Protecting Natural RPC Servers and Services

This section describes the various aspects of Natural remote procedure call protection; it covers the following topics:

- RPC Service Requests
- RPC Server Settings in Natural
- RPC Server Settings in Natural Security
- Validation of an RPC Service Request
- Security Profiles for Natural RPC Servers
- Components of an RPC Server Profile
- Creating and Maintaining RPC Server Profiles
- IAF Support
- Other RPC-Related Features

For general information about Natural remote procedure calls, please refer to the *Natural Remote Procedure Call* documentation.

RPC Service Requests

In a client/server environment, you can use Natural Security to protect the use of Natural remote procedure calls. You can protect Natural RPC servers as well as the way in which Natural RPC service requests issued by clients are handled.

An RPC service request is a request from a client to a Natural RPC server for a Natural subprogram to be invoked which is located in a library on the server.

When a remote `CALLNAT` is executed, and the Natural RPC Logon Option is set on the client, the following data are passed to the Natural RPC server for validation:

- the name of the subprogram to be invoked;
- the ID of the library on the server which contains the subprogram to be invoked;
- the Natural RPC user ID and password (that is, the Natural user ID and password supplied with the Natural RPC service request);
- the EntireX user ID (validation depends on Logon Option; see below).

See also the section *Using Security* in the *Natural Remote Procedure Call* documentation.

RPC Server Settings in Natural

The following Natural profile parameters on a Natural RPC server should be reviewed if the server is to be protected by Natural Security:

Profile Parameter	Explanation
RPC	The settings for a Natural session which is started as a Natural RPC server are determined by the Natural profile parameter RPC. For a server to be protected by Natural Security, two subparameters of the RPC profile parameter are of particular relevance: SRVNAME and LOGONRQ. SRVNAME specifies the name of the server. This is the name which has to be used as the ID for a corresponding security profile. LOGONRQ determines whether the server is to accept only secured service requests or both public and secured service requests: ● A public request is a service request whose Natural RPC user ID and password are *not* validated; instead, the user ID which was used to start the server session (as contained in the Natural system variable *USER) will be used for the service request. ● A secured request is s service request whose Natural RPC user ID and password are validated. For a server to be protected by Natural Security so that only secured requests are accepted, set the LOGONRQ subparameter to "ON".
FSEC	With the profile parameter FSEC, you determine the FSEC system file to be associated with the Natural RPC server.
ETID	If you start the server session and specify an actual value with the profile parameter ETID, all service requests to the server will use the same specified ETID. If you start the server session with the profile parameter ETID=’ ’ (blank), no ETID can be supplied by Natural Security. If you start the server session with the profile parameter ETID=OFF, the ETIDs to be used by the service requests will be determined by the setting of the "Time-Stamp-Related ETID" in the security profile of the RPC server (see Components of an RPC Server Profile below). By setting this option to "Y", you can ensure an ETID handling, with appropriate database open/close processing, which allows you to uniquely identify each service request’s database transactions. If you start a server with replicas, the ETID parameter must be set to OFF or ’ ’ (blank).

Profile Parameter	Explanation
AUTO	The profile parameter AUTO (automatic logon) is only evaluated when the server session is started. For subsequent service requests to the running server, the AUTO parameter is ignored. If you start the server session with AUTO=OFF, you should assign a library via the profile parameter STACK=(LOGON *library-ID* ,...)

RPC Server Settings in Natural Security

Generally, the Natural Security user profiles and library profiles on the FSEC system file assigned to the Natural RPC server session determine the access rights to the requested library on the server.

Specifically for the protection of Natural RPC servers, Natural Security provides the following options:

- In the security profile of a library, you can set various options which apply when the library is accessed via a Natural RPC service request. These options are described under *Natural RPC Restrictions* in the section *Library Maintenance*.
- You can define security profiles for Natural RPC servers, as described below in the section *Security Profiles for Natural RPC Servers*.
- In the Library and User Preset Values section of Administrator Services, you can set various "Natural RPC Server Session Options", which control the logon to libraries via Natural RPC service requests.

Validation of an RPC Service Request

This section covers the following topics:

- Supported RPC Server Situations
- Security Data to Be Supplied by the Client
- Integrated Authentication Framework (IAF)
- Impersonation
- Validation on the Natural RPC Server
- Logon Mode
- Summary of Checks Based on Settings in Security Profiles

Supported RPC Server Situations

The following situations are supported by Natural Security:

- Natural RPC server protected by Natural Security only: The Natural RPC user ID is validated.

