

Implementing the IBM 3485 ATL with IBM 3592-J1A Encryption Support: Part One

By Lloyd Christensen

Introduction

I am a consultant specializing in the implementation of automated tape libraries and virtual tape systems in the z/OS environment. This past summer I was brought in by my client, one of the world's largest financial institutions, to assist with implementing IBM's 3485 Automated Tape Library along with their latest version of the 3592 tape drive. The goal of the project was to encrypt all data sent between their data centers or to off-site storage vendors. The deadline for implementation in all four North American data centers was November 1st.

This series of articles will cover:

Part 1:

- (a) An overview of the scope of the project
- (b) the implementation of the IBM 3485 libraries in each site with base library support
- (c) the implementation of the IBM 3592 tape drives with encryption support

Part 2:

- (d) disaster recovery testing using the encrypted media along with
- (e) IBM's latest virtual tape server (the Hydra) in a Peer-to-Peer configuration

Scope

The project's scope included:

1. Encrypting any tape being sent from any domestic data center to any other domestic data center or to an off-site storage vendor.
2. The client has four data centers located in Maryland, New Jersey, Nevada, and Texas.

```

Row 1 of 1 More: >
Command ==> _____ Scroll ==> PAGE

Control unit number      : F001      IBM TAPE PORT-C2 SERIAL#A1167-1
Control unit type       : 3590      Serial number . . . :

Connected switch.ports: C8.02

ENTER to continue.

-----Channel Path ID . Link Address-----
Proc.CSSID 1----- 2----- 3----- 4----- 5----- 6----- 7----- 8-----
TXCE540E.0 80.02   CO.02
    
```

Figure 1: View Control Unit Definition

```

Row 1 of 1
Command ==> _____ Scroll ==> PAGE

Select one or more processors to view the device candidate list, or
ENTER to continue without selection.

Device number . : F000,16      Device type . : 3590

          Preferred Device Candidate List
/ Proc.CSSID SS UA Time-Out STADET CHPID Explicit Null
# TXCE540E.0  00 No      Yes      No      _____
    
```

Figure 2: View Device / Processor Definition

3. There are multiple sysplex environments in each location. In some cases multiple sysplexes would share the hardware configuration. In others, each sysplex had its own hardware configuration.
4. The hardware solution is IBM's Encryption capable 3592 drives. These drives were made available for Beta testing on August 14th and officially announced on August 29th.
5. For the Proof of Concept (POC), an IBM 3584 Tape Library was installed in Maryland and connected to three hosts we will call TST1, TST2, and TST3.
6. The POC environment included ten (10) non-encryption capable 3592 tape drives and ten (10) encryption capable 3592 tape drives.
7. TST1 was a z/OS V1.6 system with DFSMS/rmm as the tape management product.
8. TST2 was a z/OS V1.7 system with DFSMS/rmm as the tape management product.
9. TST3 was a z/OS V1.7 system with CA-1™ as the tape management product.
10. Key management is the responsibility of the MVS group.
11. All of this client's businesses will use a single encryption key.
12. Tapes sent to business partners will be encrypted using a software product, MegaCrypton, and are not included in this text.
13. Electronic exchange between sites can use software encryption within products like NDM.

Customer Configuration

My client has been one of Sun/STK's largest customers for many years. The decision to implement the IBM 3485 ATL was a difficult one. The driving factors were an internal requirement to have all "net new" off-site tape data encrypted by November 1st and the inability of Sun/STK to have a deliverable encryption-capable drive in time to meet that deadline.

As I mentioned before, the customer has multiple data centers. I am going to concentrate on just one, the more complex site. This facility has a single Sun/STK Automated Cartridge System (ACS) consisting of fourteen (14) 9310 Powderhorn libraries with pass-thru ports allowing tapes to be exchanged between them. Within these fourteen libraries are 320 Sun 9840 and 56 Sun 9490 Timberline tape drives.

There are also seven (7) VSM-4s and one VSM-3 virtual tape servers. The total effective cache of these virtual tape subsystems is approximately 40 Terabytes. The one VSM-3 is located in a remote site.

This facility has multiple sysplex environments. One complex supports a consumer finance institution and will be referred to in this text as CONSUMER. Another complex supports large banking customers and will be referred to in this text as PRIVATE. CONSUMER includes multiple z/OS V1.7 hosts with a single CA-1 Tape Management Catalog. The PRIVATE complex includes multiple z/OS V1.6 and V1.7 hosts with multiple IBM DFSMS/rmm tape management complexes. All tape drives are defined via HCD to all hosts but are varied online/offline via CAMIM and dedicated to specific hosts.

