



# natural

Natural SAF Security

Version 4.1.2

Natural SAF Security

 **SOFTWARE AG**

This document applies to Natural SAF Security Version 4.1.2 and to all subsequent releases.

Specifications contained herein are subject to change and these changes will be reported in subsequent release notes or new editions.

© Copyright Software AG 1979 - 2003.  
All rights reserved.

The name Software AG and/or all Software AG product names are either trademarks or registered trademarks of Software AG. Other company and product names mentioned herein may be trademarks of their respective owners.

# Table of Contents

<b>Natural SAF Security - Overview</b>	1
Natural SAF Security - Overview	1
<b>Introducing Natural SAF Security</b>	2
Introducing Natural SAF Security	2
What is Natural SAF Security?	2
Configuring Your Security Environment - an Example	2
User Security	3
Environment Security	4
Environment-Specific Library Security	4
Natural Security Related Considerations	5
Library SYSSEC	5
Automatic Logon	5
PROFILE Command	5
Transition Period Logon	5
Utilities	5
<b>Installing and Activating Natural SAF Security</b>	6
Installing and Activating Natural SAF Security	6
Installation Prerequisites	6
Tape Contents	6
Installation Procedure	6
Step 1: Load Modules	6
Step 2: Adjust Natural Parameter Module	7
Step 3: Relink Natural	7
Step 4: Install the SAF Server	7
Activation	8
Activate Natural SAF Security Itself	8
Define SYSSAFOS Utility Profile	9
Start SAF Server	9
Check Connections and Data Transfer	9
<b>Defining Resources in the External Security System and Activating Them</b>	10
Defining Resources in the External Security System and Activating Them	10
Users	10
External Security System Definitions	10
Natural SAF Security Definitions	10
Environments	10
SAF Server Definitions	10
External Security System Definitions	10
Natural SAF Security Definitions	11
Libraries	11
Environment-Independent Access to a Library	11
Access to a Library in Specific Environments	12
Use of System Commands in a Library	12
Modifications on FUSER System File	12
RPC Services	12
Environment-Independent Use of an RPC Service	13
Use of an RPC Service in Specific Environments	13
User-Defined Resources	14
Environment-Independent Use of a User-Defined Resource	14
Use of a User-Defined Resource in Specific Environments	14
Overview of Resource-Class Definitions	15
Translation and Effects of Access Levels	15
Examples of Resource Definitions	16
Example of Resource Definitions in RACF	16

Example of Resource Definitions in CA-ACF2 . . . . .	17
Example of Resource Definitions in CA Top Secret . . . . .	17
<b>Administrator Services . . . . .</b>	<b>19</b>
Administrator Services . . . . .	19
NSF Options . . . . .	19
Security System . . . . .	20
User Options . . . . .	21
Environment Options . . . . .	22
Library Options . . . . .	23
RPC Options . . . . .	23
User-Resource Options . . . . .	24
Environment Profiles . . . . .	24
SAF Online Services . . . . .	24
<b>Application Interfaces . . . . .</b>	<b>26</b>
Application Interfaces . . . . .	26
Overview of Application Interfaces . . . . .	26
Application Interfaces for User and Password Authentication . . . . .	26
NSFNPAS . . . . .	26
NSFNPASZ . . . . .	27
NSFNPAX . . . . .	27
Application Interface for Checking Resource Access to Dedicated API Class . . . . .	28
Application Interface for Maintaining Resource Profiles . . . . .	28
Application Interfaces for Checking Access Rights to a Resource . . . . .	29
Application Interface for Obtaining Information from the SAF Server . . . . .	29
Natural Security Application Interfaces . . . . .	30

# Natural SAF Security - Overview

This documentation describes all functions of Natural SAF Security. It covers the topics listed below.

Natural SAF Security is used in conjunction with Natural Security and with an SAF-compliant external security system (RACF, CA-ACF2, or CA Top Secret).

The reader is assumed to be familiar with and have a good general understanding of Natural and Natural Security. In particular, the reader is assumed to be familiar with the Natural Security documentation.

If you are not familiar with the external security system yourself, you should get in touch with the security administrator who is in charge of that system, as the use of Natural SAF Security requires certain conditions to be met by that system.

- |  |   |
|--|---|
| ● Introducing Natural SAF Security                                       | Basic concepts of Natural SAF Security.   |
| ● Installing and Activating Natural SAF Security                         | How to install and activate Natural SAF Security.   |
| ● Defining Resources in the External Security System and Activating Them | Considerations concerning the external security system used in conjunction with Natural SAF Security. |
| ● Administrator Services   | Natural SAF Security administration functions in Natural Security.                                    |
| ● Application Interfaces   | Information on the available application interfaces.  |

Natural SAF Security uses a SAF server, which is described in the SAF Security Kernel documentation.

For information on changes, enhancements and new features provided with this version, see the Natural Release Notes.

# Introducing Natural SAF Security

This section provides an overview of Natural SAF Security. It covers the following topics:

- What is Natural SAF Security?
  - Configuring Your Security Environment - an Example
  - Natural Security Related Considerations
- 

## What is Natural SAF Security?

Natural SAF Security (NSF) is an add-on product to Natural Security. It allows you to control users' access to Natural based on user and resource definitions made in an external security system. With Natural SAF Security, you can thus protect your Natural sessions by combining security definitions made in Natural Security and security definitions made in the external security system.