- Natural RPC server protected by Natural Security and EntireX Security: The Natural RPC user ID and the EntireX user ID are validated.
- Natural RPC server protected by Natural Security and EntireX Security, and using the Integrated Authentication Framework (IAF): The IAF token is validated (see below).

Security Data to Be Supplied by the Client

Natural Clients

Security data are supplied by the Natural client if the Natural RPC Logon Option is set. In this case the following applies:

- The Natural RPC user ID and password to be used for the service request have to be specified via the Natural application programming interface USR1071 (contained in the library SYSEXT). To ensure that this user ID and password are available when needed, executing USR1071 should be one of the first tasks performed by an application on the client. If USR1071 is not executed and the client runs under Natural Security, the user ID and password from the Natural Security logon on the client are used instead.

  If the Impersonation option is set to "A" in the RPC server security profile and the server has been started with ETID=OFF, the user ID on the client is specified via the Natural application programming interface USR4371 (contained in the library SYSEXT). In addition, USR4371 can be used to set the ETID for the service request.
- The EntireX user ID is supplied via the Natural application programming interface USR2071.
- The library ID to be used for the service request has to be specified via the Natural application programming interface USR4008 (contained in the library SYSEXT). If USR4008 is not executed, the ID of the client library in which the `CALLNAT` statement was executed is used instead.

Note:
If the Natural RPC passwords used for a service request may contain special characters, make sure that the Natural character translation tables NTTABA1 and NTTABA2 on the Natural RPC server have been adjusted accordingly.

Non-Natural Clients

Please refer to the client’s remote procedure call documentation for information on how to supply the required security data with an RPC service request issued by a non-Natural client to a

- Natural RPC server protected by Natural Security;
- Natural RPC server protected by Natural Security and EntireX Security;
- Natural RPC server protected by Natural Security and EntireX Security, and using the Integrated Authentication Framework (IAF).

Integrated Authentication Framework (IAF)

If a Natural RPC server is embedded in the token-based infrastructure provided by the Integrated Authentication Framework (IAF), the validation of the token which is attached to a service request passed to the Natural RPC server is performed by EntireX Security. Instead of the Natural RPC user ID and password, the IAF token - which contains the EntireX user ID - is validated during the logon to the Natural RPC server. The EntireX user ID and password are verified by EntireX Security.

Natural Security receives a successfully verified EntireX user ID. Natural Security then also uses this EntireX user ID as the Natural RPC user ID (replacing the Natural RPC user ID supplied by the client as described above). This ensures that both IDs are identical. After this point, this user ID used is considered a "trusted" Natural RPC user ID by the Natural RPC server, and is used accordingly for subsequent security checks and access authorizations.

For further information, see the section *IAF Support* below.

For general information on IAF, see *Integrated Authentication Framework* in the EntireX Communicator documentation. See also the section *Using the Integrated Authentication Framework* in the *Natural Remote Procedure Call* documentation.

Impersonation

For user authentication on the Natural RPC server, two modes are possible:

- validation with impersonation,
- validation without impersonation.

Impersonation assumes that access to the operating system on which a Natural RPC server is running is controlled by an SAF-compliant external security system. User authentication (verification of the Natural RPC user ID and - optionally - the password) is performed by this external security system. Impersonation means that after the authentication has been successful and the user’s identity is established, any subsequent authorization checks will be performed based on this identity. This includes authorization checks for access to external resources (for example, databases or work files).

Impersonation is only possible if the Natural RPC server runs under the operating system z/OS in batch mode. Impersonation can be used if an SAF-compliant external security system is used, and user authentication is to be performed by this external security system.

Impersonation is activated by the "Impersonation" setting in the security profile of the Natural RPC server (see *Components of an RPC Server Profile* below).

Validation on the Natural RPC Server

Validation Without Impersonation

If impersonation is not active for the Natural RPC server, Natural Security will perform a logon to the requested library, using the Natural RPC user ID. The logon is performed according to the Natural Security logon rules and the security settings defined on the FSEC system file associated with the server.

- **With IAF:**
  If the Natural RPC server is embedded in the Integrated Authentication Framework (IAF), the password has been verified by EntireX, and the EntireX user ID is considered a "trusted" user ID after that point. Natural Security will replace the Natural RPC user ID with this EntireX user ID. No further password verification will be performed for this user ID.