IBM 3485 Automated Tape Library

We installed two IBM 3485 Automated Tape Libraries (ATL). Each library consists of two (2) L-23 Library Manager frames, nine (9) D-23 drive frames, and two (2) High-Availability frames. Each library has two "robots" and each "robot" is functional and in use all of the time. Each library has 55 IBM 3592 J1A tape drives. Each drive has the encryption feature enabled. Please note that only one of the two L-23 frames are within the library itself. The second L-23 is located inside one of the 3592-C06 control units.

External to the ATL are six (6) 3592-C06 control units. Each control unit can support

```

Row 1 of 10
Command ==> _____ Scroll ==> PAGE

Configuration ID . : CONS          USED FOR CONSUMERS
Device number   . : F000,16      Device type . . . : 3590
Generic / VM device type . . . . : 3590-1

ENTER to continue.

Parameter/
Feature        Value      Description
OFFLINE        Yes       Device considered online or offline at IPL
DYNAMIC        Yes       Device supports dynamic configuration
LOCANY         Yes       UCB can reside in 31 bit storage
LIBRARY        Yes       Device supports auto tape library
AUTOSWITCH     Yes       Device is automatically switchable
LIBRARY-ID     A1167    5 digit library serial number
LIBPORT-ID     01       2 digit library string ID (port number)
MTL            Yes       Device supports manual tape library
SHARABLE       Yes       Device is Sharable between systems
COMPACT        Yes       Compaction
  
```

Figure 3: View Device Parameter / Feature Definition

```

Row 1 of 1
Command ==> _____ Scroll ==> PAGE

Configuration ID . : CONS          USED FOR CONSUMERS
Device number   . : F000,16      Device type . . . : 3590
Device type     . . . . . Generic . . . . . : 3590-1

List of EDT/esoterics to which device is assigned. ENTER to continue.

EDT.Esoteric
00.IBM3590
  
```

Figure 4: View Device Parameter / Feature Definition

```

CDS Name . . . : ACTIVE
Library Name . : LNJA1107 Device Type . . : 3584-L22
Library Type . : AUTOMATED Library Id . . : A1107

Description . . : IBM 3594 LIBRARY

Console Name . . . . . :
Entry Default Data Class . :
Entry Default Use Attribute : PRIVATE
Eject Default . . . . . : KEEP

Media Type:      Media1  Media2  Media3  Media4  Media5
Scratch Threshold: 0      0      0      0      50
Scratch Number:  0      0      0      0      63
Media Type:      Media6  Media7  Media8  Media9  Media10
Scratch Threshold: 0      0      0      0      0
Scratch Number:  0      0      0      0      0

Use DOWN Command to View next Panel;
Use HELP Command for Help; Use END Command to Exit.

CDS Name . . . : ACTIVE
Library Name . : LNJA1107
Library Type . : AUTOMATED
Device Type . . : 3584-L22
Library Id . . . : A1107

Number of Slots . . : 959
Empty Slots . . . . : 477
Initial Online Status:
CNS1:      YES  CNS2: YES          PVT1:      YES  PVT2:      YES
  
```

Figure 5: DF/SMS Library Definition

up to twenty (20) tape drives; we configured ours so that five controllers each support nine (9) drives and one supports ten (10) drives. The C06 controller can support up to twenty (20) drives. The IBM 3592 drives can have encryption enabled or disabled; however, all drives behind a 3592-C06 controller must have the same features enabled. In our case all drives in the production libraries have the encryption feature enabled. Use of the encryption feature is established by the DATACLAS so you can have the feature enabled but not use it. In our case all data sent to the IBM libraries will be encrypted.

The IBM tape libraries are defined to the operating system via the IBM Hardware Configuration Definition (HCD). The HCD definition for a library requires a unique serial number. We used the serial number of one of the L-23 frames. The tape drives are also defined via HCD and the HCD definitions include the library name in which the drive resides.

Figure 1 shows the HCD definition for a controller with Control Unit Address F001. Figure 2, Figure 3, and Figure 4 show the HCD definition for the tape drives in the F000—F00F range.

DF/SMS Definitions

Library Definition: The IBM ATL also has to be defined to DF/SMS using ISMF. Use ISMF Option 10.3.1 to define the library to ISMF. In figure 5 the Library Id (A1107) is the serial number of the L-23 frame and must match the library id specified when defining the library via HCD.

