System
SECUR'ACCESS V3

System Administrator's Guide - Access to GCOS 7 Services

GCOS 7/UNIX INTEROPERABILITY

Software

Subject : This document explains the installation, troubleshooting, batch processing, and application TDS protection procedures for SECUR'ACCESS in the security context of GCOS 7 users.

Special instructions : This Revision 01 cancels and replaces Revision 00.

Software supported : GCOS 7 V7, V8

SECUR'ACCESS V3.3

Date : June 1998

Bull Electronics Angers S.A.
CEDOC
Atelier de reprographie
331, Avenue Patton
49004 ANGERS Cedex 01
FRANCE

Bull HN Information Systems Inc.
Publication Order Entry
FAX: (508) 294-7411
MA02/423S
Technology Park
Billerica, MA 01821
U.S.A.

Suggestions and criticisms concerning the form, content, and presentation of this manual are invited. A form is provided at the end of this manual for this purpose.

Bull disclaims the implied warranties of merchantability and fitness for a particular purpose and makes no express warranties except as may be stated in its written agreement with and for its customer. In no event is Bull liable to anyone for any indirect, special, or consequential damages.

The information and specifications in this document are subject to change without notice. Consult your Bull Marketing Representative for product or service availability.

Preface

TARGET AUDIENCE

If you are a system administrator in a Stella 7 context, this manual will provide the information you need to:

- Install the SECUR'ACCESS and MICR'ACCESS products
- Handle failures (troubleshooting)
- Carry out batch processing
- Protect the application TDSs

OTHER MANUALS AVAILABLE

GCOS 7 System Installation, Configuration and Updating Guide	*47 A2 19US*
Bull Customer Service Bulletin	*98-008 EN*

SECUR'ACCESS Documents

SECUR'ACCESS Security Administrator's Guide	*47 A3 01BD*
SECUR'ACCESS Delegate Administrator's Guide	*47 A3 02BD*
SECUR'ACCESS User's Guide	*47 A3 03BD*
SECUR'ACCESS Programming and Implementation Guide	*47 A3 04BD*

IDS Documents

IDS /II Reference Manual Vol 1... *47 A2 05UD*

ISM-UM/AccessMaster Documents

Stella Security Administrator's Guide.. *39 A7 79UU*
ISM-UM Administrator's Guide / Access to GCOS 7 Services......................... *47 A2 07UC*

INTEROP 7 Documents

Interoperability Software Installation 7 - Administrator's Guide....................... *47 A2 56UU*
OPEN 7 Administrator Guide *47 A2 81US*

HA Documents

High Availability Concepts..*47 A2 22UT*
High Availability Administrator's Guide...*47 A2 23UT*

Table of Contents

Appendices

Illustrations

Figures

Tables

1. Software Installation

1.1 INSTALLATION OF SECUR'ACCESS

1.1.1 Versions and Technical Status

To install SECUR'ACCESS V3, you must have the following (or later) versions of GCOS 7:

GCOS 7-V7 TS 7458

You must also have the following (or later) versions of these telecommunication programs:

- DNS V4 U1 ET22
- CNS A2 U2 ET26

1.1.2 Software Programs

The new functions use the following basic GCOS 7 software programs:

- Transaction-driven TDS
- FORMS screen manager
- IDS/II database manager
- SCAM smart card access method
- OPEN 7
- IUM-SA7 agent
- Communications Access Method (CAM)

1.1.3 Prerequisites

There are a certain number of corrections listed in the Customer Software Bulletin (CSB) for each release of SECUR'ACCESS.

1.1.4 How to Install SECUR'ACCESS

1.1.4.1 Delivery

The ISI7 installation procedure offers you delivery of the SECUR'ACCESS V3.3 software: see the *Interoperability Software Installation 7 - Administrator's Guide*. The software programs contained in the delivery materials are used to carry out:

- the first installation
- subsequent updates

At the first installation, the TDS name and the directory in which the libraries are installed may be different from SA7 (parameter SA7_DIR).

The SECUR'ACCESS version is located in the SA7-FW member of the library SA7.LIV.SL.

When you upgrade from SA7 V2.1 to SA7 V3.3, proceed as follows:

- save the SA7 V2.1 environment

- rename:
  - the SA7.SAA01, ..., SA7.SAA08 files
  - the SA7.LIV.BINIDS and SA7.LIV.SL libraries

- install version SA7 V3.3 (first installation: parameter REINSTAL = 1)

- recover the SA7 V2.1 database (using the procedures described in sections 1.1.4.6, 1.1.4.7).

To upgrade from SA7 V2.2, SA7 V3.1 or SA7 V3.2 to SA7 V3.3, set the REINSTAL parameter of the ISI7 configuration file to zero and perform an update installation.

1.1.4.2 Product Status on Completion of Installation Process

First installation

The product is installed at password level. Declarations concerning cards (entering secret sets, assigning cards) should be carried out using the tools provided for the purpose.

The only user created in the database is the security administrator SECADMIN, with the SA7 password that must be changed. This administrator will create the other security administrators, and also a master user.

1.1.4.3 Tests Before Startup

When installation is completed, you must check that all functions of SECUR'ACCESS are operational.

Execute RESTORE to take into account the H_SM_DUAL updates.

Without securing the site (do not use the SECOPT option of CONFIG):

1. Launch TDS SA7:

   ```
   S: EJ SA7-LTDS LIB=SA7.LIV.SL VL=(dvc,md);
   ```

   dvc and *md* are the type and name of the volume containing the journal (BJRNL).

2. Connect to the **master Mailbox** of the TDS SA7:

   ```
   S: EJ SA7-MASTER,,SA7.LIV.SL;
   $*$CN -dmb MSA7 -usr M1 -pw ... -sc ...
   ```

3. From a **synchronous terminal without using the Pass-Thru function**, connect to the TDS SA7 with user SECADMIN:

   ```
   $*$CN -dmb SA7 -sc ... -usr SECADMIN -pw ...
   ```

4. Activate the HSALGON TEST command

5. To assign yourself a password, use the SAUTIL1 command.

6. To access the administration menu, use the SAMENU command.

7. To check and personalize the **general parameters**, select **parameter management/1**. The parameters depend on the choice of site.

8. Modify the site's **initial password** if desired.

9. To create a user, select option **1** of the menu:

   - Give the user IOF rights (corresponding rights: main right = 799, lock 10 =1) with CR-STATUS=0
   - Assign the user a password.

10. Create at least one other master user:

    Give this user "master" rights (corresponding rights: main right = 799, lock 9 = 1).

1.1.4.4 How to Recover the Catalog

After checking the installation, checking the general parameters and modifying the site's initial password, proceed with the recovery of the catalog. For more information, see the chapter on **Batch Processing** in this document.

1.1.4.5 How to Recover the SECUR'ACCESS V2.1 Database

You have updated from SECUR'ACCESS V2.1 to SECUR'ACCESS V3 and you have decided to recover the SECUR'ACCESS V2.1 database. To do this, you must:

- unload the V2.1 database
- load the V3 database

1.1.4.6 How to Unload the V2.1 Database

To unload the V2.1 database:

1. Check in JCL SA7-REPV21A:

   - the values of the parameters
   - the files
   - the areas assigned according to the renaming carried out on the areas
   - the schema of SECUR'ACCESS V2.1

2. Launch the JCL:

   ```
   S: EJ SA7-REPV21A LIB=SA7.LIV.SL VL=(media, device, size)
   ```

   A sequential file is created on the indicated volume (media, device) with the indicated size (size) and the following characteristics:

   ```
   FILE=       SA7.FV21
   UFAS=       SEQ
               RECSIZE = 512
               CISIZE = 1024
               RECFORM = F
               SIZE = n
               INCRSIZE = 1
   ```

   The size depends on the number of users. Allow 1 cylinder for every 500 users.

1.1.4.7 How to Load the V3 Database

To load the V3 database:

1. Check the assigned areas and files in JCL SA7-REPV21B.

2. Launch the JCL: `S: EJ SA7-REPV21B LIB=SA7.LIV.SL;`

   The following question is asked:

   ```
   "--> IOF APPLICATION BY DEFAULT FOR USERS (Y/N) ?"
   ```

3. If you want all users recovered from the V2.1 database to have access rights to IOF:

   - answer **Y** (Yes)
   - otherwise, answer **N** (No)

All users already present in the V3 database will be updated using the data of V2.1.

Any user who is not in the V3 database will be created using his/her data from the V2.1 database (cycle, manager, card, etc.).

The delegate administrators in charge of a user group in the V2.1 database will keep the same responsibilities in the V3 database.

The users' history report and the **waiting for signature** file are not recovered.

Any user present in the database but not in the catalog cannot be used.

All users keep their current passwords.

4. Activate the administration actions

   If the security of your site is at the **password** level:

   Declare in the list of applications all applications protected with security level **01** (password level).

1.1.5 How to Recover the Information of a PASSWORD7 Site

PASSWORD7 and the GCOS 7 corrections needed for its functioning must be removed. To do this, you must recover the information contained in the file CATPW7 and transcribe it in the SECUR'ACCESS V3 database. To do this, proceed as follows:

1. Recover the useful values of the PASSWORD7 general parameters (minimum length of password and language code).

2. Recover the users of PASSWORD7 with their characteristics (cycle, retention date, date of creation). All users must already exist in the security database
   (See Recovery of the catalog).

3. Recover the definitions of the cycles of PASSWORD7:

   This stage must be carried out after the complete installation of SECUR'ACCESS V3 when the SECUR'ACCESS database is operational. The definition of the cycles includes the following two phases:

   - if the cycle exists: its values must be updated.
   - if the cycle does not exist: it must be created.

4. Create an SL member (in SA7.SL for example) with the name SACYCLE containing the correspondence between the cycle names of PASSWORD7 and those of SECUR'ACCESS:

Example:

```
*
*** CORRESPONDENCE OF THE CYCLES PW7 AND SA7
*
U-008
D-009
T-126
```

Position 1: name of the PASSWORD7 cycle

Position 2: separator (-)

Position 3, 4 and 5: name of the corresponding SECUR'ACCESS cycle.