- **Without IAF:**
  One check performed during the logon is based on the evaluation of the Natural RPC Restrictions > Logon Option in the security profile of the requested library. This option determines whether only the Natural RPC user ID or both the user ID and the password are to be verified by the Natural Security logon procedure:

  - If the Logon Option is set to "N" or "E", both the user ID and the password are verified.

  - If the Logon Option is set to "A" or "S", only the user ID is verified - assuming that the password has already been verified (similiar to the Natural profile parameter AUTO=ON).

  - In addition, if the Logon Option is set to "E" or "S", Natural Security checks if the Natural RPC user ID is identical to the EntireX user ID. If both IDs are not identical, the service request will be rejected.

After a successful logon, the requested subprogram will be executed.

If the processing of the service request includes an access to an external resource (for example, a database or work file), the external user ID which was used to start the Natural RPC server will be used to check the authorization for such an access.

Validation With Impersonation

Impersonation is only possible if the Natural RPC server runs under the operating system z/OS in batch mode. Impersonation can be used if an SAF-compliant external security system is used, and user authentication is to be performed by this external security system.

- **With IAF:**
  If the Natural RPC server is embedded in the Integrated Authentication Framework (IAF), the Natural server front-end passes the EntireX user ID, which in this case is identical to the Natural RPC user ID, to the external security system for verification.

- **Without IAF:**
  If impersonation is active for the Natural RPC server, the Natural server front-end passes the Natural RPC user ID and password (or the user ID only) to the external security system for verification.

After a successful user authentication by the external security system, Natural Security will perform a logon to the requested library. For this logon, Natural Security uses the Natural RPC user ID, but will not perform any password verification for this user. The logon is performed according to the Natural Security logon rules and the security settings defined on the FSEC system file associated with the server.

One check performed during the logon is based on the evaluation of the Natural RPC Restrictions > Logon Option in the security profile of the requested library: If the Logon Option is set to "E" or "S", Natural Security checks if the Natural RPC user ID is identical to the EntireX user ID. If both IDs are not identical, the RPC service request will be rejected.

After a successful logon, the requested subprogram will be executed.

If the processing of the service request includes an access to an external resource (for example, a database or work file), the Natural RPC user ID will be used to check the authorization for such an access.

Logon Mode

If you use a Natural RPC server which provides services performed by subprograms contained in a single library, you can use the Logon Mode option in the security profile of the Natural RPC server to improve performance. This reduces the number of database accesses to the Natural Security system file FSEC.

The library on the server is set at the start of the server session, and will remain unchanged until the end of the server session. Service requests for any other library will be rejected. If the library is unprotected (People-protected = N), the user's authorization to access the library is not checked. If the library is protected (People-protected=Y), the user's authorization to access the library is checked. After a successful check, the user's conditions of use of the library are determined by the library profile. Even if a special link exists between the user and the library, any settings in the special link profile will be ignored.

Note:
When you set Logon Mode to "S" to improve performance, please be aware that other Natural Security settings also influence performance, in particular the "Logon recorded" option in user and library profiles. Morever, the performance of ETID-triggered handling of database transactions cannot be optimized.

Summary of Checks Based on Settings in Security Profiles

This section summarizes the checks which are performed by Natural Security depending on settings in security profiles when a service request is issued to a Natural RPC server. The following steps are performed:

1. If an IAF server is used (RPC server profile > IAF Support), token validation is performed via this IAF server (see the section *IAF Support* below).
2. User authentication is performed (see the section *Validation on the Server* above).
3. RPC server profile > the Logon Mode option is evaluated at the start of the Natural RPC server session (see the section *Logon Mode* above).
4. Library profile > General Options > the People-protected option is evaluated.
5. If no IAF server is used: Library profile > Natural RPC Restrictions > the Logon Option is evaluated (see the section *Validation on the Server* above): Depending on its setting, it is checked whether the Natural RPC user ID is identical to the EntireX user ID.

Security Profiles for Natural RPC Servers

Default Profile

The installation procedure of Natural Security automatically creates a default security profile with the server ID "*". This profile applies to all Natural RPC servers for which no individual security profiles are defined. You can change the settings in this default profile to suit your requirements.

Note:
Should there be no default RPC server profile "*" in your FSEC system file (this may be the case because the file was not available at the installation), execute the program NSCRPCAC in the library SYSSEC. This program creates the default server profile.