This external security system must be an SAF-compliant security system. At present, Natural SAF Security supports the following external security systems:

- RACF,
- CA-ACF2,
- CA Top Secret.

When you use Natural SAF Security, you need not define users both in Natural Security and in an external security system; it is sufficient to define them in the external security system. In Natural Security, only user *groups* are defined. When Natural SAF Security is active and a user logs on to Natural, the user authorization checks will be done using the user ID and user password from the external security system. After the authorization, further security checks - particularly concerning the use of Natural libraries and utilities - will be based on the user *group* definitions in Natural Security. Although library protection via an external security system is possible, the Natural Security library security profiles provide more sophisticated and more adequate mechanisms for protecting Natural libraries.

In addition, access to Natural can be made environment-specific. A Natural environment is determined by the combination of the system files FNAT, FUSER, FDIC and FSEC. Natural environments can be defined in the external security system. By defining environments and controlling their accessibility, it is possible, for example, to fully separate the protection of a Natural development environment from that of a Natural production environment. At the same time, this avoids system-file mix-ups (for example, a test-environment FSEC file in conjunction with a production-environment FUSER file).

Also, instead of the end of transaction IDs (ETIDs) from Natural Security user profiles, Natural SAF Security provides various possibilities of generating unique ETIDs.

Moreover, Natural SAF Security allows you to protect user-defined resources which are defined in the external security system against unauthorized use.

## Configuring Your Security Environment - an Example

This section is an example of the usage of Natural SAF Security. It does not cover all aspects or possibilities offered by Natural SAF Security. In particular, it does not cover all Natural SAF Security options (NSF options). Instead, a few selected options are introduced to show you how you can set up your security environment step by step:

- user security,
- environment security,
- environment-specific library security.

Although the following explanations are based on certain assumptions, some of which may not apply to your security environment, this approach may be helpful to make yourself familiar with Natural SAF Security.

If you are not yet familiar with Natural SAF Security, it is recommended that you deal with the NSF options step by step as indicated in the explanations below, and only change those options mentioned below.

Generally, please bear in mind that before you set any NSF options, you have to make sure that the corresponding resources are defined in the external security system being used. For resource definitions, see the section Defining Resources in the External Security System and Activating Them.

## User Security

The desired security setup is assumed to be as follows:

- User security data are to be maintained not in both Natural Security and your external security system, but primarily in the external security system.
- For the logon to Natural, the user security data (user ID and password) as defined in the external system are to be used, and the user authentication is to be performed by the external security system according to the authentication rules defined in the external security system.
- Apart from the user authentication, the logon to Natural is to be performed by Natural Security according to the Natural Security logon rules.
- *Within* the Natural session, Natural Security controls what the user is allowed to do.

The necessary connection between the external security system and Natural Security is made by using user *groups* in both systems.

The above setup requires that:

- users and user groups are defined in the external security system,
- the user groups are also defined in Natural Security,
- a connection between the group definitions in the external security system and the group definitions in Natural Security is established.

Except for users with special tasks (for example, Natural Security administrators), you need not create security profiles for individual users in Natural Security, nor assign them to groups; it is sufficient that users are defined and assigned to groups in the external security system.

To establish the desired setup, you have to do the following:

In the external security system:

- Make sure that users and user groups are defined appropriately.

In Natural Security:

- Create a group security profile for every user group which is defined in the external security system. As ID for the security profile use the same ID by which the group is defined in the external security system. It is recommended that you specify a default library in the group security profile.
- In "Administrator Services > General Options > User Options" (third screen of General Options), set the following options:
  - Set "NSF \*GROUP" to "Y".
  - Set "NSC Group ID" to "Y".

## Environment Security

A Natural environment is determined by the combination of the system files FNAT, FUSER, FDIC and FSEC. When a user accesses a library, these are determined by the current values of the corresponding Natural profile parameters - with the following exception: If the Natural Security library profile of that library contains another FUSER value, this will overwrite the FUSER profile parameter.

Based on the user-security setup as described above, the desired security setup for Natural environments is assumed to be as follows:

- Access to Natural environments is to be controlled, so that not all users have access to all environments.

This setup requires that Natural environments are defined in the external security system. Access authorization to the environments will then be controlled according to the access rules defined in the external security system.

To establish the desired setup, you have to do the following:

- In the external security system: Define resource profiles for all Natural environments (system-file combinations) to be protected.
- In Natural Security: In "Administrator Services > General Options > Environment Options (fourth screen of General Options), set the option "Protect Environments" to "Y".

## Environment-Specific Library Security

Based on the user-security setup described above, the desired security setup for environment-specific library protection is assumed to be as follows:

- Library security data continue to be maintained in Natural Security.
- Access to Natural libraries is to be controlled by Natural Security, that is, access to libraries will be according to the Natural Security logon rules.
- In addition, access to a library is to be restricted to certain Natural environments (as determined by the combination of the system files FNAT, FUSER, FSEC and FDIC); for example, some users are to access a library only in a development environment, others only in a production environment.

