BaReLib

Backup/Restore Library

Version 100

Users Guide

22. July 2005

GreenHouse
Software & Consulting
Karl-Heinz Weber
Heinrichstrasse 12
D-45711 Datteln/Horneburg

Document History	1st Edition	22. July 2005	Release BaReLib 100

Trademarks or Service Marks

The following are trademarks or service marks of Tandem Computers Incorporated:
Atalla, Challenge/Response, Enform, Expand, Guardian, Guardian90, Inspect, Multilan, NonStop, TACL, Tandem.
All brand names and product names are trademarks or registered trademarks of their respective companies.

The following are trademarks or service marks of *GreenHouse Software & Consulting*:
$ARROW, $AS, CRYSTAL, CURIOUS, FTPSERV-E, FUNCTRAC, MPWD, MPWD-L, PASSYNC, SECMAN, SECOM, GSTK, SSTK.

The following are trademarks or service marks of Jelinek EDV:
SECMAIN

Please Comment

If you have questions or problems concerning the content of this document, please let me know! Send your comments to:

GreenHouse Software & Consulting
Karl-Heinz Weber
Heinrichstraße 12
D-45711 Datteln/Horneburg
Germany
Phone +49 (0)2363 72566
Fax +49 (0)2363 66106
Mobile +49 (0)172 23 18248
E-Mail: Info@GreenHouse.de
Internet: www.GreenHouse.de
PGP fingerprint: 3A32 D90A D125 5418
1150 2484 6629 2DD2

The Backup/Restore Library (BaReLib) is a new product from
GreenHouse Software & Consulting
bringing transparent DES encryption to the standard Backup and Restore programs.

Why securing data on tape?
When you have to backup data, and ship it physically from one place to another, and when you are concerned about the tapes getting lost – then this is a good solution.

Available cryptographic functions
The following DES functions are available, where the user can choose from:

- ECB DES	(Electrinoc Code Book	8*7 bit key)
- CBC DES	(Cipher Block Chaining	8*7 bit key)
- Triple ECB DES	(Triple Electronig Code Book	16*7 bit key)
- Triple CBC DES	(Triple Cipher Block Chaining	16*7 bit Key)
- Trio ECB DES	(Trio Cipher Block Chaining	24*7 bit key)

Cryptographic Key
The necessary cryptographic key is derived from a PassPhrase, using
Hash Function ISO 10118-2.

Installation

1. Logon to SUPER.SUPER
   This is needed, because BACKUP and RESTORE need to become licensed.

2. Create a copy of the original BACKUP and RESTORE files, and
   name them e.g. SBACKUP and SRESTORE (Secure BACKUP/RESTORE).

3. Set the security to: RWEP = **"OOAO"**

4. FUP LICENSE Backup and Restore

5. Put **BaReLib** into the same location into which you duplicated Backup and Restore.

6. Set the security to: RWEP = "**OOAO**"

7. Add **BaReLib** to **BACKUP** and **RESTORE** by using the following two commands:

```
RUN SBACKUP /LIB <barelib>/exit
RUN SRESTORE/LIB <barelib>/exit
```

   You'll get an error message like this one:

```
$GHS1 TAPELIB 72> backup/lib object/exit
EXIT
    ^
*ERROR-7755*  Comma expected.
ABENDED: 1,181
CPU time: 0:00:00.111
3: Premature process termination with fatal errors or diagnostics
Subsystem: TANDEM.74.G07
$GHS1 TAPELIB 73>
```

   But don't worry: The lib is attached anyway!
   Instead of doing it 'by hand', you can use the tool: **BINDLIB**, which is part of the delivery.