The maximum number of cycles to be declared in this file is **20**.

1. Launch the following task:

   ```
   S: EJ SA7-REPPW7 LIB=sl-liv;
   ```

2. Check the results of this recovery in the summary report. The following messages can appear:

   `OPEN ERROR IN INFILE STATUS`
   Problem with the file SACYCLE (see error status).

   `ERROR INDEX OUT OF RANGE`
   SACYCLE contains more than 20 items.

   `FILE SACYCLE EMPTY`
   The file SACYCLE exists, but it is empty.

   `CYCLE CREATED IN THE DATABASE`
   A CATPW7 cycle missing from the SECUR'ACCESS database has been created.

   `CYCLE ALREADY EXISTS IN THE DATABASE`
   The data of the cycle has been updated with data from the file CATPW7.

   `ABSENT FROM THE FILE SACYCLE`
   A cycle found in CATPW7 is not defined in SACYCLE.

   `ABSENT:` The user is absent from the SECUR'ACCESS database, and is not recovered.

1.1.6 How to Activate System Security

1.1.6.1 Preliminary Comments

All projects of the catalog with the right to access IOF (whether they are subject to control or not), must have access rights to the application SA7 with TDS-CODES "7FFFFFFF". This modification is usually carried out by the installation procedure.

All new projects must include this application, with the authority code 7FFFFFFF.

1.1.6.2 Update of System Startup for Automatic Launching of TDS SA7

In order to run the TDS SA7 automatically upon startup of the system:

Modify the SYSTEM member in the SITE.STARTUP library by inserting:

```
EJ SA7-MASTER LIB=sl-liv;
```

Where `sl-liv` is the name of the SL library delivered with the product.

```
EJ SA7-LTDS LIB=sl-liv  CLASS=name-class   VL=(dvc,md);
```

Where `sl-liv` is the name of the SL library delivered with the product, name-class,
where *dvc* and *md* are the type and the name of the volume containing the journal (BJRNL).

NOTE: Name-class must be an open class enabling the execution of at least two activities, including a TDS.

and, if cards are used:

```
EJ SA7-PSG LIB=sl-liv;
```

Where `sl-liv` is the name of the SL library delivered with the product.

Once the functioning of all the various components of SECUR'ACCESS (application TDSs, TDS SA7, access of "master" users) has been checked, you can set the configuration of the site with protection (SA7LOGON=YES).

NOTE: If a "CINIT ERROR" message appears when connecting to IOF, check that the TDS SA7 is operational, or check that the user is not already connected to the TDS SA7.

1.1.7 How to Generate DNS

The terminals that will be connected to SECUR'ACCESS via DATANET do not require any special generation parameter.

- For MINITEL, use the standard MINITELX model.
- For VIP terminals, check that the parameter SEGOUT has been declared on clause DV.

1.1.8 How to Install the Secret Keys

1.1.8.1 How to Enter the Secret Keys

The secret keys must be entered before assignment of the cards by the administration and before the keys are used for access control. This entry must be followed by checking of the keys (with the command SA7-CHECK; see next section). You can choose to proceed with the checking process automatically. In this case, the GSP server is launched automatically after the keys are entered. The entry of the keys is reserved for the SECADMIN user. It is accomplished using the commands:

```
S: MWINLIB BIN SA7.BIN;
S: SA7-IGB;
S: SA7-KEYS;
```

A screen appears for the confirmation of the name of the library CU containing the CUs of the site's GSP server (default value: SA7.LIV.CU).

Another screen is used to confirm the name of the LM library containing the site's LM PSGCOM_C (default value: SA7.LIV.LM).

A menu is used to choose the types of cards used. Each key value is entered in double input.

For cards of type M6

The following information is requested:

- A digital entry with three positions. This entry is used to mask the secret keys in the software and must not start with a zero.
- Four hexadecimal elements. These non-secret elements:
  - Are used in certificate calculation.
  - Are supplied by BULL CP8 (“MCT” on the CP8 form).
  - Correspond to address word 0888 of the smart card.
  - To release the cards used with PIN, an issuer key that corresponds to word 0890 of the card.

  One person enters the first six secret keys in hexadecimal.
  A second person, on another screen, enters the last six secret keys in hexadecimal.

For SCOT-type cards (60 or 110)

The following information is requested:

- The basis elements. These 16-byte hexadecimal elements are used to mask the secret keys in the software and are chosen by the installer.
- The "mother" secret set, 16-byte hexadecimal.
- The "patterns", 16-byte hexadecimal. These patterns:
  - Are used to obtain the diversified secret set and the key 1A for unlocking.
  - Represent the contents of the words of the card at addresses 0888 and 0890.

For TB100 cards

The following information is requested:

- The basis elements. These 16-byte hexadecimal elements are used to mask the secret keys in the software and are chosen by the installer.
- The sender key (key IK), 16-byte hexadecimal.
- The authentication key (key AK), 16-byte hexadecimal.

1.1.8.2 How to Check the Secret Keys

Only the SECADMIN user can check the secret keys of the M6, SCOT 60, SCOT110 and TB100 cards. To carry out this verification, use the commands:

```
S: MWINLIB BIN SA7.BIN;
S: SA7-IGB;
S: SA7-CHECK;
```

- In the screen which appears, confirm the name of the LM library containing LM PSGCOM_C.
- The check is carried out for each type of card for which keys are entered.
  If the result is correct, the procedure proceeds automatically to the next check. When all checks are completed, the new LM is created in the selected LM library.
- The checking of the secret keys is carried out by requesting certificates with a card of the appropriate type (M6, SCOT 60, SCOT 110, TB100).
  This certificate can be obtained with a card reader:
  - **With an on-line card reader:** insert the card to be checked.
  - **With an authenticator (CAD1004):** use the function C + 9. The procedure is the following:

    1. Read the serial number of a card on the authenticator.
    2. Fill in the corresponding entry on the screen. For a card of type M6, SCOT 60, SCOT 110: the serial number must be preceded by 8 zeros.
    3. Calculate the certificate using the function C + 0 on the CAD1004.
    4. Fill in the corresponding entry with the result.

1.1.9 Precautions Prior to Activating Security

To activate security on the site once the installation is completed, use the SECOPT option under CONFIG (see Appendix **The SECOPT declaration**).

After RESTORE of GCOS 7, all requests for connection to IOF or to a TDS are checked by SECUR'ACCESS.

It is therefore best to ensure:

- The proper functioning:
  - of the TDS SA7
  - of the SECADMIN user

    correct creation
    correct password
    if the user has a card: correct personal code, no opposition, retention date not yet reached)
- The presence of at least one user having **MASTER TDS** and **IOF** rights.
- The validity of the SECUR'ACCESS general parameters.
- That the GSP server (see JCL SA7-PSG) runs with a priority higher than or equal to that of a TDS.
- The update of the STARTUP SYSTEM (in SITE.STARTUP) for the automatic launch of:
  - the task of opening the MASTER MAILBOX:
    ```
    S: EJ SA7-MASTER   LIB=sl-liv;
    ```
    where `sl-liv` is the name of the SL library delivered with the product.
  - TDS SA7:
    ```
    S: EJ SA7-LTDS LIB=sl-liv  CLASS=name-class  VL=(dvc,md);
    ```
    where `sl-liv` is the name of the SL library delivered with the product, and *dvc* and *md* are the type and name of the volume containing the journal (BJRNL).
  - and if cards are used, the GSP server:
    ```
    S: EJ SA7-PSG LIB=sl-liv;
    ```
    where `sl-liv` is the name of the SL library delivered with the product.
- Allow for the following possible restarts:

RESTART WARM	Allow for an automatic reply to the question of ROLLBACK (by H_SYS_REPLY) and do not restart the TDS SA7. Restart the GSP server and SA7-MASTER.
COLD or CLEAN	Restart TDS SA7, SA7-MASTER and the GSP server.

Protection of the OPERATOR console

To prevent a TJ of the security TDS from denying access to service, protect the OPERATOR console (authorized personnel only). The operator must be sure to:

- Disconnect after each operation
- Use SECUR'ACCESS to control access to the IOF application for the system console.

1.1.10 How to Manage Downloaded Programs

To shorten the time needed for the downloading of LECAM, specific programs have been created for the management of the M6 cards. To manage these cards on LECAM, the following programs are available:

H-SECUR_ALL	manages all families of cards that can be used with the system.
H-SECUR_M6_1	only manages cards of the M6 family.
H-SECUR_M6_2	only manages cards of the M6 family without use of the PIN code.

If you choose to use one of these programs:

Using the administration function, modify the general parameters, indicating the name of the selected program in the **LECAM Program** field.

1.2 HOW TO INSTALL MICR'ACCESS

1.2.1 Introduction

The product MICR'ACCESS V2.2 transforms a microcomputer of the ZDSxx type into a synchronous terminal. It enables connection to the DPS 7 on which the SECUR'ACCESS software is running.

This terminal manages the functions sent by SECUR'ACCESS for controlling access to the DPS 7.

MICR'ACCESS:

- Emulates the keyboard, screen and printer of Bull terminals of the DKU 7107 type.

- Carries out file transfers with MICROFIT and FTF protocols.

- Accommodates emulation of a magnetic badge using the CP8 card.

1.2.2 Environment

1.2.2.1 Hardware Environment

Each ZDSxx-type microcomputer must have at least the following equipment:

- a 3"1/2 diskette drive,
- a hard disk with 2 Mbytes of free memory,
- 512 Kbytes of RAM,
- an external CP8 card reader, type TLP 224,
- a serial port for the connection of the card reader,
- a synchronous telecommunication card made by the ATLANTIS company:
  - XCOM,
  - MELODY-V32,
  - XMEM,
  - USX.

NOTES:

1. The USX card is an XMEM card on which a child card is connected that is capable of managing VIP communications via TCU and TCS.

2. The TLP 224 external reader must be connected to one of the microcomputer's serial ports: COM1 or COM2.

1.2.2.2 Software Environment

MICR'ACCESS runs in MS-DOS 3.1 and later versions. It uses the VTI$B interface of the ATLANTIS company. The modules needed to launch the emulator depend on the type of link used.