The necessary connection between the external security system and Natural Security is made via one-character aliases. The environment-specific access authorization to a library is checked as follows: When a user attempts to access a library, the environment in which the library is located is determined by the current values of the Natural profile parameters FNAT, FDIC, FSEC and FUSER - with the FUSER value being overwritten by the one specified in the Natural Security library profile. For this environment, a Natural Security environment profile has to exist, in which a one-character alias is specified. For the combination of this alias and the library (*alias.library-ID*), a resource profile has to exist in the external security system. The access level defined in this resource profile determines whether the user is allowed to log on to the library in that environment.

To establish the desired setup, you have to do the following:

In the external security system:

- Make sure that the resource profiles for the Natural libraries are defined with the same IDs by which the libraries are defined in Natural Security.
- Define a resource profile for every environment-library combination (that is, *alias.library-ID*) to be protected.

In Natural Security:

- Define an environment profile for every Natural environment (system-file combination).
- In "Administrator Services > General Options > Library Options (fourth screen of General Options), set the following options:

- Set "Protect Libraries" to "Y".
- Set "with Environment" to "Y".

## Natural Security Related Considerations

The following Natural Security items should be considered when using Natural SAF Security.

### Library SYSSEC

The library SYSSEC can only be accessed by users who, in addition to being defined in the external security system, are defined as "Administrators" in Natural Security.

### Automatic Logon

If the Natural profile parameter AUTO=ON (Automatic Logon) is set, a user can only log on to Natural if a default library is defined for him/her. The default library can be specified in the Natural Security group security profile. See also the section Automatic Logon in the Natural Security documentation.

Natural SAF Security provides a user option "NSC Logon Priv. Library" by which it is possible that a user who logs on without specifying a library ID will be logged on to the library whose ID is the same as the current value of the Natural system variable \*USER value.

### PROFILE Command

When Natural SAF Security is active, the Natural system command PROFILE indicates whether the user and his/her group are defined in Natural Security:

- If neither the current user ID nor group ID are defined in Natural Security, the user type will be shown as "Ext. User".
- If the current user ID is not defined in Natural Security, but the current group ID is defined in Natural Security, the user type will be shown as "Ext. User/Grp".

### Transition Period Logon

If the Natural Security general option Transition Period Logon is set to "N", only unprotected libraries can be accessed via Natural SAF Security. Undefined libraries can only be accessed if Transition Period Logon is set to "Y".

### Utilities

For users for whom neither a user security profile nor a group security profile exists in Natural Security, the default utility profiles apply.

For users for whom no user security profile, but a group security profile exists, the use of utilities is controlled by the group-library-specific utility profiles and group-specific utility profiles associated with this group.

Natural SAF Security provides an additional utility: SAF Online Services (SYSSAFOS). To be able to access this utility, a utility security profile for SYSSAFOS has to be defined in Natural Security.

Utility profiles are described in the section Protecting Utilities of the Natural Security documentation.

# Installing and Activating Natural SAF Security

This section describes how to install and activate Natural SAF Security. It covers the following topics:

- Installation Prerequisites
  - Tape Contents
  - Installation Procedure
  - Activation
- 

## Installation Prerequisites

Natural SAF Security can only be installed if the following products have been installed:

- Natural Version 4.1.2 (or above),
- Natural Security Version 4.1.2 (or above),
- Adabas Version 7.4.2 (or above),
- Adabas Limited Libraries Version 7.4.2 (or above),
- an SAF-compliant security system.

## Tape Contents

The Natural SAF Security installation tape contains the following datasets (*nnn* in the dataset names denoting the version number):

Dataset	Contents
NSF <i>nnn</i> .ALLINPL	The Natural INPL dataset containing updates to Natural Security.
NSF <i>nnn</i> .MVSLOAD	The load library, containing the Natural SAF Security assembly module NATGWSAF.
NSF <i>nnn</i> .MVSJOBS	Example jobs for installing Natural SAF Security.

## Installation Procedure

This section describes step by step how to install Natural SAF Security.

### Step 1: Load Modules

(Job I005)

#### Note:

The INPL job will overwrite the Natural Security user exit LOGONEX1. If you have modified this user exit, please take care to secure your modified copy appropriately (by copying it into one of your own libraries) before you execute this job.

Load the Natural SAF Security modules using the Natural utility INPL (assigning dataset NSF*nnn*.ALLINPL to work file CMWKF01).

## Step 2: Adjust Natural Parameter Module

(Job I010)

Add the following parameter to your Natural parameter modules:

```
NSFSIZE=8
```

Then reassemble the parameter modules.

## Step 3: Relink Natural

(Job I060 from the Natural installation tape)

Relink your Natural nucleus to include the modified parameter module and Natural SAF Security modules:

```
INCLUDE SMALOAD (NATPARM)
INCLUDE NSFLOAD (NATGWSAF)
```

## Step 4: Install the SAF Server

The SAF server (SAF Security Kernel) is delivered with Adabas Limited Libraries.

Install and configure the SAF server and its associated Daemon as described in the SAF Security Kernel documentation.

In the configuration module of the SAF server, the following Natural SAF Security options may have to be set:

### Number of Cached Resource Checks

Natural SAF Security allows you to have resource checks cached. If you wish resource checks to be cached, you have to specify the number of successful resource checks to be cached for each resource class, using the following parameters of the configuration module:

Parameter	Default Value	Function
NANUSF	0	Number of cached environment checks.
NANUTC	0	Number of cached library checks.
NANUSV	0	Number of cached RPC-service checks.