In Figure 5 we have set a scratch threshold for Media-5 at fifty (50) tapes. When the scratch count for that media type drops to 50, an appropriate message is written to the operator console. We are only using one media type in our production libraries (Media-5). Please keep in mind that this number is a total number of scratch tapes of the specified media type. IBM does not support scratch pools like Sun does. I will discuss how to use multiple tape pools a little later.

Storage Group Definition: IBM tape libraries are assigned to a Storage Group through ISMF Option 6. The Storage Group is defined as TYPE=TAPE. The specific library names that are to be a part of the storage group are identified. An example of our definition of a Storage Group called “SGIBMTP” is in Figure 6.

```
CDS Name : ACTIVE

Enter Line Operators below:

      LINE      STORGRP  CYCLE    LIBRARY  LIBRARY  LIBRARY  LIBRARY
      OPERATOR  NAME      END TIME NAME     NAME     NAME     NAME
---(1)---  --(2)---  --(28)-- --(29)-- --(30)-- --(31)-- --(32)--
              SGIBMTP      ----  LNJA1107 LNJA1111 -----
---(2)---  --(2)---  --(28)-- --(29)-- --(30)-- --(31)-- --(32)--
              SGIBMTP1     ----  LNJA1107 -----
---(3)---  --(2)---  --(28)-- --(29)-- --(30)-- --(31)-- --(32)--
              SGIBMTP2     ----  LNJA1111 -----
```

Figure 6: DF/SMS Storage Group Definition

```

                                DATA CLASS DISPLAY                                Page 3 of 5
Command ==>

CDS Name . . . : CITI.SCDS
Data Class Name : DCNCRCTW

Encryption Management
Key Label 1: KM_COMPANY_WIDE
Encoding for Key Label : L

Key Label 2: KM_COMPANY_WIDE
Encoding for Key Label 2: L

CDS Name . . . . . : ACTIVE
Data Class Name . . : DCNCRCTW

Data Set Name Type . . . . . :
If Extended . . . . . :
Extended Addressability . . : NO
Record Access Bias . . . . . :
Space Constraint Relief . . . : NO
Reduce Space Up To (%) . . . :
Dynamic Volume Count . . . . :
Compaction . . . . . : YES
Spanned / Nonspanned . . . . :
Media Interchange
Media Type . . . . . : MEDIA5
Recording Technology . . . . : EEFMT2
Performance Scaling . . . . . :
Performance Segmentation . . :
Use UP/DOWN Command to View other Panels;
Use HELP Command for Help; Use END Command to Exit.

CDS Name . . . : ACTIVE
Data Class Name : DCNCRCTW

Encryption Management
Key Label 1: ENCRYPTION.SERVER.2006.01
Encoding for Key Label 1 : L

Key Label 2:
Encoding for Key Label 2 :
```

Figure 7: DF/SMS Data Class Definition

I recommend that in a multiple library environment like this one that you define multiple storage groups. For example, we have two libraries in this environment. There should be three storage groups. One, SGIBMTP, includes both libraries (LNJA1107, LNJA1111). Each library should also have its own storage group (example: SGIBMTP1 and SGIBMTP2). When you route an allo-

cation to the storage group SGIBMTP, any drive in either library can be used. If you want to route an allocation to a specific library, you need to be able to send it to a storage group that only contains that library. This was a problem for us when using CA-1’s tape initialization program—drives were selected without regard for which library the tapes were in.

```

/*-----*/
/* Add filter lists for IBM 3592 Tape drives with and without */
/* encryption enabled. */
/*-----*/
FILTLIST DC_IBMTAPE          INCLUDE('DCNCRCTW')
FILTLIST DC_IBM_LIB1        INCLUDE('IBMLIB1')
FILTLIST DC_IBM_LIB2        ICNLUDE('IBMLIB2')
FILTLIST DC_IBM_LIBS        INCLUDE('IBMLIBS')
FILTLIST DC_DSN_NCRYPT_CTW   INCLUDE(**.IBMTAPE.ENCRYPT.***)
/*-----*/
/* Add routines to assign DATACLAS for IBM Tape whether using */
/* encryption or not. */
/*-----*/
SELECT
  /*-----*/
  /* Honor specific IBM Tape DATACLAS Request */
  /*-----*/
  WHEN (&DATACLAS = DC_IBMTAPE)
  DO
    SET &DATACLAS = &DATACLAS
    WRITE 'DC SPECIFICALLY REQUESTED: ' &DATCLAS
    EXIT
  END
  /*-----*/
  /* Honor specific IBM Tape Library Request */
  /*-----*/
  WHEN (&UNIT = &DC_IBM_LIB1)
  DO
    SET &DATACLAS = 'DCIBMTP1'
    WRITE 'DC SET BECAUSE OF UNIT REQUESTED'
    EXIT
  END
  WHEN (&UNIT = &DC_IBM_LIB2)
  DO
    SET &DATACLAS = 'DCIBMTP2'
    WRITE 'DC SET BECAUSE OF UNIT REQUESTED'
    EXIT
  END
  WHEN (&UNIT = &DC_IBM_LIBS)
  DO
    SET &DATACLAS = 'DCNCRCTW'
    WRITE 'DC SET BECAUSE OF UNIT REQUESTED'
    EXIT
  END
  WHEN (&DSN = &DC_DSN_NCRYPT_CTW)
  DO
    SET &DATACLAS = 'DCNCRCTW'
    WRITE 'DC SET BY DSN PATTERN MATCH'
    EXIT
  END
END