8. Use the **SHOWLIB** tool, which is part of the delivery as well to check, if **BaReLib** is already attached.

Configuration file
To inform **BaReLib** about the cryptographic function as well as the passphrase, these attributes have to be defined in a small EDIT type configuration file.
The EDIT file does have this structure:

```
!
! Definition of cryptographic engine.
! Has to be one of:
! - NONE
! - ECB
! - CBC
! - TripleECB
! - TripleCBC
! - TrioECB
!
CODETYPE  triplecbc

!
! Passphrase used to generate the cryptographic key(s)
! Should be at least 32 bytes long
!
!            12345678901234567890123456789012
PASSPHRASE   HalTandonloDuDah0nteN_Sequ!ia_Be,ch_Ginkgo\Te#t

!
! When CipherBlock Chaining is used, the initial chaining vector
! can be related to the user, doing the Backup and Restore.
! This requires the Restore user to have the same name
! (GUARDIAN name, e.g. GHS.CARL, or Alias name, e.g. CarlWeber)
! and optional the same ID (e.g. 100,5) as the user, who
! performed the Backup.
! The following attributes are supported:
! - NO
!   The user, performing the Restore, can be any.
! - NAME
!   The user, performing the Restore, must have the same system
!   name as the user who did the Backup.
! - NAMEID
!   The user, performing the Restore, must have the same system
!   name as well as the same ID as the user who did the Backup.
!
SAMEUSER  NO
```

Lines, beginning with an
- exclamation mark (!)
- double minus sign (--)
- double euqal sign (==)

are treated as comment, and are skipped.

Key words are NOT case sensitive.

Keywords
The following keywords are supported:

- CODETYPE
- PASSPHRASE
- SAMEUSER

- CODETYPE
  Defines the cryprographic function to be used.
  This can be one of:
  - NONE; when present causes the LIB to skip encoding/decoding
  - ECB
  - CBC
  - TripleECB
  - TripleCBC
  - TrioECB
  The keyword CODETYPE and its attributes are NOT case sensitive.

- PASSPHRASE
  Is the passphrase, from which the cryptographic key(s) are derived.
  The passphrase is limited to the maximum EDIT file line length.
  The keyword PASSPHRASE is not case sensitive, while the PassPhrase string IS case sensitive!
  When PassPhrase is missing, or empty, BaReLib does not perform any cryptographic function.

- SAMEUSER
  The creator of the BACKUP tape can enforce, that the user running RESTORE has to have the same system name (GUARDIAN or Alias name) and optional to habe the same ID. This feature ensures, that only a defined user may restore the tape.
  Three options are available:
  - NO this feature is shut off
  - NAME the RESTORE user has to have the same system name
  - NAMEID the Restore user has to have the same system name ANDE ID

Action Matrix

Crypt Type	PassPhrase	SameUser
NONE	n/a	n/a
ECB	Required	n/a
CBC	Required	optional
TripleECB	Required	n/a
TripleCBC	Required	optional
TrioECB	Required	n/a

Securing the configuration file
Secure the configuration file as tight as possible. The recommended RWEP security is: "**OOOO**".

Assigning the configuration file
BaReLib uses two methods to get the configurations file name:

1. DEFINE
2. Users default location

1. DEFINE
   The configuration file name can be defined as a MAP DEFINE.
   The used DEFINE name is: **=BARECONF**.
   The TACL command to set this DEFINE looks like this:
   ```
   ADD DEFINE =BARECONF,CLASS MAP,FILE <BaReConf file name>
   ```
   e.g.
   ```
   ADD DEFINE =BARECONF,CLASS MAP,FILE $ghs1.grenhous.myconf
   ```
   The configuratiuon file name can be any valid disk file name.

2. Users Default Location
   In case there is no **DEFINE BARECONF**, **BaReLib** checks for a file named **BAREFONF** in the users default location.
   The configuration file in the users default location name MUST be named **BARECONF**!

In case there is no configuration file available, or in case the configuration file can not be read (e.g. error 48), the library does not use any cryptographic function, and BACKUP/RESTORE work as usual.

Example
1. Create a configuration file with the editor (or use an already existing one), and set the cryprographic type, and pass phrase.

2. Define the configuration file, e.g.:
```
ADD DEFINE =BARECONF CLASS MAP,FILE $ghs1.tapelib.bareconf
```
Or put the file into your default location and name it: **BaReCONF**.