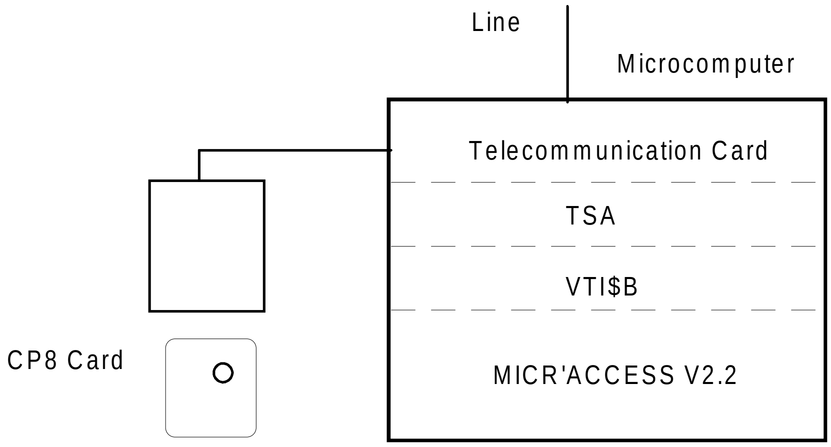

Figure 1-1. MICR'ACCESS EnvironmentTitle

MICR'ACCESS V2.2 is made up of several code modules. The installation of the product requires the use of the following two modules:

- Main module **MA22011** containing the emulation application.
- A communication module. The selected module corresponds to a type of telecommunication and contains all the files needed for the functioning of:
  - **MA22111**: X25 on an XCOM card
  - **MA22211**: VIP on an XCOM card
  - **MA22311**: X25 on a USX or XMEM card
  - **MA22411**: VIP on a USX or XMEM card
  - **MA22511**: TCU-TCS on a USX card
  - **MA22611**: X32 on a MELODY-V32 card

These different modules are delivered with SECUR'ACCESS. They are available in a library on the DPS 7000 and must be downloaded to the microcomputer.

1.2.3 How to Install MICR'ACCESS

The TLP 224 external reader is connected to one of the serial ports of the microcomputer.

1.2.3.1 How to Download the MICR'ACCESS Software

The different modules needed for MICR'ACCESS must be recovered in a binary library of the DPS 7 on which SECUR'ACCESS has been installed.

You need only download these modules using a file transfer tool with the DPS 7. You can use the standard ATLANTIS emulator supplied with the delivery of the communication cards.

> **IMPORTANT**
>
> These files must be transferred in binary mode.

NOTE: You do not need to download all of the modules. Only the main module (MA22011) and the selected communication module are used.

1.2.3.2 How to Install the Software on the Microcomputer

Standard Installation

The modules are compressed and are delivered in the form of auto-extractable executable binary files in DOS. You need only copy them in the installation directory of MICR'ACCESS and run them.

To install MICR'ACCESS on the microcomputer:

1. Under DOS, with the cursor set on:
   C:>

2. Enter the following DOS command to create the installation directory for MICR'ACCESS:
   ```
   MD MICR'ACC
   ```

3. Place the cursor in this installation directory using the DOS command:
   ```
   CD MICR'ACC
   ```

4. Copy the two module files (MA22011.EXE and MA22x11.EXE) in the MICR'ACC installation directory.

5. To decompress these two files, open them. You need only enter the names of the two modules successively on the DOS command line:
   `MA22011`
   `MA22x11` (where x corresponds to the number of the selected communication module).

6. Copy the various files of MICR'ACCESS in the installation directory.

7. To save space on the hard disk, you can delete the two compressed module files by entering the following erase commands in succession:
   `DEL MA22011.EXE`
   `DEL MA22x11.EXE` (where x corresponds to the number of the selected communication module).

The installation of MICR'ACCESS on the microcomputer is complete.

1.2.3.3 How to Set the Configuration of MICR'ACCESS

MICR'ACCESS is installed on your microcomputer. You can now proceed with the configuration:

- of the file autoexec.bat
- of the installation directory

Modification of the AUTOEXEC.BAT file

To launch the CP8 handler during the boot, you can modify the machine's autoexec.bat file. At the end of the file, add the following MS-DOS command:

```
C:\MICR'ACC\ICCHSCR
```

NOTE: If you are using an XMEM, USX or MELODY-V32 card, add the following path to the PATH variable of the AUTOEXEC.BAT file: `PATH C:\MICR'ACC;.`

Modification of the MICR'ACCESS installation directory

By default, all the files are copied in the specific directory:

```
C:\MICR'ACC
```

However, you can install the different software programs in the directories selected by the user. To do this:

1. Modify the access path defined by default as "C:\MICR'ACC" during installation.

2. Modify the launching procedures of MICR'ACCESS (files: m'a.bat, m'ascp.bat, m'aw3.bat and m'aw3scp.bat). The examples given in this document use the name of the installation directory defined by default: MICR'ACC.

1.2.3.4 How to Launch MICR'ACCESS

To use MICR'ACCESS, see the MICR'ACCESS User's Manual.

1.3 IUM-SA7 Agent Installation

IUM-SA7 is an RPC agent whose server section (called SA7SRV) is installed on GCOS 7 using the automatic installation tool ISI 7.

ISI 7 also carries out the installation of OPEN 7 and GX-RPC, which are prerequisites to the operation of SA7SRV.

For further details, please refer to the following:

- Interop7 document:
  Interoperability Software Installation 7 - Administrator's Guide

- ISM-UM/AccessMaster document:
  Security Administrator's Guide/Access to GCOS 7 Services

2. Batch Processing

2.1 HOW TO RECOVER THE CATALOG

It is important to maintain the consistency between the catalog and the SECUR'ACCESS database. After installation or when you doubt the consistency, use the catalog recovery tools. In order to ensure consistency between the catalog and the security database:

1. Update the database based on the catalog.

2. Manage on your terminal the users whose passwords are spaces.

3. Declare the passive users.

2.1.1 How to Update the Database

To update the database:

Use the command:

```
S: EJ SA7-RCAT1 LIB=SA7.SL
```

SA7-RCAT1 updates the database based on the catalog and recovers the data which is not in the database.

Users whose passwords contain spaces are created in the database with user code A and are recorded in a file (member PRT-COM12) which will be processed in the next stage (SA7-RCAT2).

Answer the following three questions:

- `I.O.F. APPLICATIONS BY DEFAULT FOR USER? (Y/N)`

  To give users IOF access rights by default:
  - Answer **Y** (Yes).

  To deny users IOF access rights by default, even if the IOF application is defined in their project:
  - Answer **N** (No).

- `EDITION OF USERS? (Y/N)`

  To create in the Job report (JOR) a summary list of the users handled:
  - Answer **Y** (Yes).

- `DISPLAY OF USERS FOUND IN DATABASE (Y/N)`

  To list on your terminal the users present in the database:
  - Answer **Y** (Yes).

2.1.2 How to Handle Passwords Made up of Spaces

To handle users whose passwords contain spaces only, use the FORMS and enter the following command on a synchronous terminal:

```
S: AI SA7-RCAT2 LIB=SA7.SL
```

Users without a password are displayed on the terminal with the code **P**. You can do one of the following:

- Leave this code with the value **P**, in which case the user is considered a pseudo-user corresponding to a passive terminal. The user's password is not modified.
- Reset this code to the value 'space'. In this case the user's password will take the value of the site password, or will be set to 12 zeros if the site password has not been defined. This user is then created with code **A** (active user).

2.1.3 How to Change the User Code in the Database

To validate the modifications introduced in 2.1.2, run the command:

```
EJ SA7-RCAT3 LIB=SA7.SL;
```

Users whose code has been attributed the value 'space' become type **A** users in the SECURITY database. Their passwords are updated in the GCOS 7 catalog.

2.2 HOW TO LOAD THE DATABASE

2.2.1 Purpose

From a library member you can:

- create users in the SECUR'ACCESS database and the GCOS 7 catalog, or create user-project links in the catalog
- modify a user's characteristics in the SECUR'ACCESS database
- delete user-project links, or delete users, from the SECUR'ACCESS database and the GCOS 7 catalog.

The records in this library member are created using GCL commands. (See 2.2.4, **How to Create the INPUT_GBASE File using GCL**).

They can later be updated using a text editor.

If the values of the language code and the cycles are not specified in the 'user' or 'project' records, their values are those of the general parameters.

2.2.2 How to Launch the Loading of the Database

Only the security administrator can launch this job (otherwise, "ILLEGAL ACCESS" message). This user must have the proper catalog rights to update the catalog.

To launch the loading of the database:

1. Create the parameter file for the INPUT_GBASE member.
2. Check the JCL: SA7-GBASE (library names).
3. Enter the command:

```
S: EJ SA7-GBASE LIB=SA7.LIV.SL;
```

A report of actions taken and anomalies appears in the JOR.

2.2.3 INPUT_GBASE Parameter Files

The following two types of records are used:

- project records
- user records

Project records

This type of record contains all the values common to a user group. A new record cancels the values defined in the previous record and defines new values for a new user group. The general parameters are assigned to undefined values.

The table below lists the project parameters and their characteristics:

Table 2-1. Parameters of a project record

Row	Field	Length	Value	Comment
1	Identifier	1	#	Mandatory
2	Project	12		Mandatory
3	Person responsible	12		Optional
4	Language code	3		Optional
5	Cycle code	3		Optional
6	Password cycle	3		Optional
7	Password	12		Optional
8	Rights and locks	3+10		Optional

The project record includes the following fields:

Field 1 The mandatory identifier of the record. Its value is #.

Field 2 The mandatory project name. It must be one of the following:

- The name of a project that exists in the catalog. (In the case of a request to delete a user, the project-user link is deleted from the catalog. If no other project-user link exists, the user is also deleted from the SA7 database.)
- The character '∗'. (In the case of a request to delete a user, this user is deleted from the GCOS 7 catalog (with all the project-user links) and the SA7 database.)