### Alternate Resource Names

If you wish to change the default names for the resource classes, you have to change the following parameters of the configuration module:

Parameter	Default Value	Function
NACLSF	NSFSAG	Resource-class name for environments.
NACLTC	NTCSAG	Resource-class name for libraries.
NACLSV	NSVSAG	Resource-class name for RPC services.
NACLAP	NPGSAG	Resource-class name for user-defined resources.

After the above steps have been performed, the installation of Natural SAF Security is complete.

To be able to use Natural SAF Security, you have to activate it as described in the following section.

## Activation

The activation of Natural SAF Security comprises the following steps:

1. Activate Natural SAF Security Itself
2. Define SYSSAFOS Utility Profile
3. Start SAF Server
4. Check Connections and Data Transfer

### Activate Natural SAF Security Itself

Before you activate Natural SAF Security, you should define the necessary resources in the external security system, as described in the section Defining Resources in the External Security System and Activating Them. In particular, do not set any Natural SAF Security options other than the ones mentioned below, unless you have defined the corresponding resources in the external security system.

If you are not yet familiar with Natural SAF Security, it is recommended that you read the section Introducing Natural SAF Security before you activate it.

The activation of Natural SAF Security has to be performed within Natural Security. You have to meet the following prerequisites to be able to activate Natural SAF Security:

- You have to be defined as a user of type "Administrator" in Natural Security.
- You have to be linked to the library SYSSEC in Natural Security.

 To activate Natural SAF Security:

1. Invoke Natural and log on to the Natural Security library SYSSEC.
2. On the Natural Security Main Menu, select "Administrator Services". The Administrator Services Menu will be displayed.
3. Select "General options". The Set General Options screen will be displayed.
4. Press PF8 twice. The General Options 3 (NSF) screen will be displayed.
5. On this screen:
  - Set all four options listed under "Security System": Specify values for the fields "External Security System", "Server ID" and "Natural Security", and set the field "Protection Level" to "2". For details on these fields, see NSF Options. The setting of these four options activates Natural SAF Security.
  - Set the option "NSF \*USER-NAME", which is listed under "User Options", to "Y". This will be used by the check described below.
  - *Do not* change the values of any other fields on the screens General Options 3 (NSF) and General Options 4 (NSF)!

 For the activation of Natural SAF Security to take effect, end your Natural session.

The activation as described above only "switches on" Natural SAF Security as such, using default settings. The subsequent configuration of your security environment can then be performed gradually step by step as outlined in the section Introducing Natural SAF Security.

## Define SYSSAFOS Utility Profile

The load job performed in Step 1 of the installation procedure loads the utility library SYSSAFOS; this library contains the SAF Online Services. To be able to access this utility, you have to define a utility security profile for SYSSAFOS in Natural Security (as described in the section Protecting Utilities of the Natural Security documentation).

## Start SAF Server

Once Natural SAF Security has been activated, start the SAF server, as described in the SAF Security Kernel documentation.

If the SAF server is already running (which may be the case if it is being used by another product), restart it.

Access to Natural is now controlled by Natural SAF Security.

## Check Connections and Data Transfer

Log on to Natural (with Natural profile parameter AUTO=OFF), using the password which is defined for you in the external security system.

Within your Natural session, enter the system command PROFILE.

If the logon with that password has been successful, and the field User Name on the PROFILE screen shows the name by which you are defined in the external security system, this confirms that the connections between the external security system, the SAF server and Natural SAF Security are established, and that the data transfer from the external security system to Natural SAF Security works correctly.

# Defining Resources in the External Security System and Activating Them

This section describes which resources have to be defined in the external security system in conjunction with Natural SAF Security, and how they are activated. It covers the following topics:

- Users
- Environments
- Libraries
- RPC Services
- User-Defined Resources
- Overview of Resource-Class Definitions
- Translation and Effects of Access Levels
- Examples of Resource Definitions

## Note on terminology:

Some external security systems use the term "resource profile", others the term "rule". In this documentation the term "resource profile" is used.

Some external security systems use the term "resource class", others the term "resource type". In this documentation the term "resource class" is used.

---

## Users

### External Security System Definitions

The existing user definitions in the external security system can be used. No additional user-specific definitions have to be made in the external security system.

### Natural SAF Security Definitions

If the NSF user options "NSF \*GROUP" and "NSF \*USER-NAME" are set to "Y", the user's group and user name as defined in the external security system are passed to Natural SAF Security.

## Environments

### SAF Server Definitions

The resource-class name for Natural environments is defined with the macro parameter NACLSE in the configuration module of the SAF server (see Step 4 of the Natural SAF Security installation procedure). The default name is "NSFSAG".

### External Security System Definitions

A Natural environment is determined by the combination of the Natural system files FNAT, FDIC, FSEC and FUSER. For each system-file combination that is to be protected, a resource profile has to be defined in the external security system.

The identification of the resource profile must be a 40-digit number corresponding to the database ID / file number (DBID/FNR) combinations of the four system files. The database IDs and file numbers must be specified in the following sequence:

1. FNAT DBID and FNR,
2. FDIC DBID and FNR,
3. FSEC DBID and FNR,
4. FUSER DBID and FNR.

Each DBID and FNR must be specified as a 5-digit number (padded with leading zeros).