Asterisk Notation for Server IDs

If you do not wish to define a security profile for every single server, you can use asterisk notation for the server ID: If you create a server security profile an choose as server ID a character string followed by an asterisk (*), the profile will apply to all servers whose IDs begin with that character string. For an individual server within such a range, you may still define an individual security profile.

For example, if you defined a server security profile with the ID "A*", it would apply to all servers whose IDs begin with "A" (such a "ARPC1", "AA01", "ABC", "ADE" etc.). A profile with the ID "ABC*" would in turn apply to, for example, "ABCA", "ABCXYZ" etc.

Server Profile Components and Functions

The components of server security profiles and the functions used to create and maintain them are described below.

Some Natural Security functions use the code "RP" to represent the object type "Natural RPC servers".

Components of an RPC Server Profile

The following type of screen is the primary profile screen which appears when you invoke one of the functions Add, Copy, Modify, Display for the security profile of a Natural RPC server:

```
11:55:00                    *** NATURAL SECURITY ***                 2009-07-31
                           - Modify Nat. RPC Server -

                                              Modified .. 2009-07-31 by SAG

Nat. RPC Server ... RPCS01


--------------- Options -------------
Impersonation ............ (N,Y,A): Y
Lock User ................ (N,X,*): X
Time-Stamp-Related ETID .... (N,Y): Y
Logon Mode ................. (N,S): S
IAF Support ............. .. (N,Y): N







Additional Options ... N


Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10--PF11--PF12---
      Help  PrevM Exit  AddOp       Flip              IAF               Canc
```

The individual items you may define as part of a Natural RPC server's security profile are explained below.

Field	Explanation	
Impersonation	Impersonation is only relevant if an SAF-compliant external security system is used for user authentication. Impersonation is described above under *Validation of an RPC Service Request*. This option activates impersonation for the server:	
	N	Impersonation is not active.
	Y	Impersonation is active - with verification of the user ID and the password.
	A	Impersonation is active - with verification of the user ID, but not the password.
	Impersonation is only possible if the server runs under the z/OS operating system in batch mode. If it does not, the setting of this option will be ignored.	
Lock User	This option only applies to libraries in whose security profiles the Lock User option (in the *Natural RPC Restrictions* section of the library profile) is set to "*". For these libraries, it controls the locking of users when they attempt to access these libraries on the server via Natural RPC service calls:	
	N	The Lock User feature is not active.
	X	The Lock User feature is active for access attempts to libraries on the server via Natural RPC service calls. Once a user has reached the maximum number of logon attempts without supplying the correct password, he/she will be locked, that is, the user ID will be made "invalid". Natural Security "remembers" unsuccessful attempts across sessions: The error counters for the client user IDs which were tried out unsuccessfully are kept for access attempts in subsequent sessions, thus reducing the number of subsequent attempts with these IDs. The error counter for a user ID is only reset after a successful logon.
	*	The value of the "Lock user option" in the *Library And User Preset Values* of Administrator Services determines whether or not the Lock User feature is active for access attempts to libraries via Natural RPC service calls.
	For details on the Lock User feature, see also the *Lock User Option* in the General Options section of *Administrator Services*.	

Field	Explanation	
Time-Stamp-Related ETID	This option only applies to secured service requests passed from Natural clients to the Natural RPC server. It determines which ETIDs are to be used for these clients during the server session:	
	N	The "Default ETID" as defined in the user security profile of the Natural client determines the ETID to be used.
	Y	A time-stamp-related ETID will be generated for every service request that accesses the Natural RPC server under the control of Natural Security. The ETID is generated when the server is accessed, and will remain in effect until the service request has been processed.
	*	The setting of the ETID option in the *Library And User Preset Values*, which applies to the user security profile, will determine the ETID to be used.
	If this option is set to "Y" or "*", it is recommended that the RPC server session be started with the Natural profile parameter ETID=OFF. For public service requests, this option has no effect; for them, the ETID of the Natural RPC server, as established at the start of the server session, is used. For information on time-stamp-related ETIDs, see also ETID under *Library And User Preset Values* in the *Administrator Services* section.	
Logon Mode	This option can be used if only one library on the Natural RPC server is accessed:	
	N	No special logon mode applies.
	S	Static Mode applies: The library on the Natural RPC server is set at the start of the server session. It will remain unchanged until the end of the server session. The server will only process service requests for this one library. Any service request with a different library ID will be rejected. If this option is set, the conditions of use of the library are determined by the library profile. Even if a special link exists between the user and the library, any special link profile will be ignored.
	Provided that the Natural RPC server provides services performed by subprograms contained in a single library, you can use this option to improve performance. See also *Validation of an RPC Service Request* above.	