Field 3 The name of the delegate administrator responsible for the following new users groups.

Field 4 The default language code (250 = French, 826 = English).

Field 5 The default cycle for the confidential codes.

Field 6 The default cycle for the passwords.

Field 7 The first user password. For passive users, this password is managed by SECUR'ACCESS and not by the catalog.

Field 8 The list of default rights and locks: each right (3c) is followed by locks (10c). This list can contain 10 rights.

User records

The user record is used to delete, create or change a user's parameters. The values given here modify or are added to the default values given in the header record for this user.

The user record contains the following fields:

Table 2-2. Parameters of a User Record

Row	Field	Length	Value	Comment
1	Identifier	1	space	Mandatory
2	User ident.	12		Mandatory
3	Action code	1		Mandatory
4	User code	1		Mandatory
5	User name	20		Optional
6	User first name	12		Optional
7	Default project	1		Optional
8	Person responsible	12		Optional
9	Card type	2		Optional
10	Card serial n°	16		Optional
11	Change code	1		Optional
12	Language code	3		Optional
13	Confidential code cycle	3		Optional
14	Password cycle	3		Optional
15	Password	12		Optional
16	Rights and locks	10*(13)		Optional
17	Expiry date	6		Optional
18	Service word	20		Optional

The user record includes the following fields:

Field 1 The mandatory identifier of the record; equals one space.

Field 2 The user identifier. It follows the rules of the catalog.

Field 3 The action code. It can have the following values:

space
If the user exists in the database, this user is modified. If the user does not exist in the database, he is created, and is also created in the catalog (if he does not already exist there) with the password specified in field 15.
If this password is not specified, the user is created with the site password (providing it exists) or with a value of 12 zeros. (A passive user is created in the catalog with a password = 'space'.)

D The user is deleted, or the project-user link is deleted, depending on the value of the previous 'project' field.

Field 4

The user code. It can have the following values:
S security administrator
D delegate administrator
F (letter "F") pseudo-user for the replacement cards
P pseudo user for the passive terminals
A normal user

Fields 5-6

The user's name and first name.

Field 7

The default project:
0 = the project is not a default project
1 = the project is a default project (default value)

Field 8

The name of the delegate administrator responsible for this user.

Field 9

The card type: indicate the type of card used (M6, MC, MD, MP) if the user has a card.

Field 10

If you have given a card type, this is the serial number of the card.

Field 11

If the user has a card, indicate the mode of changing the code:
1 = confidential code
2 = PIN
3 = PIN handled like a confidential code

Field 12

The user’s language code (250 = French, 826 = English).

Field 13

The cycle of the user's confidential code.

Field 14

The cycle of the user’s password.

Field 15

The first user password. For a passive user, this password is managed by SECUR'ACCESS and not by the catalog.

Field 16

The list of the user's rights and locks. Each right (3c) is followed by locks (10c). This list can contain 10 rights.

Field 17

The date (DDMMYY format) after which the user can no longer connect to applications checked by SECUR'ACCESS.

Field 18

The service word (20 characters). The text entered in this field is left to the initiative of the security administrator.

Example:

```
#PROJET1     DURAND            060            7990000000001
 DUPONT      D
 DUBOIS      D
 USER1        ARONALD              JEAN        1
M600000000000543211   030
 USER2        DROMUALD             ANDRE       0
 USER31       PPRINTER31                       1
 AZQSRT
#PROJET2                       090XXXXWWWW
 USER1 ANOM-USER1    FIRST NAME      1
 USER22       PPRINTER22
```

In this example:

- The users DUPONT and DUBOIS are deleted from the project PROJET1 in the catalog. If these users belong to another project, they are not deleted from the SA7 database.
- The users described up to PROJET2 are under the responsibility of DURAND. They have a language code taken from the general parameters of SECUR'ACCESS, a password cycle of 060 and right 799, lock 0000000001.
- User USER1, type A, has an M6 card whose serial number is 0000000000054321 and uses the confidential code (whose cycle is 030).
- User USER2 is a delegate for whom PROJET1 is not the default project.
- User USER31 is a passive user whose SECUR'ACCESS password is AZQSRT.
- A new record "#" indicates a change of project and a change of password cycle, a default value for the password of the "passive users" among the following users. The other default values are taken from the general parameters.
- User USER1 is created (or changed); Project PROJET2 is not the default project.
- Passive user USER22 is created (or changed) with the default values.

2.2.4 How to Create the INPUT_GBASE File using GCL

To facilitate the creation of the INPUT_BASE file, there is a GCL command MAINTAIN_GBASE (MNGB) in the library SA7.BIN. Use the command: MNGB? to define the name of the INPUT_GBASE member and the opening mode (OUTPUT or APPEND). If the member already exists, the OUTPUT mode will reset the INPUT_GBASE member. A hidden parameter is used to define the LM library.

Under the prompt **G** the following four commands are available:

Table 2-3. GCL Commands MAINTAIN_GBASE

Procedure	Alias	Domain	Action
MAINTAIN_GBASE	MNGB	H_NOCTX	
CREATE_PROJECT_RECORD	CRPR	GBASE	Create a project record
CREATE_USER_RECORD	CRUR	GBASE	Create a user record
LIST_SUBFILE_CONTENTS	LSS	GBASE	List the contents of the INPUT GBASE file
QUIT	Q	GBASE	Exit MNGB

2.3 HOW TO RESET THE AUDIT FILE

To reset the AUDIT file, use the JCL command:

```
S: EJ SA7-CLSA13  LIB= sl-liv;
```

Where `sl-liv` is the name of the SL library delivered with the product.

2.4 HOW TO DEFINE THE LIST UPDATING FREQUENCY

The ISM-UM export-import functions use files containing lists of objects to be processed. These lists are created from the GCOS 7 catalog by batch processing. They are updated regularly. To update the lists:

Insert the following command line into the SYSTEM member of the SITE.STARTUP library:

```
EJ SA7-LSP LIB=SA7.IUM.SL  EVERY=frequency;
```

- In this way you start batch processing for this member.
- To adjust the frequency, give a value to the EVERY parameter. The frequency can be a number and be expressed as follows:

  EVERY=1D with **D** for **Day**
  EVERY=2H with **H** for **Hour**
  EVERY=1M with **M** for **Month**

2.5 HOW TO MODIFY SCREEN FORMS AND MESSAGES

2.5.1 Modifying Screen Forms

You can modify screen forms using the JCL command MV-SAGRIL. The forms are delivered to the member SAGRIL in the library SA7.LIV.SL.

Screen forms are delivered either in English (code 826) or in French (code 250). You can translate the forms into other languages, however the length of the field labels must be respected.

Below is an example of the file format, for the screen form SAG391 which requests a password.

```
10    --SAG391 M 826
20    16 SA7 V3/SWAP V1.
30    13 ALEA    :
40    13 CERTIFICATE  :
50    13 PASSWORD:
60    13 USER    :
70    13 SURNAME :
80    13 FIRST NAME   :
90    75 TYPE THE CODE FIRST (IF CONTROL BY CODE)
100   75
110   75
120   75
130   75
140   75
150   75
160   75
170   10 MESSAGES   :
180   14 CODE (A/V) :
190   *
200   --SAG391 M 250
210   16 SA7 V3/SWAP V1.
 .
 .
 .
```

Explanation:

Line 10

The form name (here SAG391), preceded by '––' and followed by an action code:
M = Modify
C = Create
D = Delete
'Space' = No action

and a language code:

826 English
250 French
380 Italian
280 German
724 Spanish (etc.)

Lines 20 to 180	Contain the form labels. The maximum length of the label is indicated at the beginning of each line. (For example, line 130 indicates that the label cannot exceed 75 characters.) Lines 30, 40, 60, 70, 80, 90 are not displayed if the user connects under his name (instead of using a CP8 card). The type of connection is checked by a program.
Line 190	The character '*' is a separator.

2.5.2 Modifying Messages

The member SAMES1 of the library SA7.LIV.SL contains messages. The code names of these messages begin with S##, as follows:

S##A00 to S##A10	Service messages
S##A11 to S##A99	Titles of functions
S##000 to S##999	Messages related to the status of anomalies
S##C01 to S##ZZZ	Other messages.

The messages are delivered in English (code 826) and French (code 250). If you modify them, the field lengths must be respected.

The file format is identical to the format for screen forms, except that the length of the message is not indicated (see example below).

```
1860 *
1870 -S##C05 C 826
1880 THE DEADLINE MUST BE INFERIOR TO THE VALIDITY
1890 *
1900 -S##C06 C 826
1910 THE CYCLE HAS BEEN MODIFIED
1920 *
1930 -S##C07 C 826
1940 THE CYCLE HAS BEEN DESTROYED
1950 *
1960 -S##C08 C 826
1970 THE CYCLE DOES NOT EXIST
1980 *
1990 -S##C09 C 826
2000 MODIFICATION OF CYCLE 000 NOT ALLOWED
2010 *
```

2.5.3 Starting the JCL Commands MV-SAGRIL and MV-SAMES1

To load screen forms and messages, you must first stop TDS SA7 and the protected TDS programs, then start the following two jobs:

```
EJ MV-SAGRIL LIB=SA7.LIV.SL;
EJ MV-SAMES1 LIB=SA7.LIV.SL;
```

These two jobs reset the action codes to SPACE in the members SAGRIL and SAMES1.

If you need to make modifications in the future, you must add the action code **M** in the screen forms or messages to be modified.

3. Protection of TDS Applications

3.1 HOW TO DECLARE SECURITY FILES

To declare security files in the Application TDSs, declare:

- The files SAA01, SAA08 and SA13 in the catalog, with SHARE=MONITOR and JRNAL=BEFORE

- ACCESS=WRITE in the JCL.

See Appendix D for information on accessing SECUR'ACCESS files.

3.2 HOW TO PROTECT A TDS

To implement security functions for a TDS:

- Use the new options of TP7GEN as follows:
  - SA7=YES (with NO being the default value).
  - If you use "FULL IDS", the security modules that are executed are those delivered in H_SM_DUAL. Declare the value SA7IDS=YES.