For example, the following environment:

```
FNAT=(00011,00035),  
FDIC=(00011,00033),  
FSEC=(00011,00034),  
FUSER=(00011,00032)
```

would have to be specified as follows:

```
0001100035000110003300011000340001100032
```

The access level specified in the resource profile determines whether a user has access to the environment. A user needs at least READ access to be able to access a Natural environment.

## Natural SAF Security Definitions

The NSF environment option "Protect Environments" determines if access to a Natural environment is to be controlled by Natural SAF Security. If this option is set to "Y", the access level defined for the environment in the external security system determines whether a user has access to it or not.

## Libraries

With Natural SAF Security, Natural libraries can be protected to control users' access to them. You can protect a Natural library:

- independently of the environment, or
- in specific environments.

## Environment-Independent Access to a Library

### SAF Server Definitions

The resource-class name for Natural libraries is defined with the macro parameter NACLTC in the configuration module of the SAF server (see Step 4 of the Natural SAF Security installation procedure). The default name is "NTCSAG".

### External Security System Definitions

If a Natural library is to be protected, a resource profile has to be defined for it in the external security system. The resource-profile name must correspond to the library ID and may be up to 8 characters long.

The access level specified in the resource profile is checked when a user logs on to a Natural library. A user needs at least READ access to be able to log on to a library.

## Natural SAF Security Definitions

The NSF library option "Protect Libraries" determines if access to Natural libraries is to be controlled by Natural SAF Security. If this option is set to "Y", the access level defined for a library in the external security system determines whether a user can log on to the library or not.

## Access to a Library in Specific Environments

### SAF Server Definitions

The resource-class name for Natural libraries is defined with the macro parameter NACLTC in the configuration module of the SAF server (see Step 4 of the Natural SAF Security installation procedure). The default name is "NTCSAG".

### External Security System Definitions

If a Natural library is to be protected in a specific Natural environment (Natural system-file combination), a resource profile for the environment-library combination has to be defined in the external security system. A Natural environment is determined by a one-character alias. The resource-profile name must consist of the alias and the library ID (up to 8 characters), separated by a period:

*a.library-ID*

### Natural Security Definitions

In Natural Security, you have to define an environment profile for the environment. In the environment profile, the alias to be used has to be specified.

### Natural SAF Security Definitions

The NSF library option "Protect Libraries" has to be set to "Y" to activate Natural SAF Security's library-access control.

The environment-specific library-access check is activated by setting the NSF library option "with Environment" to "Y". Access to the library is then only possible in environments to which the user has READ access.

## Use of System Commands in a Library

If the NSF library option "Disable Natural Commands" is set to "Y", the access level defined for the library (or library-environment combination) in the external security system also determines whether or not users may use Natural system commands within the library. A user needs at least CONTROL access to use system commands.

## Modifications on FUSER System File

If the NSF library option "Set FUSER Read-Only" is set to "Y", the access level defined for the library (or library-environment combination) in the external security system also determines whether or not a user may make modifications on the FUSER system file from within the library. A user needs at least ALTER access to make modifications on the FUSER file.

## RPC Services

With Natural SAF Security, Natural RPC services can be protected against unauthorized use. You can protect a Natural RPC service:

- independently of the environment, or
- in specific environments.

## Environment-Independent Use of an RPC Service

### SAF Server Definitions

The resource-class name for Natural RPC services is defined with the macro parameter NACL SV in the configuration module of the SAF server (see Step 4 of the Natural SAF Security installation procedure). The default name is "NSVSAG".

### External Security System Definitions

If a Natural RPC service is to be protected, a resource profile has to be defined for it in the external security system.

The resource-profile name must correspond to the library ID and subprogram name, each of which may be up to 8 characters long and which must be separated by a period:

*library-ID.subprogram-name*

The access level specified in the resource profile determines whether a user can use the service or not. A user needs at least READ access to be able to execute a Natural subprogram via RPC.

### Natural SAF Security Definitions

The NSF RPC option "Protect Services" determines if access to Natural RPC services is to be controlled by Natural SAF Security. If this option is set to "Y", the access level defined for the RPC service in the external security system determines whether a user can use the service or not.

## Use of an RPC Service in Specific Environments

### SAF Server Definitions

The resource-class name for Natural RPC services is defined with the macro parameter NACL SV in the configuration module of the SAF server (see Step 4 of the Natural SAF Security installation procedure). The default name is "NSVSAG".

### External Security System Definitions

If a Natural RPC service is to be protected in a specific Natural environment (Natural system-file combination), a resource profile has to be defined for the environment-service combination in the external security system. A Natural environment is determined by a one-character alias. The resource-profile name must consist of the alias, the library ID (up to 8 characters), and the subprogram name, separated from one another by periods:

*a.library-ID.subprogram-name*

### Natural Security Definitions

In Natural Security, you have to define an environment profile for the environment. In the environment profile, the alias to be used has to be specified.

## Natural SAF Security Definitions

The NSF RPC option "Protect Services" has to be set to "Y" to activate Natural SAF Security's service-access control.

The environment-specific service-access check is activated by setting the NSF RPC option "with Environment" to "Y". Use of the RPC service is then only possible in environments to which the user has READ access.

## User-Defined Resources

With Natural SAF Security, user-defined resources can be protected against unauthorized use. You can protect a user-defined resource:

- independently of the environment, or
- in specific environments.