Field	Explanation	
IAF Support	This option is used to activate the support of the Integrated Authentication Framework (IAF) for the server:	
	N	IAF support is not active.
	Y	IAF support is active: The RPC server will use an IAF server for token validation. When you set this option to "Y", you will be prompted to select the IAF server to be used. If only one IAF server is defined to Natural Security or one of the IAF servers is defined as default server, this server will be used without your being prompted. The name of the IAF server assigned is displayed. To change the assignment, you press PF9 to select another IAF server.
	See the section *IAF Support* below for further information.	

Additional Options

If you either mark the field "Additional Options" with "Y" or press PF4, a window will be displayed from which you can select the following options:

- Maintenance Information
- Security Notes
- Owners

The options for which something has already been specified or defined are marked with a plus sign (+).

You can select one or more items from the window by marking them with any character. For each item selected, an additional window will be displayed:

Additional Option	Explanation
Maintenance Information (display only)	In this window, the following information is displayed: • the date and time when the security profile was created, the ID of the ADMINISTRATOR who created it, and (if applicable) the IDs of the co-owners who countersigned for the creation; • the date and time when the security profile was last modified, the ID of the ADMINISTRATOR who made the last modification, and (if applicable) the IDs of the co-owners who countersigned for the modification.
Security Notes	In this window, you may enter your notes on the security profile.
Owners	In this window, you may enter up to eight IDs of ADMINISTRATORs. Only the ADMINISTRATORs specified here will be allowed to maintain this server security profile. If no owner is specified, any user of type ADMINISTRATOR may maintain the security profile. For each owner, the number of co-owners whose countersignatures will be required for maintenance permission may optionally be specified in the field after the ID. For information on owners and co-owners, see the section *Countersignatures*.

Creating and Maintaining RPC Server Profiles

This section describes the functions used to create and maintain security profiles for Natural RPC servers. It covers the following topics:

- Invoking Maintenance for Natural RPC Servers
- Adding a New Server Profile
- Selecting Existing Server Profiles for Processing
- Copying a Server Profile
- Modifying a Server Profile
- Renaming a Server Profile
- Deleting a Server Profile
- Displaying a Server Profile

Invoking Maintenance for Natural RPC Servers

On the Main Menu, enter code "M" for "Maintenance". A window will be displayed.

In the window, mark object type "Natural RPC Server" with a character or with the cursor. The Natural RPC Server Maintenance selection list will be displayed.

From this selection list, you invoke all Natural RPC server maintenance functions as described below.

Adding a New Server Profile

To define a Natural RPC server to Natural Security, you create a security profile for it.

In the command line of the Natural RPC Server Maintenance selection list, enter the command `ADD` .

A window will be displayed. In this window, enter an *ID* for the server. This ID corresponds to the server name as specified with the Natural profile parameter RPC (see RPC Server Settings in Natural above), and must conform to the naming conventions for Natural RPC servers. Asterisk notation for the server ID is possible, as described under *Security Profiles for Natural RPC Servers* above.

After you have entered a valid ID, the Add Natural RPC Server screen will be displayed.

The individual items you may define on this screen and any additional windows that may be part of a server security profile are described under *Components of an RPC Server Profile* above.

When you add a new server profile, the owners specified in your own user security profile will automatically be copied into the server security profile you are creating.

Selecting Existing Server Profiles for Processing

When you invoke Natural RPC Server Maintenance, a list of all Natural RPC server profiles that have been defined to Natural Security will be displayed.

If you do not want a list of all existing profiles, but wish only certain servers to be listed, you may use the Start Value option as described in the section *Finding Your Way In Natural Security*.

On the Main Menu, enter code "M" for "Maintenance". A window will be displayed. In the window, mark object type "Natural RPC Server" with a character or with the cursor (and, if desired, enter a start value). The Natural RPC Server Maintenance selection list will be displayed:

```
14:49:01                    *** NATURAL SECURITY ***                 2009-07-31
                         - Nat. RPC Server Maintenance -

 Co Nat. RPC Server                                          Message
 __ _____________________________________________________ _____________________
 __ *
 __ ASERV
 __ RPC*
 __ RPCABC01
 __ RPCABC02
 __ RPSRV2112









Command ===>
Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10--PF11--PF12---
Help        Exit              Flip  -     +                      Canc
```

For each server, the server ID is displayed.