    Otherwise, the security modules that are executed are those delivered in TPR99 and this TPR must be included in the SMLIB of the TDS starting with SA7.SMTPR. Load it using SYSMAINT. Declare the value SA7IDS=NO. The default value is YES
  - SA7CULIB= CU library containing the SA7 subprogram. For the full IDS, the default value is SA7.CUFIDS. Otherwise: SA7.CU_USER.
  - SA7CUDVC=device class of the SA7CULIB library. If the library is in the catalog, set the value to NIL.
  - SA7CUMD = media of the SA7CULIB library. If the library is in the catalog, set the value to NIL.
- Do not use the option USE SA7 in the STDS.

Execution of TP7GEN generates the security transactions and declarations of the security files in the STDS.

- Change the startup JCL of the TDS by doing an ASSIGN of the security files.

NOTES:

1. Application controls in a TDS are possible only with the option of active security on the site (SECOPT).
2. Operational examples are given in the library SA7.LIV.SL: see the MAQ∗ members.
3. It is possible to protect only some of the Application TDSs at one time.

3.3 HOW TO DECLARE THE SECURITY SUBPROGRAMS

To declare the security subprograms:

- Use the LINKER link editor to link subprograms SAS308, SAS309 and SAS310 with the calling TPRs. Never declare them in USE in the STDS .
- If a transaction contains a TPR which calls one of these subprograms, the following clause is required:

```
SUPPRESS CONCURRENT ACCESS SAA02, SAA03, SAA04, SAA05, SAA06,
SAA07
```

3.4 HOW TO DECLARE THE TRANSACTION STORAGE

For those transactions that call for a security check, the minimum size of the TRANSACTION STORAGE to be declared in the STDS is 118.

This size can be increased by that of the PRIVATE STORAGE by TP7GEN.

3.5 HOW TO CONTROL ACCESS ON PASSTHROUGH

The **PassThrough** transaction must be declared as follows in the STDS:

```
MESSAGE "PT" ASSIGN H_SEC_LGONPT...
```

This transaction is automatically added in the STDS generated with the option SA7=YES.

To execute a **PassThrough**, if a TPR is followed by the TPR H_TP7_PTTPR1, you must change this TPR to chain to the TPR H_SEC_LGONPT as soon as the TDS is protected. In fact TPR H_SEC_LGONPT provides the automatic sequence on H_TP7_PTTPR1.

ATTENTION

If the **PassThrough** function is used to log on to a TDS from IOF, the time interval since the last check is not taken into account.

3.6 HOW TO USE IDS II

3.6.1 IDS/II Status 40

The modules and subprograms designed to operate in IDS/II status 40 are delivered in the library SM SA7.SMTPR (TPR99).

1. Transfer TPR99 to the library tds.SMLIB of the TDS to be protected.

   You can transfer TPR99 to another TPR (TPR6 in the example below) using the following procedure:

   ```
   LMN SM LIB=<tds>.SMLIB;
   INLIB1 SA7.SMTPR;
   INIT MEMBER=TPR6 STN=B ESSTE=30 REPLACE;
   MOVE MEMBERS=TPR99, INLIB=INLIB1, REPLACE=1, NEW=TPR6;
   INIT MEMBER=TPR6, STN=B, ESSTE=8D, NEWSTE=30;
   QUIT;
   ```

2. In the STDS, set the number of TPR sharable modules to the value 100. In order to do this, use the command:

   ```
   NUMBER OF TPR SHARABLE MODULES IS 100.
   ```

3. To edit links of TPR applications calling control, use the subprogram SA7 in the SA7.CU_USER library (in USE in the STDS), and the subprograms SAS308, SAS309, SAS310.

3.6.2 IDS/II Status 50 (Full IDS/II)

The modules and subprograms for operation in Full IDS/II are located in the SM H_SM_DUAL.

1. To edit links of TPR applications calling control, use the subprogram SA7 in the SA7.LIV.CUFIDS library (in USE in the STDS), and the subprograms SAS308, SAS309, SAS310.

   The binary of the schema of the SA7 database (SCSA7) is delivered in IDS/II status 40.

2. Use the CONVERT program for conversion, with the startup of the next JCL:

   S: EJ SA7-CONV LIB=SA7.LIV.SL or GCL CONVERT command in the BIN SA7.BIN library.

   The GCL CONVERT command creates the library BIN SA7.LIV.BINFIDS if it does not exist already. For more information on these commands see *IDS/II Reference Manual Vol 1*. The result is transferred to the SA7.LIV.BINFIDS library.

The STDS must contain the clause "USE IDS-SUBSCHEMA." following the clause "USE FORMS."

The Startup JCL of the TDS must not contain the instructions: ASSIGN SWA01 DUMMY; ... concerning areas SWA01 to SWA60.

3.7 PROTECTION OF TDS HA

In order to protect TDS HA you must first of all, when installing SECUR'ACCESS, set the value of TDSHA to 1 and specify the volume name TDSHA_VOLUME in the ISI7 configuration file. (See *Interoperability Software Installation 7 - Administrator's Guid*e.)

The volume TDSHA_VOLUME must be shared by both machines in the HA environment (current and backup machines). The result of this is to create:

- a file SA7BLUE.SAA08 for TDS HA protected by the BLUE journal
- a file SA7GREEN.SAA08 for TDS HA protected by the GREEN journal.

TDS SA7 is a TDS of the type non-HA. This means that you must install SECUR'ACCESS on both machines (current and backup), and give different names to each TDS (SA7_DIR parameter).

You will find an example of the JCL sequences for the preparation (TP7PREP), generation (TP7GEN) and startup of TDS HA in the member MAQ_README of the library SA7.LIV.SL.

3.7.1 Preparing TDS HA

In the JCL sequence TP7PREP, you must specify the type of journal that you use to protect the TDS files (BLUE or GREEN).

```
$JOB TP7PREP HOLDOUT;
MVL SA7H,MS/B10,BFU096;
IVK TP7PREP,SYS.HSLLIB,VALUES=(&1,&2,&3,&2,&3,COBOL,SYSFILE=CAT,
   FILESTAT=CAT,CATNAME=SA7H,DEAL=Y,SMSZ=10,MAXSM=100,
   SW1SZ=16,BLKSZ=8192,
   OWNER=SYSADMIN,IMPORT=NO,HA=YES,JAS=BLUE);
$ENDJOB;
```

3.7.2 Generating TDS HA

The JCL sequence TP7GEN is not modified. <SA7_tdsname> represents the name of the TDS SA7 on the machine on which the generation is executed.

TDS with IDS2/Status 40

```
$JOB TP7GEN    HOLDOUT;
COMMENT '**********************************';
COMMENT '*     PROTECTION OF TDS SA7H,    *';
COMMENT '*          WITH IDS2/ETAT 40     *';
COMMENT '**********************************';
IVK TP7GEN,SYS.HSLLIB,VALUES=(SA7H,LM=SA7H.LMLIB,
                              SA7=YES,
                              SA7IDS=NO,
                              SA7CULIB=<SA7_tdsname>.CU_USER,
                              SA7CUDVC=NIL,SA7CUMD=NIL
                             );
COMMENT '*********************************';
COMMENT '*      INTEGRATION OF TPR99     *';
COMMENT '*********************************';
LIB SM INLIB1=<SA7_tdsname>.SMTPR;
LIBMAINT SM LIB=SA7H.SMLIB
             COMMANDS=' MV IL1:TPR99 REPLACE;'
             PRTFILE=DUMMY;
$ENDJOB;
```

TDS with IDS/Status 50 or Full IDS

```
$JOB TP7GEN    HOLDOUT;
COMMENT '**********************************';
COMMENT '*     PROTECTION OF TDS SA7H,    *';
COMMENT '*          WITH IDS2/ETAT 50     *';
COMMENT '**********************************';
IVK TP7GEN,SYS.HSLLIB,VALUES=(SA7H,LM=SA7H.LMLIB,
                              SA7=YES,
                              SA7IDS=YES,
                              SA7CULIB=<SA7_tdsname>.CUFIDS,
                              SA7CUDVC=NIL,SA7CUMD=NIL
                             );
$ENDJOB;
```

3.7.3 Starting Up TDS HA

Before starting TDS HA you must create, on a shared disk, the following libraries:

<nameTDSHA>.BIN,
<nameTDSHA>.LIV.BINIDS if your TDS uses IDS status 40
<nameTDSHA>.LIV.BINFIDS if your TDS uses IDS status 50.

These files are copies of, respectively, the files SA7.BIN, SA7.LIV.BINIDS and SA7.LIV.BINFIDS.

In the example below, the file SAA08 is protected by the BLUE journal. If your TDS uses the GREEN journal, replace SA7BLUE with SA7GREEN.

