 LIB

END OF DISPLAY+
```

How can I tell that a tape drive supports encryption?

- Second features byte in ZTSTB cuu 2 will give encryption capability status
  - This does not mean that the volume currently mounted is encrypted, just that the device is capable of encryption
  - CTS2ENC - X'40'



```
 ztstb 433 2
CSMP0097I 15.39.02 CPU-B SS-BSS  SSU-HPN  IS-01
COS30003I 15.39.02 TAPE STATUS TABLE SECTION 2

ADDRESS       - 0244C200   HEX LENGTH - 0100  MOD NUM - 0002 _
MOD QUEUE     - 0B12F400 0B134800    BYPASS QUEUE - 00000000 00000000
QUEUE LENGTH  - 00000002
STATUS FLAGS  - 00       ERP FLAGS     - 0      FMT FLAGS    - A0 _
CUR FORMAT    - 02       SEIZE FLAG     - 00    SIOSC CC     - 03
PATH MASK     - C0       FEATURES       - DFC0  SEIZING PROG - *CP* _
BLOCKS        - 0000167C            DEVICE TYPE   - 3590 (3592-E05)
SENSE LENGTH  - 00                  I/O RETRIES   - 0000
FAILING CCW   - 0124227A 02367500    ERROR SCSW    - 02BA04A8 00000010 _
DEV DEP DATA  - 00000000 00000000 040E01C2 00000030 00000000 00000000
DOR BLOCK     - 04331000 0082C000 0B12F450 00000000 0B12F400 _
SENSE DATA    - 0244807A 12100023 00000000 00000000
                00000034 01303880 68042300 32EE1511
DEFAULT CAT   - 0101
USER DATA     - 00000000 00000000 +
```

Are encrypted tapes slower?

- Short answer... NO
  - "At all transaction sizes and compression ratios, the TS1120 write data rates with encryption-enabled matches the high write data rates of the TS1120 (non-encrypting) tape drive."
  - ~80 meg/sec with 128K blocksize*
- Long answer... mounts take longer.
  - z/TPF must wait for key exchange between the CU and the EKM
  - z/TPF also must wait for the tape format information to be re-written when a new key is used.
  - Both delays occur when VOL1 is being written
- No delays at tape switch time.
  - This is why ALT tapes are mounted as encrypted or unencrypted

*z/TPF guest under VM... for example purposes only, your mileage may vary

Aside from PJ31479, what else do I need?

- IBM Encryption Key Manager component for the Java platform (EKM)
  - http://www-1.ibm.com/support/docview.wss?&uid=ssg1S4000504
  - The EKM is supported on z/OS, i5/OS, AIX, Linux, HP-UX, Sun Solaris & Windows.
- TCP/IP connectivity from the tape control unit to the EKM above
- TS1120 Encryption Enabled tape drive
- TS1120 model C06 tape controller or 3590-J70 tape controller

Other tape encryption options

- TS7700 (VTS)
  - Encryption support included with the R1.2 code level
    - GA 3/9/07
  - Tape data is written as encrypted when it is moved from cache to tape
  - Requires TS1120 encryption enabled drives as the back end storage for the VTS.
  - Translucent to TPF
    - User exit CORU allows Advanced Policy Managment (APM) attributes to be set when a tape is loaded.
    - TPF 4.1 APAR PJ31643
    - z/TPF APAR PJ31934

- Application encrypted data
  - No specific hardware requirements
  - Application encrypts and decrypts data on its own.

Additional Resources

- IBM System Storage TS1120 Tape Encryption Planning, Implementation, and Usage Guide
  - http://www.redbooks.ibm.com/abstracts/sg247320.html
- TS7700 Encryption Support White Paper
  - ftp://ftp.software.ibm.com/storage/Encryption/TS7700_Encryption_Support_V10.pdf

Trademarks

IBM, z/OS. i5/OS, and AIX are trademarks of International Business Machines Corporation in the United States, other countries, or both.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
Windows is a trademark of Microsoft Corporation in the United States, other countries, or both.
UNIX is a registered trademark of The Open Group in the United States and other countries.
Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

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.

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.

This presentation and the claims outlined in it were reviewed for compliance with US law. Adaptations of these claims for use in other geographies must be reviewed by the local country counsel for compliance with local laws.