```

Figure 8: DATACLAS ACS Code Additions

```

/*-----*/
/* Add filter lists for IBM 3592 Tape drives by DATACLAS values */
/*-----*/
FILTLIST SC_IBMTAPE        INCLUDE('DCNCRCTW',DCIBMTP*)
/*-----*/
/* Add routine to assign any allocation with the IBM Tape DATACLAS */
/* values to STORCLAS='SCIBMTAP' and pass on to STORGRP */
/*-----*/
SELECT
  WHEN (&DATACLAS = SC_IBMTAPE)
  DO
    SET &STORCLAS = 'SCIBMTAP'
    EXIT
  END

```

Figure 9: STORCLAS ACS Additions

```

SELECT
  WHEN (&DATACLAS = 'DCNCRCTW')
  DO
    SET &STORGRP = 'SGIBMTP'
    WRITE 'SG SET BY DATACLAS'
    EXIT
  END
  WHEN (&DATACLAS = 'DCIMBTPS')
  DO
    SET &STORGRP = 'SGIBMTPS'
    WRITE 'SG SET BY UNIT REQUEST'
    EXIT
  END
  WHEN (&DATACLAS = 'DCIMBTP1')
  DO
    SET &STORGRP = 'SGIBMTP1'
    WRITE 'SG SET BY UNIT REQUEST'
    EXIT
  END
  WHEN (&DATACLAS = 'DCIMBTP2')
  DO
    SET &STORGRP = 'SGIBMTP2'
    WRITE 'SG SET BY UNIT REQUEST'
    EXIT
  END
END

```

Figure 10: STORGRP ACS Additions

Data Class Definition: Data is directed to the IBM library and to encrypted tape through the ACS routines that assign a DATACLAS value. The DATACLAS definition uses a new value, the key label for the encryption key(s). In our case the encryption key labels themselves are defined via ICSF, our key manager. An example of a DATACLAS definition is shown in Figure 7.

DF/SMS ACS Code Additions: We have defined a data class, DCNCRCTW, which will write to Media-5 category tape and will encrypt the data using the ICSF defined key label: **ENCRYPTION.SERVER.2006.01**. We have to identify the data that should be assigned this data class. In our case we built multiple filter lists in the ACS code based upon entries in the DFSMS/rmm Vital Records Specification or the CA-1 Vault Pattern Data Set. We also allow specific requests by DATACLAS name and by esoteric device name.

Datasets get assigned to the encrypted tape devices only by assigning a DF/SMS DATACLAS with the encryption attributes (for example, DCNCRCTW). The DATACLAS may be assigned by:

- ▼ Specific request through JCL
- ▼ Requesting an esoteric device name (for example: E3592CTW) that the DF/SMS DATACLAS ACS code will then assign to the appropriate DATACLAS (DCNCRCTW)
- ▼ Meeting some selection criteria such as Data Set Name, program name, DD name, etc. in the DF/SMS

DATACLAS ACS code and being assigned an appropriate DATACLAS (DCNCRCTW)

The ACS code following has a filter list of encryption-enabled DATACLAS names. A specific request for one of these names will be honored. Filter lists for esoteric device names—and these do not need to be defined to MVS—can also be checked and assigned specific corresponding DATACLAS values. Finally there are filter lists for Data Set Name patterns that will be assigned the appropriate DATACLAS (DCNCRCTW). See Figures 8, 9 and 10.

Using Multiple Scratch Pools

The IBM ATL does not support multiple scratch pools within a tape management system like the Sun/STK libraries do; however, you can use multiple scratch pools coming from different tape management systems. In our case we have seven different tape management complexes (a mix of DFSMS/rmm and CA-1) sharing these two libraries.