TDS with IDS/Status 40

```
*        TP7JCLACT
*
$JOB SA7H-ACT CLASS=J HOLDOUT USER=SA7;
MVL TDSNAME=SA7H,
    HA=Y;
LIB SM INLIB1=(&TDSNAME.SMLIB);
SYSMAINT COMFILE=*LTPR;
$INPUT LTPR;
MNSYSSM;
LOAD MODULE=TPR INPUT=INLIB1 REPLACE OLDVERS;
LOAD MODULE=TPR99 INPUT=INLIB1 REPLACE OLDVERS;
QUIT;
QUIT;
$ENDINPUT;
JOBLIB SM &TDSNAME.SMLIB;
$CONSOLE SA7;
STEP &TDSNAME FILE=(&TDSNAME.LMLIB) OPTIONS='HA='&HA''   ;
SIZE 1500,NBBUF=128,POOLSIZE=500;
ASSIGN DBUGFILE &TDSNAME.DEBUG SHARE=DIR;
COMMENT '*** ASSIGNMENTS FOR APPLICATION CHECKS ***';
ASSIGN H_BJRNL DVC=MS/B10 MD=BFU0I6 FILESTAT=TEMPRY NEXT POOL;
ASSIGN BLIB       &TDSNAME.BIN ACCESS=READ;
ASSIGN DDLIB1     &TDSNAME.LIV.BINIDS   ACCESS=READ;
ASSIGN SAA08      SA7BLUE.SAA08           ACCESS=WRITE;
ASSIGN IDSOPT  &TDSNAME.SL SUBFILE=OPTIDS  SHARE=DIR ACCESS=READ ;
ENDSTEP;
SYSMAINT COMFILE=*UTPR;
$INPUT UTPR;
SM;
UNLOAD MODULE=TPR EFN=&TDSNAME.SMLIB;
UNLOAD MODULE=TPR99 EFN=&TDSNAME.SMLIB;
QUIT;
$ENDINPUT;
$ENDJOB;
*
```

```
*        TP7JCLBAC
*
$JOB SA7H-BAC CLASS=P HOLDOUT USER=SA7;
MVL TDSNAME=SA7H,
    HA=Y;
LIB SM INLIB1=(&TDSNAME.SMLIB);
SYSMAINT COMFILE=*LTPR;
$INPUT LTPR;
MNSYSSM;
LOAD MODULE=TPR INPUT=INLIB1 REPLACE OLDVERS;
LOAD MODULE=TPR99 INPUT=INLIB1 REPLACE OLDVERS;
QUIT;
QUIT;
$ENDINPUT;
JOBLIB SM &TDSNAME.SMLIB;
$CONSOLE SA7;
STEP &TDSNAME FILE=(&TDSNAME.LMLIB) OPTIONS='HA='&HA''   ;
SIZE 1500,NBBUF=128,POOLSIZE=500;
COMMENT '*** ASSIGNMENTS FOR APPLICATION CHECKS ***';
ASSIGN BLIB       &TDSNAME.BIN ACCESS=READ;
ASSIGN DDLIB1     &TDSNAME.LIV.BINIDS   ACCESS=READ;
ASSIGN H_BJRNL DVC=MS/B10 MD=BFU0I6 FILESTAT=TEMPRY NEXT POOL;
ASSIGN IDSOPT &TDSNAME.SL SUBFILE=OPTIDS ACCESS=READ;
ENDSTEP;
SYSMAINT COMFILE=*UTPR;
$INPUT UTPR;
SM;
UNLOAD MODULE=TPR EFN=&TDSNAME.SMLIB;
UNLOAD MODULE=TPR99 EFN=&TDSNAME.SMLIB;
QUIT;
$ENDINPUT;
$ENDJOB;
```

TDS with IDS/Status 50 or Full IDS

```
*        TP7JCLACT
*
$JOB SA7H-ACT CLASS=J HOLDOUT USER=SA7;
MVL TDSNAME=SA7H,
    HA=Y;
LIB SM INLIB1=(&TDSNAME.SMLIB);
SYSMAINT COMFILE=*LTPR;
$INPUT LTPR;
MNSYSSM;
LOAD MODULE=TPR INPUT=INLIB1 REPLACE OLDVERS;
QUIT;
QUIT;
$ENDINPUT;
JOBLIB SM &TDSNAME.SMLIB;
$CONSOLE SA7;
STEP &TDSNAME FILE=(&TDSNAME.LMLIB) OPTIONS='HA='&HA''   ;
SIZE 1500,NBBUF=128,POOLSIZE=500;
ASSIGN DBUGFILE &TDSNAME.DEBUG SHARE=DIR;
COMMENT '*** ASSIGNMENTS FOR APPLICATION CHECKS ***';
ASSIGN H_BJRNL DVC=MS/B10 MD=BFU0I6 FILESTAT=TEMPRY NEXT POOL;
ASSIGN BLIB     &TDSNAME.BIN ACCESS=READ;
ASSIGN DDLIB1   &TDSNAME.LIV.BINFIDS   ACCESS=READ;
ASSIGN SAA08    SA7BLUE.SAA08          ACCESS=WRITE;
ASSIGN IDSOPT   &TDSNAME.SL SUBFILE=OPTIDS  SHARE=DIR ACCESS=READ;
ENDSTEP;
```

```
SYSMAINT COMFILE=*UTPR;
$INPUT UTPR;
SM;
UNLOAD MODULE=TPR EFN=&TDSNAME.SMLIB;
QUIT;
$ENDINPUT;
$ENDJOB;
*
*
*        TP7JCLBAC
*
$JOB SA7H-BAC CLASS=P HOLDOUT USER=SA7;
MVL TDSNAME=SA7H,
    HA=Y;
LIB SM INLIB1=(&TDSNAME.SMLIB);
SYSMAINT COMFILE=*LTPR;
$INPUT LTPR;
MNSYSSM;
LOAD MODULE=TPR INPUT=INLIB1 REPLACE OLDVERS;
QUIT;
QUIT;
$ENDINPUT;
JOBLIB SM &TDSNAME.SMLIB;
$CONSOLE SA7;
STEP &TDSNAME FILE=(&TDSNAME.LMLIB) OPTIONS='HA='&HA''   ;
SIZE 1500,NBBUF=128,POOLSIZE=500;
COMMENT '*** ASSIGNMENTS FOR APPLICATION CHECKS ***';
ASSIGN BLIB       &TDSNAME.BIN ACCESS=READ;
ASSIGN DDLIB1     &TDSNAME.LIV.BINFIDS   ACCESS=READ;
ASSIGN H_BJRNL DVC=MS/B10 MD=BFU0I6 FILESTAT=TEMPRY NEXT POOL;
ASSIGN IDSOPT &TDSNAME.SL SUBFILE=OPTIDS ACCESS=READ;
ENDSTEP;
SYSMAINT COMFILE=*UTPR;
$INPUT UTPR;
SM;
UNLOAD MODULE=TPR EFN=&TDSNAME.SMLIB;
QUIT;
$ENDINPUT;
$ENDJOB;
```

4. IUM-SA7 Agent under GCOS 7

4.1 HOW TO START UP THE SA7SRV SERVER

The part of the IUM-SA7 agent that runs under GCOS 7 is an RPC server called SA7SRV which remains constantly in wait for requests from ISM-UM.

4.1.1 Prerequisites

To start up the SA7SRV server, OPEN 7, GX-RPC7 and sockg7 must be installed and active.

NOTE: If the GCOS 7 site is not protected or if SA7 is not active, the SA7SRV server will start up, but upon the first request it will inform ISM-UM that it cannot administer this unprotected site.

4.1.2 Startup Procedure for the SA7SRV Server

Upon installation, ISI7 automatically installs and starts up all the software programs needed for the operation of the SA7SRV server.

For more information, see the *Interoperability Software Installation 7 - Administrator's Guide*.

After the SA7SRV server is activated by ISI7, a test is carried out to check the communication between the client part and the server part of the IUM-SA7 agent. This test also checks that the GCOS 7 system is protected.

4.1.3 How to Restart the SA7SRV Server after it Aborted

If the SA7SRV server is halted while OPEN 7 and GX-RPC7 are active, in order to restart the server :

1. Log on as SYSADMIN user.

2. Enter the JCL command used by ISI7 :

```
EJ EXEC_SI7_SA7SRV LIB=SA7.IUM.SL
```

4.1.4 How to Restart SA7SRV Server after a GCOS 7 Crash

After a restart of GCOS 7, if you want to activate the IUM-SA7 agent :

1. Restart OPEN 7. For more information on the procedure, see the document *OPEN 7 Administrator Guide*. This procedure is used to automatically start the **subux** sub-system as well as the socket server used by the SA7SRV server.

2. Load the SM **sys.dcm.system.**

3. Re-start the SA7SRV server.

4.2 HOW TO HALT THE SA7SRV SERVER

To halt the SA7SRV server :

1. Load the binary library **sys.dcm.rpc.binlib**. To do this:
   Use the command **mwinlib bin sys.dcm.rpc.binlib**.

2. Enter the “terminate a RPC server” command :

```
TERMINATE_RPC_SERVER <Number of RON>
```

or

```
trpcs <number of RON>
```

5. Troubleshooting

5.1 HOW TO RESTART A COMPONENT OF THE SYSTEM

5.1.1 How to Handle a Failure of the TDS SA7

The TDS SA7 is not accessible due to:

- a TELECOM halt
- a crash
- a premature termination
- a CJ of the TDS SA7
- an unavailable SA7

TELECOM halt

A TELECOM halt does not affect the TDS SA7. Restart the TELECOMs

Crash

In case of crash, see the **Procedures after a crash**.

Premature Termination

In the case of a premature termination, restart TDS SA7 (with rollback of the SA7 database and file SA13).

CJ of the TDS SA7

You can have files in FLNAV. In this case, do LOADFILE or FILREST for the files in FLNAV.

SA7 unavailable

When the SA7 is unavailable, see **Procedure: What to do if the TDS SA7 is unavailable**.

5.1.2 How to Handle a Failure of the SA7 Database

The database is unavailable due to:

- a crash
- inconsistency of the database
- its being offset in relation to the catalog

Crash

In case of a crash, see the section, **What to do in case of RESTART WARM**. A crash can take place following one of the following messages:

- IO EXCEPTION
- CHANNEL EXCEPTION ON MC
- HARDWARE FAILURE

Inconsistency of the database

To handle an inconsistency of the database, see the section on **What to do if the SECUR'ACCESS database is inconsistent** in this chapter.

Offset in relation to the catalog

The security database can be offset in relation to the catalog after a:

- crash
- IDS II software error on SA7

In this case, the user cannot connect to a protected application, but can connect to an unprotected application. To re-establish consistency:

1. Halt the GSP (TJ) server and the TDS SA7.

2. If the database and the catalog have been saved at the same time, restore the SA7 database and the catalog of the last save operation. Otherwise, recover the catalog (see **Batch Processing**).

3. Restart the GSP server and the TDS SA7.

5.1.3 How to Handle a Catalog Failure

A catalog failure can be due to:

- a crash
- an inconsistent file
- its being offset in relation to the SA7 database

Crash

See the section **What to do in case of RESTART WARM** in case of:

- IO EXCEPTION
- CHANNEL EXCEPTION ON MC
- HARDWARE FAILURE

Inconsistent file

See **What to do if the files are inconsistent** in this chapter.