## Environment-Independent Use of a User-Defined Resource

### SAF Server Definitions

The resource-class name for user-defined resources is defined with the macro parameter NACLAP in the configuration module of the SAF server (see Step 4 of the Natural SAF Security installation procedure). The default name is "NPGSAG".

### External Security System Definitions

If a user-defined resource is to be protected, a resource profile has to be defined for it in the external security system.

The name of a resource profile can, for example, consist of a library ID, main function and subfunction. The library ID may be up to 8 characters long, the main function is usually (but not necessarily) the name of the programming object, and the subfunction is a 3-character code identifying the function to be performed. Each of the three must be separated from one another by a period:

*library-ID.main-function.sub-function*

The resource profile determines whether a user may access a user-defined resource or not.

### Natural SAF Security Definitions

The necessary security requests are handled via application interfaces provided by Natural SAF Security.

## Use of a User-Defined Resource in Specific Environments

### SAF Server Definitions

The resource-class name for user-defined resources is defined with the macro parameter NACLAP in the configuration module of the SAF server (see Step 4 of the Natural SAF Security installation procedure). The default name is "NPGSAG".

### External Security System Definitions

If a user-defined resource is to be protected in a specific Natural environment (Natural system-file combination), a resource profile has to be defined for the environment-resource combination in the external security system. A Natural environment is determined by a one-character alias. The resource-profile name is composed as above, prefixed by the alias, for example:

*a.library-ID.main-function.sub-function*

The resource profile determines whether a user may access a user-defined resource in that environment or not.

### Natural Security Definitions

In Natural Security, you have to define an environment profile for the environment. In the environment profile, the alias to be used has to be specified.

### Natural SAF Security Definitions

The environment-specific resource-access check is activated by setting the NSF user-resource option "with Environment" to "Y".

The necessary security requests are handled via application interfaces provided by Natural SAF Security.

## Overview of Resource-Class Definitions

The following table summarized the resource-class definitions to be made in the configuration module of the SAF server:

Resource	Macro Parameter in Configuration Module	Default Name	Length of Resource-Profile Name
Environments	NACLSF	NSFSAG	40
Libraries	NACLTC	NTCSAG	10
RPC services	NACLSV	NSVSAG	19
User-defined resources	NACLAP	NPGSAG	23

## Translation and Effects of Access Levels

The following table shows how CA-ACF2 translates RACF attributes, and also gives an overview of the effects of the access levels:

RACF Attribute	CA-ACF2 Resource Rule	Disabling of Natural Commands	Read-Only FUSER System File
READ	READ	Commands are disabled (same as profile parameter NC=ON).	FUSER file is read-only.
UPDATE	UPDATE	Commands are disabled (same as profile parameter NC=ON).	FUSER file is read-only.
CONTROL	DELETE	Commands are allowed (same as profile parameter NC=OFF).	FUSER file is read-only.
ALTER	ADD	Commands are allowed (same as profile parameter NC=OFF).	Modification on FUSER file are allowed.

## Examples of Resource Definitions

This section provides examples of how resources are defined in the external security system:

- Example of Resource Definitions in RACF
- Example of Resource Definitions in CA-ACF2
- Example of Resource Definitions in CA Top Secret

### Example of Resource Definitions in RACF

This is an example of how to define resources in RACF.

For details on RACF features, see IBM's RACF documentation. See also the SAF Security Kernel documentation.

#### Adding a Class to the Class Descriptor Table

For details on how to add a resource class to the RACF class descriptor table, see IBM's SPL RACF manual; for an example, see "IBM SYS1.SAMPLIB", member RACINSTL. Allocate a maximum length of 40 for the class. Define the class to enable discrete and generic profile use. Check further attributes controlling the level of RACF messages generated when performing RACROUTE calls, as well as the required level of SMF recording. Sample definitions are provided in source member RACFCLSX.

Add the resource class "NSFSAG" for Natural environments.

#### Updating the OS/390 Router Table

Update the OS/390 router table, as described in IBM's SPL RACF manual; for an example, see "IBM SYS1.SAMPLIB", member RACINSTL, section RFTABLE.

#### Activating a New Resource Class

Activate the new resource class "NSFSAG" with SETROPTS (see IBM's RACF Command Language Reference manual):

```
SETROPTS CLASSACT(NSFSAG)
SETROPTS GENCMD(NSFSAG)
SETROPTS GENERIC(NSFSAG)
```

#### Adding a Resource Profile for Environments and Permitting Access to it

Assume the following Natural environment (system-file combination) to be protected:

```
FNAT = (76,225)
FDIC = (76,148)
FSEC = (76,223)
FUSER=(76,1000)
```

To add a resource profile for the above environment, and grant READ access to user ID "ADE", issue the following RACF commands:

```
RDEFINE NSFSAG 0007600225000760014800076002300007601000 UACC(NONE)
PERMIT 0007600225000760014800076002300007601000 CLASS(NSFSAG) ACCESS(READ) ID(ADE)
```

## Example of Resource Definitions in CA-ACF2

This is an example of how to define resources in CA-ACF2.

For details on CA-ACF2 features, see Computer Associates' CA-ACF2 documentation. See also the SAF Security Kernel documentation.