The list can be scrolled as described in the section *Finding Your Way In Natural Security*.

Selecting a Function

The following maintenance functions are available for Natural RPC server profiles (possible code abbreviations are underlined):

Code	Function
CO	Copy server profile
MO	Modify server profile
RE	Rename server profile
DE	Delete server profile
DI	Display server profile

To invoke a function for a server profile, mark the server with the appropriate function code in column "Co".

You may select various server profiles for various functions at the same time; that is, you can mark several servers on the screen with a function code. For each server marked, the appropriate processing screen will be displayed. You may then perform the selected functions for one server profile after another.

Copying a Server Profile

The Copy Server Profile function is used to define a new Natural RPC server to Natural Security by creating a security profile which is identical to an already existing Natural RPC server security profile.

What is Copied?

All components of the existing security profile will be copied into the new security profile - except the owners (these will be copied from your own user security profile into the new server security profile you are creating).

Any *links* from users to the existing server will *not* be copied.

How to Copy

On the Maintenance selection list, mark the server whose security profile you wish to duplicate with function code "CO".

A window will be displayed. In the window, enter the ID of the new server. The ID corresponds to the server name as specified with the Natural profile parameter RPC (see RPC Server Settings in Natural above), and must conform to the naming conventions for Natural RPC servers. Asterisk notation for the server ID is possible, as described under *Security Profiles for Natural RPC Servers* above.

After you have entered a valid ID, the new security profile will be displayed.

The individual components of the security profile you may define or modify are described under *Components of an RPC Server Profile* above.

Modifying a Server Profile

The Modify Server Profile function is used to change an existing Natural RPC server security profile.

On the Natural RPC Server Maintenance selection list, you mark the server whose security profile you wish to change with function code "MO". The security profile of the selected server will be displayed.

The individual components of the security profile you may define or modify are described under *Components of an RPC Server Profile* above.

Renaming a Server Profile

The Rename function allows you to change the server ID of an existing Natural RPC server security profile.

On the Natural RPC Server Maintenance selection list, you mark the server whose ID you wish to change with function code "RE". A window will be displayed in which you can enter a new ID for the server profile.

The ID corresponds to the server name as specified with the Natural profile parameter RPC (see RPC Server Settings in Natural above), and must conform to the naming conventions for Natural RPC servers. Asterisk notation for the server ID is possible, as described under *Security Profiles for Natural RPC Servers* above.

Deleting a Server Profile

The Delete Server Profile function is used to delete an existing Natural RPC server security profile.

On the Natural RPC Server Maintenance selection list, you mark the server whose profile you wish to delete with function code "DE". A window will be displayed.

- If you have invoked the Delete function and should then decide against deleting the given server security profile, leave the Delete Server Profile window by pressing ENTER without having typed in anything.
- If you wish to delete the given server security profile, enter the server ID in the window to confirm the deletion.

If you mark more than one server profile with "DE", a window will appear in which you are asked whether you wish to confirm the deletion of each server security profile with entering the server ID, or whether all server profiles selected for deletion are to be deleted without this individual confirmation. Be careful not to delete a server profile accidentally.

Displaying a Server Profile

The Display Server Profile function is used to display an existing Natural RPC server security profile.

On the Natural RPC Server Maintenance selection list, you mark the server whose security profile you wish to view with function code "DI". The security profile of the selected server will be displayed.

The individual components of the security profile are explained under *Components of an RPC Server Profile* above.

IAF Support

This section describes the support of the Integrated Authentication Framework (IAF), which is a component of EntireX. It covers the following topics:

- Using IAF Servers
- Creating and Maintaining IAF Server Security Profiles
- Components of an IAF Server Security Profile

For details of IAF, see *Introduction to the Integrated Authentication Framework* in the EntireX Communicator documentation. See also the section *Using the Integrated Authentication Framework* in the *Natural Remote Procedure Call* documentation.

Using IAF Servers

If IAF is installed, a Natural RPC server can use an IAF server for token validation.

An IAF server which to be used has to be defined to Natural Security, that is, a security profile has to be created for it, as described below under *Creating and Maintaining IAF Server Security Profiles*.