Offset in relation to the SA7 database

If the catalog is offset in relation to the SA7 database, the user can no longer log on. See **Offset in relation to the Catalog** in the section **How to handle a failure of the SA7 database**.

5.1.4 How to Handle a GSP Server Failure

A failure of the GSP server can be due to:

- a TELECOM halt
- a crash
- a CJ

TELECOM halt

If all the sessions communicating with the GSP server are closed, the server will free its resources one minute after the last TELECOM supervisor halts. The GSP server remains on standby. To restart the GSP server:

1. Use the following command to restart the TELECOMs:

   ```
   ESC PSG START
   ```

   To stop the GSP server, use the TSYS command.

2. If a session remains active, the GSP server remains active and does not free any of its resources.

   To make the GSP server operational, restart the TELECOMs.

Crash

In case of a crash, restart the GSP server using the command:

```
S: EJR SA7-PSG ...
```

CJ

To correct the CJ:

1. Stop the TDS SA7.

2. In order restart the GSP server, use the **EJR** command.

3. Restart the TDS SA7.

5.1.5 How to Handle an Agent Failure

On the SA7SRV server, you can encounter two types of failures:

- on the processing of the server
- during administration operation.

5.1.5.1 How to Analyze an SA7SRV Error Message

The SA7SRV server can experience a failure during its startup. In this case, it aborts and a message explaining the reason is either written in the JOB output or sent to the terminal. Check the list of messages and corrective actions available:

- Abort with the user message:

  ```
  "*** MI CONTROL: NO MI AVAILABLE FOR IUM-SA7 MANAGEMENT ***
  ```

  Do not use the SA7SRV server. Contact your Bull representative.

- Abort with the user message:

  ```
  "*** ERROR IN H-UNIX-SUBCMS ***"
  ```

  Check that the subux system is running on OPEN 7.

- Abort with the job output message:

  `"Fault data descriptor"` (in the JOR)

  Check that the SM "H_SM_DCM" is loaded.

- Abort with user message:

  `"RPC: abort execution==>no accessible protocol"` (in the JOR)

  Check that the socket server is running on OPEN 7.

- Abort with the JOB message:

  ```
  "ERROR: cpg to v -f SA7.IUM-SL -S ST7SEC + BINDING /tmp/SA7SEC -
   BINDING;"
  ```

  - If the abort is on OPEN 7 (oscit vl=0x600) (in RON:2:1), check that the **/tmp** directory in OPEN 7 is not full.

  - If the abort is on OPEN 7 (oscit vl=0x100) (in RON:2:1), check that the user starting the SA7SRV is a "sysadmin" user.

For any other problems, refer to your Bull representative, providing him/her with the job outputs (RON:1, RON:2:1 ...).

5.1.5.2 How to Analyze an Operation Error Message

During operation, you can encounter two types of failures:

- The IUM-SA7 agent does not respond
- TDS/SA7 status

IUM-SA7 agent does not respond

If the IUM-SA7 agent does not respond, the message RPC_X_COMM_FAILURE is received by ISM_UM:

1. Check the functioning of the socket server.

2. If necessary, stop the socket server then restart the socket server.

3. Restart the agent.

Problem of TDS/SA7 status

In case of a problem with TDS/SA7 status:

1. Stop the IUM-SA7 agent.

2. Check that the GCOS 7 Security Administrator known from IUM is no longer connected to SECUR'ACCESS.

3. Restart this agent.

5.2 PROCEDURES AFTER A CRASH

5.2.1 Symptoms of a Crash

A crash is notified on the system console by the following messages:

- CHANNEL EXCEPTION ON MC
- IO EXCEPTION
- HARDWARE FAILURE
- CALL TO PANIC (called by a GCOS 7 component)
- SYSTEM RESTART (crash triggered by SR)

5.2.2 What to Do in Case of RESTART WARM

To restart security in case of RESTART WARM:

1. Restart the TDS SA7 (with REPEAT option) either manually or automatically, using the `SYS.REPLY` command.

   The ROLLBACK procedure of the SA7 database and the SA13 file is started. If ROLLBACK fails, proceed with the restoration of the database and the file.

2. Restart the GSP server, the TDS SA7 and SA7-MASTER.

3. Restart the IUM-SA7 agent.

5.3 WHAT TO DO IF THE TDS SA7 IS UNAVAILABLE

If you have a problem in connection, check that the TDS SA7 is operational. To do this, you can use:

- the MAIN console
- any other terminal

From the MAIN console

You can log on as:

- user of the OPERATOR project if the SECOPT option includes the clause `SA7NOCSL=YES`

- or, as user SECADMIN.

From any terminal

From any terminal for users of the OPERATOR project, or for the SECADMIN user.

- **If access is protected by the card and its code**, log on to IOF.

  - If authentication is impossible because a component of SECUR'ACCESS is unavailable, the password level check is done in downgraded mode (catalog check).

  - If the password is rejected because of a catalog access problem, access is authorized.

- **If access is protected by password**, SECUR'ACCESS checks the password.

  - If this check fails because a component of SECUR'ACCESS is unavailable, the password level check is done in downgraded mode (catalog check).

  - If the password is rejected because of a catalog access problem, access is authorized.

5.4 WHAT TO DO IF THE FILES ARE INCONSISTENT

In order to continue working after the message **Inconsistent files**, restart:

- the SECUR'ACCESS database and/or
- the catalog

5.4.1 What to Do if the SECUR'ACCESS Database is Inconsistent

Restore the SECUR'ACCESS database and the files from the save files and from the AFTER journal (ROLLFORWARD static if AFTER journal).

5.4.2 What to Do if the Catalog is Inconsistent

If there is an R-Set or P2-Set disk on line:

From R-Set or P2-Set, do a FILREST from the save file.

If there is no R-Set or P2-Set disk, or production disk:

1. Set the cursor under SIP.
2. Do a RESTORE of the system disk from a system disk save image.

5.5 HOW TO EXECUTE A SAVE

Depending on how often users are updated in the SECUR'ACCESS database and in the catalog, carry out simultaneous save operations of the database and the catalog.

- If you can halt the TDS SA7, do a simple save of the SA7 database and the SA13 file.
- If you cannot halt the TDS SA7, you can do four types of saves:
  - by SABASE transaction under TDS SA7
  - by RDDF7, possibly on the same site
  - by mirror disk
  - by simple save

5.5.1 How to Handle a Save by SABASE Transaction

The SABASE transaction under TDS SA7 enables you to save on a sequential file of the SA7 database.

5.5.2 How to Handle a Save by RDDF7 on the Same Site

RDDF7, possibly on the same site, enables you to duplicate the SA7 database.

- If RDDF7 is halted, double writes are stored in a buffer file.
- If RDDF7 is active, you must have the AFTER journal.

5.5.3 How to Handle a Save by Mirror Disk

The mirror disk function is used only on the SA7 database because the mirror disk function does not work and the catalog is on a resident disk.

5.5.4 How to Do a Simple Save

A simple save is carried out on:

- the SA7 database
- the catalog

On the SA7 database

To save the SA7 database:

1. Make sure that no update of the database is taking place.

2. To carry out the save on tape or work disk, use the `VOLSAVE DIRTY` command. You can also use the `FILREST` command (and `FILSAVE` on tape)

On the catalog

To save the catalog, carry out a simple save.

A. New GCOS 7 Technical Status

When a new GCOS 7 Technical Status is implemented, you must carry out the following operations :

1. Using version V3.2 (or later) of SECUR'ACCESS, copy the members SA7VL and SA7_MBXNAME from the library SA7.LIV.SL to the library SYS.HSLLIB.

   ```
   LMN SL LIB=SYS.HSLLIB;
   IL1 SA7.LIV.SL;
   MOVE SA7VL INLIB1;
   MOVE SA7_MBXNAME INLIB1, INFORM=SARF, OUTFORM=SARF;
   QUIT;
   ```

2. Update the SM H_SM_DUAL with JCL SA7-SMDUAL from the library SL SA7.LIV.SL.

3. Update the library SYS.HBINLIB by transferring the security modules that can be downloaded from SA7.LIV.BIN.

   ```
   S: LMN BIN SYS.HBINLIB;
   C: IL1 SA7.BIN;
   C: MV *SECUR* IL1;
   C: QUIT;
   ```

4. Apply the corrections specific to SECUR'ACCESS V3.3 (see the Customer Service Bulletin for SECUR'ACCESS).

5. Carry out a RESTORE session on your system.

B. The SECOPT Declaration

B.1 PURPOSE

The SECOPT declaration is added into the CONFIG file and is used to select security-related options.

B.2 FORMAT

The SECOPT format is as follows:

```
SECOPT          SA7LOGON=(NO/YES)
                SA7ADMIN=(NO/YES)
                SA7NOCSL=(NO/YES)
                NETSEC=(NO/YES)
                CHKPW=(NO/YES);
```

B.3 DESCRIPTION OF THE PARAMETERS

The SECOPT parameters are:

SA7LOGON

If set to NO (default value), user access rights are validated at connection time by VCAM.
If set to YES, user access rights are validated at connection time by TDS/IOF applications (which call SECUR'ACCESS V3).

SA7ADMIN

If set to NO (default value), user administration is managed by SYSADMIN (using the MNCAT facility).
If set to YES, user administration is managed by the SECUR'ACCESS administrator (using SECUR'ACCESS V3).

SA7NOCSL

If set to NO (default value), the identity of users logging on to the local system console is validated by SECUR'ACCESS V3.
If set to YES, the identity of users logging on to the local system console is not validated by SECUR'ACCESS V3.

NETSEC and CHKPW

See the *System Installation Configuration and Updating Guide*.

C. Management of the GSP Server

C.1 DESCRIPTION

This server has a "MAILBOX" whose parameters can be set and which can be managed through commands.

For more information see the SECUR'ACCESS Security Administrator’s Guide
(47 A3 01BD).