### Adding a CLASMAP Record for Environments

Add a CLASMAP record for Natural environments as follows:

```
ENTITYLN(0) MUSID() RESOURCE(NSFSAG) RSRCTYPE(NSF)
```

### Defining a Resource Rule for an Environment and Allowing Access to it

Assume the following Natural environment (system-file combination) to be protected:

```
FNAT = (76,225)
FDIC = (76,148)
FSEC = (76,223)
FUSER=(76,1000)
```

To allow the above environment for all user IDs, define the following rule:

```
$KEY(0007600225000760014800076002300007601000) TYPE(NSF) UID(*) SERVICE(READ,UPDATE)
ALLOW
```

### Disallowing Access to an Environment

To disallow access to the above environment for user ID "ADE", define the following rule:

```
$KEY(0007600225000760014800076002300007601000) TYPE(NSF) UID(ADE) SERVICE(READ,UPDATE)
PREVENT
```

## Example of Resource Definitions in CA Top Secret

This is an example of how to define resources in CA Top Secret.

For details on CA Top Secret features, see Computer Associates' CA Top Secret documentation. See also the SAF Security Kernel documentation.

### Adding a Resource Type for Environments to the Resource Definition Table

To add the resource type "NSFSAG" for Natural environments to the CA Top Secret resource definition table (RDT), issue the following command (see Computer Associates' CA Top Secret Reference Guide for details):

```
TSS ADD(RDT) RESCLASS(NSFSAG)
RESCODE(HEXCODE)
ATTR(LONG)
ACLST(NONE,READ,CONTROL)
DEFACC(NONE)
```

### Adding a Resource Profile for an Environment and Assigning Ownership

Ownership must be assigned to a resource profile, before access to it can be permitted.

Assume the following Natural environment (system-file combination) to be protected:

```
FNAT = (76,225)
FDIC = (76,148)
FSEC = (76,223)
FUSER=(76,1000)
```

To define a resource profile for the above environment, and assign user "USER1" as owner to this resource profile, issue the following command:

```
TSS ADD(USER1) NSFSAG(0007600225000760014800076002300007601000)
```

### **Permitting Access to an Environment**

To grant user "ADE" READ access to the above environment, issue the following command:

```
TSS PER(ADE) NSFSAG(0007600225000760014800076002300007601000) FAC(fac) ACCESS (READ)
```

# Administrator Services

The Administrator Services subsystem of Natural Security provides the following functions which are used in conjunction with Natural SAF Security:

- NSF Options
- Environment Profiles
- SAF Online Services

In order to use these functions:

- you need to have access to the Natural Security library SYSSEC;
- you have to be defined in Natural Security as a user of type "Administrator";
- you need to have access to the Administrator Services subsystem of Natural Security (as described in the section Access to Administrator Services of the Natural Security documentation).



The user ID "DBA" should not be used for testing purposes. If you log on to SYSSEC as user "DBA", any Natural SAF Security settings and checks will be ignored. As indicated in the Natural Security installation documentation, the user ID "DBA" should only be used for the initial definition of Natural Security administrators and for recovering the Natural Security environment.

---

## NSF Options

Natural Security's "General Options" provide several additional options which are used in conjunction with Natural SAF Security to setup your security environment. These "NSF options" are only available if Natural SAF Security is installed.

For any changes of these options to take effect, you have to restart the SAF server and then restart your Natural session.



To invoke the NSF options:

1. On the Natural Security Main Menu, select "Administrator Services". The Administrator Services Menu 1 will be displayed.
2. On the Administrator Services Menu 1, select "General options". The first General Options screen will be displayed.
3. General Options consists of four screens. With PF7 and PF8, you can switch between the screens. General Options 3 and 4 contain the NSF options.

The following types of NSF options are available:

- Security System
- User Options
- Environment Options
- Library Options
- RPC Options
- User-Resource Options

The individual options are described below.

General Options 3 (NSF):

```

16:21:26                *** NATURAL SECURITY ***                2003-09-24
                        - General Options 3 (NSF) -                Server Id 00000

                                Created ... 2003-07-09 by ADE
                                Modified .. 2003-09-24 by ADE

Security System
  External Security System ... _____ Server ID ..... _____
  Natural Security ..... FSEC           Protection Level ..... 1

User Options
NSF *GROUP ..... Y (Y,N)   NSC Group ID ..... Y (Y,N)
NSF *USER-NAME ..... Y (Y,N) NSC User ID ..... N (Y,N)
NSF *ETID ..... (N,O,B,A,J,T) N   NSC Logon Priv.Library N (Y,N)
NSF *USER Automatic Logon .. N (Y,N)

Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10--PF11--PF12---
      Help           Exit           Def.  Flip  NSC   NSF2                               Canc
    
```