We have two hosts in the Consumer environment, CNS1 and CNS2. Each has its own CA-1 tape management system. In the DEV-SUPxx members for each host we have to specify a category number for each media type. The IBM ATL gets the category number from the DEVSUPxx member and stores the category number along with the volume serial number its inventory.

For example, on CNS1 and CNS2 our DEVSUPxx parmlib members include:

CNS1	CNS2
MEDIA5=0015	MEDIA5=0025
MEDIA7=0017	MEDIA7=0027

Within the tape management catalog on CNS1 we have volumes B0000B—B3999B. Tapes entered into the library get assigned a category of '0015' (for Media-5). On CNS2 we have volumes C0000C—C0299C. Tapes entered into the library get a category code of '0025' (for Media-5).

In an environment with multiple tape management catalogs and DFSMS/rmm it is necessary to specify the parm REJECTANY-USE(*). When a volume is entered into the IBM library and you have RMM tape management catalogs, the volume will be automatically defined to every RMM tape catalog. If you have multiple RMM control data sets, it may be used by the wrong system. Specifying REJECTANYUSE(*) in the RMM

```
//STEP001 EXEC PGM=IEBDG
//SYSPRINT DD SYSOUT=*
//OUTDSN DD DSN=my-tsoid.TCX544.IBMTAPE.ENCRYPT.CNS1.D1128,
// DISP=(NEW,CATLG,DELETE),
// RECFM=FB,LRECL=80,BLKSIZE=0,
// UNIT=CART,LABEL=(1,SL,RETPD=1),DATACLAS=DCNCRCTW
//SYSIN DD *
DSD OUTPUT=(OUTDSN)
FD NAME=TEXT1,LENGTH=80,FORMAT=AL,ACTION=RP,STARTLOC=1
REPEAT QUANTITY=1000
CREATE QUANTITY=2500,NAME=TEXT1
END
/*
```

Figure 11: Test job JCL

```
IEF403I ITCXS470 - STARTED - TIME=10.24.05
IEF233A M F003,PRIVAT,SL,ITCX544,STEP001, 775
my-tsoid.IBMTAPE.ENCRYPT.CNS1.D1129
IEC705I TAPE ON F003,B0020B,SL,COMP,ITCX5470,STEP001,my-tsoid.IBMTAPE.ENCRYPT.
CNS1.D1128
IEC205I OUTDSN,ITCX544,STEP001,FILESEQ=1, COMPLETE VOLUME LIST, 572
DSN=my-tsoid.IBMTAPE.ENCRYPT.CNS1.D102900.VOLS=B0020B,
LISTED VOL(S) HAVE BEEN DATA ENCRYPTED,KL1CD:L,KL2CD:L,
KL1=ENCRYPTION.SERVER.2006.01,KL2=ENCRYPTION.
SERVER.2006.01,TOTALBLOCKS=6113,
PERFORMANCE SCALED
IEF234E K F003,B0020B,PVT,ITCX544,STEP001
```

Figure 12: Test job output

parameter library will ensure that the volume is only defined to the host in which the OAM exit CBRUXENT defines that volume as being eligible for use. The drawback to this is that systems with different tape management catalogs can't share tapes that are in the same library—and this problem is not limited to an IBM library. We have a group that routinely uses SMF data from a variety of systems, and different tape management catalogs, that now has to find another solution even though their data is still in the Sun/STK silos.

drives. I have also given some warnings about using multiple tape management catalogs.

In Part 2, I will discuss implementing IBM's Hydra, the latest virtual tape server, in a Peer-to-Peer (PTP) configuration in our Continuity of Business (COB) environment. All data created during a COB test will be written to virtual tape with replication between the two virtual tape servers in that PTP configuration.

Job Log Messages

My test jobs mostly consisted of running an IEBDG job with the JCL and SYSIN control cards shown in Figure 11.

The output of this test job shows the IEF206I message. Within that message you can see confirmation the volume was encrypted and the key label(s) used for encryption. The DATACLAS can have two different key label names. We chose to use only one key label. The job log is shown in Figure 12.

Conclusion

We have installed a number of IBM 3485 Automated Tape Libraries and IBM 3592 J1A encryption-enabled tape drives. In this part of the article I have shown HCD and ISMF configuration panels and shown sample DFSMS ACS routines to direct encrypted data to these

NaSPA member Lloyd Christensen is President of Christensen Storage Systems Tuning Inc.