Using the COBOL Wrapper with Natural Security and Impersonation

Using the COBOL Wrapper with Natural Security and Impersonation

This chapter explains how clients built with the COBOL Wrapper can communicate with Natural RPC Servers running under Natural Security and RPC servers running with impersonation. See *Impersonation* under z/OS Batch | z/OS CICS | z/OS IMS | z/VSE CICS.

This chapter assumes that you are familiar with the concepts of Natural Security and impersonation. To communicate with such a server you will need the following components:

- the *Generic RPC Services Modules*, which are provided to create and get a security token,
- the *RPC Communication Area*

To authenticate against Natural Security or impersonated RPC server

1. Specify a user ID, password and optional Natural library in the RPC communication area:

```
*  Client information :                 bytes 101-300
    10 COMM-USERID.
              15 COMM-USERID1      PIC X(8).
              15 COMM-USERID2      PIC X(8).
    10 COMM-PASSWORD               PIC X(8).
    10 COMM-LIBRARY                PIC X(8).
    10 COMM-SECURITY-TOKEN-LENGTH  PIC 9(4) BINARY.
    10 COMM-SECURITY-TOKEN         PIC X(100).
    10 FILLER                      PIC X(66).
```

2. Create a security token with the function Create Security Token `CT` provided by the generic RPC services module.

   In the scenarios *Micro Focus*, *Batch*, *CICS* and *IMS* with the *Call Interface*:

   - For *RPC Communication Area* setting `Linkage` and `External`:

```
  MOVE "2000" TO COMM-VERSION.
  MOVE "CT"   TO COMM-FUNCTION.
* Set user ID and password in RPC Communication Area
  MOVE "NAT-USER"  TO COMM-USERID.
  MOVE "NAT-PWD"   TO COMM-PASSWORD.
* Additional for Natural Security set library in RPC Communication Area
  MOVE "NAT-LIB"   TO COMM-LIBRARY.
  CALL "COBSRVI" USING ERX-COMMUNICATION-AREA
  ON EXCEPTION
  . . .
  NOT ON EXCEPTION
  . . .
  END-CALL.
```

   - For *RPC Communication Area* setting `Copybook`. Add the following COBOL Statements to the `COBINIT` copybook:

Using the COBOL Wrapper with Natural Security and Impersonation

```
MOVE "CT"   TO COMM-FUNCTION.
 * Set user ID and password in RPC Communication Area
MOVE "NAT-USER"  TO COMM-USERID.
MOVE "NAT-PWD"   TO COMM-PASSWORD.
 * Additional for Natural Security set library in RPC Communication Area
MOVE "NAT-LIB"   TO COMM-LIBRARY.
CALL "COBSRVI" USING ERX-COMMUNICATION-AREA
```

See also *Using the Generated Copybooks*.

Or:
In the scenario *Using the COBOL Wrapper for CICS with `DFHCOMMAREA` Calling Convention (z/OS and z/VSE)* with *the EXEC CICS LINK Interface*:

```
MOVE "2000" TO COMM-VERSION.
MOVE "CT"   TO COMM-FUNCTION.
* Set user ID and password in RPC Communication Area
MOVE "NAT-USER"  TO COMM-USERID.
MOVE "NAT-PWD"   TO COMM-PASSWORD.
* Additional for Natural Security set library in RPC Communication Area
MOVE "NAT-LIB"   TO COMM-LIBRARY.
EXEC CICS LINK PROGRAM  ("COBSRVI")
               RESP     (CICS-RESP1)
               RESP2    (CICS-RESP2)
               COMMAREA (ERX-COMMUNICATION-AREA)
               LENGTH   (LENGTH OF ERX-COMMUNICATION-AREA)
END-EXEC.
IF WORKRESP = DFHRESP(NORMAL)
   IF (COMM-RETURN-CODE = 0) THEN
*       Perform success-handling
    ELSE
*       Perform error-handling
    END-IF
ELSE
*    Perform error-handling
END-IF.
```

After successful return from the generic RPC services module, the security fields in the RPC communication area are properly set, so they can be used in subsequent RPC requests to a secure RPC server, such as:

- Natural RPC server running with Natural Security
- RPC server running with impersonation. See *Impersonation* under z/OS Batch | z/OS CICS | z/OS IMS | z/VSE CICS.