It must be started up AFTER the startup of the TELECOM server(s). Halting it is linked to the termination of GCOS 7 (TSYS command on the operator console).

C.2 THE COMMANDS

ESC PSG START: Indicates to the GSP Server that the TELECOM supervisor(s) are restarted.

ESC PSG STATUS: Gives the following information on the status of the GSP Server:
CNX USERS : n Number of user sessions in progress (TDS/IOF).
CNX PSG : n Number of open sessions toward the GSP Server.
TTSVR : Y/N Y: halt of TELECOMs is requested.
TSYS : Y/N Y: halt of GCOS 7 is requested.
RELEASED : Y/N Y: the "MAILBOX" of the GSP Server is free. The START command is required after the TELECOMs are restarted.

ESC PSG HELP: Gives the list of commands.

ESC PSG DEBUG/NDEBUG:
Activates or deactivates the trace of events received by the server. This trace is written in the job occurrence report (JOR).

C.3 OPERATION

When the TELECOM supervisor(s) are halted by the operator, two cases are possible:

- All the sessions (TDS, IOF or PSG) in communication with the GSP Server are closed.
- At least one session with the GSP Server remains open.

The TELECOMs are stopped and there are no open sessions.

The GSP Server frees its resources one minute after the last TELECOM supervisor is halted (in order to generate DATANET for example).

The GSP Server remains on standby and can be restarted by the ESC PSG START command after the TELECOMs are restarted, or halted by the TSYS command.

NOTES:

1. Without the ESC PSG START command (after restart of the TELECOMs), the security checks that use a CP8 card cannot function.

2. Do not use the ESC PSG START command **BEFORE** restarting the TELECOMs.

The TELECOMs are halted and there is at least one session open.

The GSP Server remains active and does not free any of its resources. If the TELECOMs are restarted, it will be immediately operational.

If the user running the open session logs off, the GSP Server goes on standby.

D. SECUR'ACCESS Files

D.1 TABLE OF ACCESS TO SECUR'ACCESS V3 FILES

Table D-1 provides access information for SECUR'ACCESS V3 files.

Table D-1. Access to SECUR'ACCESS V3 files

		TDS SA7		**Other TDSs**	
Files	Catalog	STDS	JCL	STDS	JCL
SAA01	MON/BEF	I/O	W	I/O	W
SAA02	MON/BEF	I/O	W	I	R
SAA03	MON/BEF	I/O	W	I	R
SAA04	MON/BEF	I/O	W	I	R
SAA05	MON/BEF	I/O	W	I	R
SAA06	MON/BEF	I	R	I	R
SAA07	MON/BEF	I	R	I	R
SAA08	MON/BEF	I/O	W	I/O	W
SA13	MON/BEF	I/O	W	I/O	W

The abbreviations used in this table have the following meanings:

MON	Monitored
BEF	Before log
I	Input
O	Output
W	Write
R	Read
One	One write
NOR	Normal
NO	NO journal

NOTE : REPEAT option must be used on STEP TDS.

D.2 FORMAT OF THE SA7.SA13 FILE

FORMAT	UFAS
CISIZE	2048
ORG	INDEXED
RECFORM	F
RECSIZE	210
CIFSP	20
KEYLOC	1
KEYLGTH	22

Glossary

ACCESSMASTER

Bull S.A. security product which allows a consistent security policy across an entire I.T. system.

APPLICATION

Program or set of programs describing a specific problem and allowing to settle it. An application can be split into modules.

ASYNCHRONOUS TERMINAL

Terminal in which the execution of each operation is started following a sign bit which is emitted at the end of the previous operation, without necessarily taking the machine cycle into account.

AUTHENTICATION

Verification that the person, who is trying to log on or who is already connected, is really the user known to the system. The authentication is executed using a password or a CP8 smart card.

AUTHENTICATOR

Autonomous smart card reader with a keyboard and a display window for obtaining the serial number of the card and certificates. It is a certifier, modified so that SECUR'ACCESS can use M6 cards and TB10 cards. The authenticator is also called an "unconnected reader".

AUTHORIZATION

Verification that the user has the right to access all or part of the application. The authorization is initiated by the application, which asks SECUR'ACCESS to check the user's access rights.

CAD1004

Authenticator that can be loaded by PROCARD to process M4 mask, M6 mask, TB10 mask cards and cards of the SCOT family.

CAM

Communication Access Method.
Communication interface between tasks on the DPS 7000.

CATALOG

Particular type of file indexing a set of objects organized according to a tree structure. This structure is composed of a root, master directories, directories and files. The catalog gathers data concerning objects that it contains, for example access rights and site information. The use of catalogs file management and use easier.

CERTIFICATE

Result of a computation performed by the card and involving a random number - challenge -, the confidential code, secret data from the card and data known to the card.

CHALLENGE

Random number (64 bits) supplied in input for certificate computation. By extension for SECUR'ACCESS, it is the number which appears on the control and signature screen forms in the form of 4 digits to complete the 4 digits of the confidential code.

CNS

Communications Network Software. The operating system of Bull's CNP7 processor.

CONNECTED READER

Smart card reader integrated in a terminal allowing dialog between the card and SECUR'ACCESS. In contrast to the unconnected reader - or authenticator -, actions requested from the card are executed automatically between the system and the card.

CP8 SMART CARD

Card including a microprocessor similar to a plastic credit card of ISO 2896 norm on which a CP8 component integrating the microprocessor is inserted.

DATANET

Front-end processor or communications concentrator in a Bull network.

DES

Data Encryption Standard.
Reversible, symmetric scramble algorithm for secret keys.

DNS

Distributed Network Supervisor
The operating system for Bull's Datanet.

DPS

Distributed Processing System.

FORMS

Multi-terminal display interface software enabling applications to work with a virtual terminal.

GCL

GCOS 7 Command Language

GCOS 7

GCOS = General Comprehensive Operating System
Basic software of the DPS 7000.

GSP

Generalized Security Processor.
This a PC equipped with the SECURITEX card, providing security functions when an M4 mask card or a card of the SCOT family (SCOT10, SCOT100) is used.

IDENTIFICATION

Verification that the user is known to the system. The user's identification is performed using his/her identifier.

IDS/II

Management system providing to independent users the access to an integrated data base. The data base logical structure is described by a diagram in DDL (Data Description Language). The data base physical features are described in DMCL (Device/Media Control Language).

IOF

Interactive Operation Facility.
Open GCOS 7 system giving several users time-shared access to the resources offered on the DPS 7000 with the necessary tools.

ISM

Integrated System Management.
Allows consistent management of distributed systems and network resources in a multi-supplier site.

ISM-UM

Integrated System Management-User Management
ISM application for a distributed environment which manages users, their privileges, services and subscriptions to services. It forms the main part of ISM.

JCL

Job Control Language.
Language used to write command files for execution of tasks under GCOS 7.

LCP8

Keyboard-mounted CP8 smart card reader for QUESTAR 210/310 terminals. Can be remotely loaded from a GCOS 7.

LECAM

Smart card reader which can be connected to the MINITEL.

LOGON

Program executed at the moment of user connection (under TDS). Also, name given to the connection phase itself.

MASK

Type of smart card program. By extension, it defines the type of card.

MCS

Control and Security Module.
Installed in the GSP, this module contains the security elements for the verification computations for certificates from the user's smart cards.

MI

Marketing Identifier.
Commercial unit used to identify part or all of a software product.

MINITEL

Mass-distribution videotex terminal distributed by FRANCE TELECOM. Certain types can also work in 80-column asynchronous mode.

M6, MC, MD, MQ

Types of card masks (see MASK).

MC	SCOT60
MD	SCOT110
MQ	TB100

NS

Network Station.
See the manual on DATANET generation.

PRIVILEGE

If the control level of a project is defined as "privileged", then this control level is the one which will be taken into account on connection to the project.

PROCARD

Specialized smart card for loading the CAD1004s. It contains the program which manages the reader for M4 mask, M6 mask, TB10 mask cards or cards of the SCOT family for SECUR'ACCESS purposes. The program is identified by an application number and a release number.

PROJECT

For the GCOS 7 catalog, the project is a set of users who can access a set of applications. Each user is known under the name of at least one project.

SCAM

Smart Card Access Method.
Method of access to the GSP server functions and the card readers (reserved for SECUR'ACCESS).

SIB

Security Information Base.
Database containing objects, and the links between the objects, managed by ISM-UM.

SCOT FAMILY

Type of card masks family including MA and MB (see MASK).

SERIAL NUMBER

Identifier of a smart card. This identifier is unique and is stored on the card itself.

SITE CATALOG

Catalog which contains data necessary to the access control to the system (users' names, projects' names, environments...), descriptions of the site files and descriptions of the private catalogs associated with projects.

SPOM

Self Programmable On chip Microprocessor.
Identifies the type of micro-processor installed on a smart card.

STARTUP

Set of commands run when the DPS 7000 starts up (system startup), or when a user connects up to IOF.

SYNCHRONOUS TERMINAL

Terminal in which the operations are executed according to a certain number of complete cycles.

SYSADMIN

Project in the GCOS 7 catalog grouping users who have GCOS 7 system management functions.

SYSOUT

File for holding the records intended for printing.

TB100

TRT BULL100

Multi-service smart card allowing storage of data into *public*, *secret*, *access* and *transaction* partitions. Name given to MP mask cards (see MASK).

TDS

Transaction Driven Subsystem
GCOS 7 subsystem allowing the creation, the management and the running of transactional applications, that is to say applications in which the processing to perform is determined by the data entered.

TLP

Smart card reader distributed by Bull-CP8.

TSB

Technical Software Bulletin.
This document contains all the information concerning the installation and execution environment of a software product. For SECUR'ACCESS, it is accompanied by an appendix describing the different phases of installation.

UFAS

United File Access Method.
See UFAS manual: 47A201UF. UFAS is a unified data management method for the DPS 7 system.

UNCONNECTED READER

See AUTHENTICATOR

WITNESS

For SECUR'ACCESS, this is a user who can authenticate himself/herself correctly in the place of someone else, thereby guaranteeing this person's identity to a security administrator.

Index