3. Check the configuration file Define, e.g.:
```
$GHS1 TAPELIB 53> info define =bareconf,detail
     Define Name        =bareconf
     CLASS              MAP
     FILE               \BEECH.$GHS1.TAPELIB.BARECONF
 $GHS1 TAPELIB 54>
```

4. Execute BACKUP
A typical BACKUP session looks like this:
```
$GHS1 TAPELIB 55> run backup $tape0,*,listall,open,nounload,blocksize 52
File Mode BACKUP Program - T9074G07 (07NOV2003) (AEZ)
BaReLib (100) - T7172G06 - (21Jul2005)  GreenHouse Software & Consulting
Drives: ($TAPE0)
System: \BEECH  Operating System: G06  Tape Version: 3
Backup options:  NO AUDITED, BLOCKSIZE 52, NO IGNORE, OPEN, PARTONLY OFF,
                 INDEXES IMPLICIT
*WARNING-7144*  This tape can only be restored with RESTORE (D30 or later).
*WARNING-7147*  Files created and stored via OSS will not be backed up.
```

```
Backup time: 22Jul2005 14:46                                          Page: 1

Tape: 1       Code             EOF      Last modif   Owner RWEP   Type   Rec Bl
$GHS1.TAPELIB
 ACCELERA      101            2492 20Jul2005 10:21 100,5   UUOO
 BACKUP        100L        3584000  4Feb2004  8:14 100,5   OOOO
 BARECONF      101            2470 19Jul2005 14:57 100,5   UUOO
 G304797G      100          159744 22Jul2005 13:21 100,5   UUOO
 OBJECT        100          159744 22Jul2005 14:43 100,5   UUOO
 PROCTEST      100          146146 11Jul2005 10:14 100,5   UUOO
 README        101           10968 22Jul2005 14:44 100,5   UUOO
 RESTORE       100L        3491840  4Feb2004  8:14 100,5   OOOO
 SAVE          101            2980 11Jul2005 17:58 100,5   UUOO
 TAPELIBO      101          100070 21Jul2005 13:14 100,5   OO--
 TAPELIBS      101           80104 22Jul2005 14:42 100,5   OO--
 TAPELIOO      101           67204 11Jul2005 13:07 100,5   OO--
 TEST          100            8252 22Jul2005 13:43 100,5   UUOO
 TESTSRC       101            2642 22Jul2005 13:43 100,5   UUOO

Summary Information

Files dumped = 14  Files not dumped = 0
BaReFonf file: $GHS1.TAPELIB.BARECONF
Used cryptographic function: ECB-DES
Time used to encode data: 00:00'31,283.758
Bytes encoded:            7.820.206
$GHS1 TAPELIB 56>
```

5. Ship the tape through one channel, and the configuration file through a different one.

At the remote site, perform these steps:

1. Load the configuration file onto the Tandem system

2. Define the configuration file, e.g.:

```
ADD DEFINE =BARECONF CLASS MAP,FILE $ghs1.tapelib.bareconf
```

3. Check the configuration file Define, e.g.:

```
$GHS1 TAPELIB 53> info define =bareconf,detail
     Define Name        =bareconf
     CLASS              MAP
     FILE               \BEECH.$GHS1.TAPELIB.BARECONF
 $GHS1 TAPELIB 54>
```

4. Execute RESTORE

```
$GHS1 TAPELIB 56> run restore $tape0,*.*.*,vol
$ghs1.test,purge,listall,nounload
File Mode RESTORE Program - T9074G07 (07NOV2003) (AEZ)
BaReLib (100) - T7172G06 - (21Jul2005)  GreenHouse Software & Consulting
Drives: ($TAPE0)
System: \BEECH  Operating System: G06  Tape Version: 3
Backup options:  NO AUDITED, BLOCKSIZE 52, NO IGNORE, OPEN, PARTONLY OFF,
                 INDEXES IMPLICIT
Restore time: 22Jul2005 14:48  Backup time: 22Jul2005 14:46          Page: 1

Tape: 1       Code             EOF      Last modif   Owner RWEP   Type   Rec Bl
```

```
$GHS1.TEST
 ACCELERA       101            2492 20Jul2005 10:21 100,5   UUOO
 BACKUP         100L        3584000  4Feb2004  8:14 100,5   OOOO
 BARECONF       101            2470 19Jul2005 14:57 100,5   UUOO
 G304797G       100          159744 22Jul2005 13:21 100,5   UUOO
 OBJECT         100          159744 22Jul2005 14:43 100,5   UUOO
 PROCTEST       100          146146 11Jul2005 10:14 100,5   UUOO
 README         101           10968 22Jul2005 14:44 100,5   UUOO
 RESTORE        100L        3491840  4Feb2004  8:14 100,5   OOOO
 SAVE           101            2980 11Jul2005 17:58 100,5   UUOO
 TAPELIBO       101          100070 21Jul2005 13:14 100,5   OO--
 TAPELIBS       101           80104 22Jul2005 14:42 100,5   OO--
 TAPELIOO       101           67204 11Jul2005 13:07 100,5   OO--
 TEST           100            8252 22Jul2005 13:43 100,5   UUOO


 TESTSRC        101            2642 22Jul2005 13:43 100,5   UUOO

Summary Information

Files restored = 14  Files not restored = 0
BaReFonf file: $GHS1.TAPELIB.BARECONF
Used cryptographic function: ECB-DES
Time used to decode data: 00:00'35,283.017


Bytes decoded:            7.820.206
$GHS1 TAPELIB 57>
```