In the security profile of the Natural RPC server, you activate IAF support by setting the option IAF Support to "Y". When you do so, you will be prompted to select the IAF server to be used by the RPC server. If only one IAF server is defined to Natural Security or one of the IAF servers is defined as default server, this one will be used without your being prompted.

Creating and Maintaining IAF Server Security Profiles

If you press PF10 on the Administrator Services > General Options screen, a list of all IAF servers for which security profiles have been defined will be displayed. From the list, you can select an existing IAF server profile for modification or deletion, or create a new security profile for an IAF server.

To create a new IAF server security profile, you press PF4 on the IAF server selection list. The Add IAF Server screen will be displayed. The items you can define on this screen as part of an IAF server security profile are described below under *Components of an IAF Server Security Profile*.

If no IAF server profiles have been defined yet, pressing PF10 on the General Options screen will invoke the Add IAF Server screen directly for you to define the first IAF server profile.

If only one IAF server profile has been defined, pressing PF10 on the General Options screen will invoke this profile directly for modification.

The following functions are available (possible code abbreviations are underlined) on the IAF Server Maintenance selection list:

Code	Function
MO	Modify IAF server profile.
DE	Delete IAF server profile.

To invoke a function for an IAF server profile, mark the daemon with the appropriate function code in column "Co".

You may select various profiles for various functions at the same time; that is, you can mark several IAF servers on the screen with a function code. For each server marked, the appropriate processing screen will be displayed. You can then perform the selected functions for one profile after another.

To reset all fields in an IAF server security profile, you press PF9 on the security profile screen.

Components of an IAF Server Security Profile

The individual items you can define as part of an IAF server security profile are described below.

The items correspond to appropriate settings in EntireX, which are described in detail in the EntireX Communicator documentation.

IAF Server Identification

Field	Explanation
NSC ID of IAF server	In this field, you specify the Natural Security ID of the IAF server. This is the ID by which the IAF server is assigned to a Natural RPC server in the RPC server profile (see IAF Support under Components of an RPC Server Profile above).
Default	If you mark this field with "X", this IAF server will be used by all Natural RPC servers, unless you change the IAF server assignment in individual Natural RPC server profiles.
Description	In this field, you can enter a descriptive name for the IAF server.

IAF Configuration

Field	Explanation
Operating system	In this field, you specify the operating system of the IAF server: 1 = z/OS, 2 = UNIX/Windows.
Transport method	In this field, you specify the transport method of the IAF server: 1 = SSL, 2 = SVC.
Host name	In this field, you specify the host name of the IAF server. For SSL, this is the IP address or the DNS name. For SVC, this is the NODE specified in the attribute file of the IAF server.
Port/SVC number	If the server type is SSL, you specify the port number. If the server type is SVC, you specify the SVC number.
Verify server (Y/N)	If this field is set to "Y", the subject name in the certificate of the IAF server must match the host name of the IAF server.

SSL Parameters for z/OS (Operating system = 1)

Field	Explanation
Trust store	In this field, you specify the location of the store containing certificates of trusted Certificate Authorities (CA certificates). You specify the RACF keyring which contains the CA certificate as follows: *user-ID/keyring-name*. If you omit the *user-ID*, the keyring will be associated with RACF user ID under which the Natural RPC server is started.
Key label	In this field, you specify the label of the user certificate in the the RACF keyring which is used to authenticate the RACF user ID of the Natural RPC server to the IAF server. This value has to be specified only if VERIFY-CLIENT=YES is specified in the attribute file of the IAF server.

SSL Parameters for UNIX and Windows (Operating system = 2)

Field	Explanation
Trust store	In this field, you specify the file name location of the CA certificate store. Example: C:/Certs/ExxCACert.pem
Key store	In this field, you specify the SSL certificate; it may contain the private key. Example: MyAppCert.pem
Key file	In this field, you specify the file which contains the EntireX Broker's private key, if it is not contained in the key store. Example: MyAppKey.pem
Key password	In this field, you specify the password which is used to protect the private key and to unlock the key file (e.g. MyAppKey.pem).

Other RPC-Related Features

User Exit LOGONEX4

The Natural Security user exit LOGONEX4 is invoked by the Natural Security RPC logon program after a successful logon of a Natural RPC client to a Natural RPC server. For details, see *RPC-Related User Exit* in the section *User Exits*.

Password Change via RPC Service Request - User Exit USR2074

The Natural user exit USR2074, contained in the library SYSEXT, allows you to change the user password via a Natural RPC service request.