Access to an encoded type by the 'normal' BACKUP

An encoded tape can be listed by **BACKUP** WITHOUT the need to know any key, or cryptographic function.

Restoring an encoded tape

Restoring data from an encoded tape requires the correct cryptographis method as well as pass phrase and the correct user, when requested at **BACKUP** time.

A wrong method or PassPhrase results in something like this:

```
$GHS1 TAPELIB 64> run $system.system.restore $tape0,*.*.*,vol
$ghs1.test,listall,nounload,purge
File Mode RESTORE Program - T9074G07 (07NOV2003) (AEZ)
(C)2000 Compaq (C)2003 Hewlett Packard Development Company, L.P.
Drives: ($TAPE0)
System: \BEECH  Operating System: G06  Tape Version: 3
Backup options:  NO AUDITED, BLOCKSIZE 52, NO IGNORE, OPEN, PARTONLY OFF,
                 INDEXES IMPLICIT
*ERROR-2012*  $SYSTEM.SYS03.RESTORE : Internal error. String overflow.
              STR^PADRIGHT+%27
              ARCHTAPEREST^READDATABLOCK+%256
              RESTORE^READTAPEBLOCK+%15
              RESTORE^READINSTANCE+%4
              GENERICRESTOREDATA+%37
              RESTORE^DATA+%220
              RESTORE^PHYSICALFILE+%515
              RESTORE^SINGLEPART+%73
              RESTORE^FILE+%1311
```

```
               RESTORELOOP^ONETAPESET+%637
               RESTORELOOP+%463
               RESTOREMAIN^PROC+%420
               DEJUREMAINPROC+%1
ABENDED: 1,127
CPU time: 0:00:00.125
3: Premature process termination with fatal errors or diagnostics
Subsystem: TANDEM.75.G07
$GHS1 TAPELIB 65>
```

Performance:
Using cryptographic functions on a Tandem system is a performance hug. To backup 7.5 MBytes costs some 32 seconds on an empty S7000 CPU. The number might decrease dramatically when using newer/better S type CPUs.

Safety:
I do know, that symmetric cryptographic systems lack a key management. BaReLib is intended to provide the user with a robust cryptographic mechanism, that secures data on tape. It is NOT intended to provide a sophisticated key management as well.

How will it be used?
When you have to backup data, and ship it physically from one place to another, and when you are concerned about the tapes getting lost - then do this:

1. Create the BaReConf configuration file:
   - define the cryptographic method
   - define the PassPhrase
2. Define the configuration file
3. Run SBACKUP

4. Ship the BACKUP tape through one channel, e.g. UPS, FedEX, what ever
5. Ship the BaReConf file through another channel, e.g. E-Mail, or even on a floppy, to the target location. You also can call the remote site and tell the passphrase.

6. Install the configuration file on the target system
7. Define the configuration file
8. Run SRESTORE

Before you use **`BaReLib`** for production purposes, please test it to get familiar with the handling.

What to do when the PassPhrase got lost?
Do NOT blame GreenHouse!
No configuration attributes are stored during BACKUP time.
There is NO way in recovering a missing PassPhrase/cryptographic key.
In case you lost the PassPhrase, your safely lost logical access to your data.