Security System

Option	Explanation
<b>External Security System</b>	<p>In this field, you specify the external security system to be used.</p> <p>Possible values are: RACF, ACF2 (= CA-ACF2) and TOPS (= CA Top Secret) and SAF.</p> <p>The default value is "SAF": this means that only NSF Options which apply to all supported external security systems are evaluated, while those which are specific to a certain security system will be ignored.</p> <p><b>Note:</b> The value of this option is evaluated internally by Natural SAF Security only, but is not communicated to the SAF server. In the SAF server, the external security system is specified in the configuration module.</p>
<b>Server ID</b>	<p>In this field, you specify the node ID of the SAF server to be used (that is, the value of the parameter GWDBID as specified in the SAF server installation).</p>
<b>Natural Security</b>	<p><i>This field is reserved for future use. At present, it must contain "FSEC".</i></p>
<b>Protection Level</b>	<p>This field is used to activate Natural SAF Security. Possible values are:</p> <p><b>1</b> - Natural SAF Security is not active, and the SAF server is not accessed. Access to the Natural session is controlled by Natural Security.</p> <p><b>2</b> - Natural SAF Security is active. Access to the Natural session is controlled by the SAF server. <i>Within</i> the session, Natural Security determines what users are allowed to do.</p>

## User Options

Option	Explanation
<b>NSF *GROUP</b>	<p>Determines whether the group ID defined in the external security system is to be used as value for the Natural system variable *GROUP (Y/N).</p> <p>It is recommended that this option be set to "Y" (see also option "NSC Group ID" below).</p>
<b>NSC Group ID</b>	<p>Determines whether the group IDs defined in the external security system also have to be defined in Natural Security (Y/N).</p> <p>It is recommended that this option be set to "Y"; any conditions of use associated with the Natural Security group profile can then be controlled by Natural Security.</p> <p>RACF allows for a user to be in multiple groups. If this option is set to "Y", any of these groups can be used for a logon to a protected library, and they will be evaluated by the Natural logon procedure to select the group to be used for the logon.</p>
<b>NSF *USER-NAME</b>	<p>Determines whether the user name defined in the external security system is to be used as value for the Natural system variable *USER-NAME (Y/N).</p>
<b>NSC User ID</b>	<p>Determines whether, in addition to being defined in the external security system, users also have to be defined in Natural Security (Y/N).</p> <p>If set to "Y", the Natural Security user profile will be used once the user has successfully logged on to the external security system. After the initial logon, the conditions of use associated with the Natural Security user profile will be controlled by Natural Security. However, Natural Security will not perform any password checks.</p>
<b>NSF *ETID</b>	<p>Determines if and how ETIDs (end of transaction IDs) are to be generated by Natural SAF Security at the start of the Natural session:</p> <ul style="list-style-type: none"> <li><b>N</b> No ETIDs are generated by Natural SAF Security; they are generated by Natural Security.</li> <li><b>O</b> Generate ETIDs only for online users.</li> <li><b>B</b> Generate ETIDs only for batch-mode users.</li> <li><b>A</b> Generate ETIDs for all (online and batch-mode) users.</li> <li><b>J</b> Use the job name as ETID (for batch-mode users only).</li> <li><b>T</b> Use the value of the Natural system variable *INIT-ID as ETID.</li> </ul>
<b>NSC Logon Priv. Library</b>	<p>This option controls users' access to private libraries:</p> <ul style="list-style-type: none"> <li><b>N</b> Access to private libraries is controlled by Natural Security.</li> <li><b>Y</b> When a user logs on without specifying a library ID, the current value of the Natural system variable *USER will be used as library ID. If the library option "Protect Libraries" (see below) is set, this requires a corresponding resource profile for this library.</li> </ul>

<b>NSF *USER Automatic Logon</b>	<p>When Automatic Logon is used (Natural profile parameter AUTO=ON), Natural uses the value of the Natural system variable *INIT-USER as value for the Natural system variable *USER. To prevent this, you can use this option.</p> <p><b>Y</b> The *INIT-USER value is not used for *USER.</p> <p><b>N</b> The *INIT-USER value is used for *USER (this is the default).</p>
----------------------------------	---

**General Options 4 (NSF):**

```

16:11:39                *** NATURAL SECURITY ***                2003-09-24
                        - General Options 4 (NSF) -                Server Id 00000

                                Created ... 2003-07-09 by ADE
                                Modified .. 2003-09-24 by ADE

Environment Options
Protect Environments ..... N (Y,N)  Allow Undef. Environments .. N (Y,N)

Library Options
Protect Libraries ..... N (Y,R,N) with Environment ..... N (Y,N)
Disable Natural Commands... N (Y,N)  Set FUSER Read-Only ..... N (Y,N)

RPC Options
Protect Services ..... N (Y,R,N) with Environment ..... N (Y,N)

User-Resource Options
with Environment ..... N (Y,N)  Allow Undef. Resources ..... N (Y,N)

Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10--PF11--PF12---
      Help      Exit      Def.  Flip  NSF1                        Canc
    
```

**Environment Options**

Option	Explanation
<b>Protect Environments</b>	<p>Determines whether the environment profile of the system-file combination (FNAT, FUSER, FDIC, FSEC) is to be checked at the logon (Y/N).</p> <ul style="list-style-type: none"> <li>• If this is set to "Y", the access level defined for the environment in the external security system determines whether a user has access to it or not.</li> <li>• If this is set to "N", users have access to any environment.</li> </ul> <p>See also Environment Profiles below.</p>
<b>Allow Undef. Environments</b>	<p>Determines whether undefined system-file combinations are to be accepted at the logon (Y/N).</p> <p>This option is only relevant if RACF is used as external security system. With other external security systems, this option will be ignored.</p>

## Library Options

Option	Explanation
<b>Protect Libraries</b>	<p>Determines whether the library access level is to be checked via the SAF server (Y/N/R).</p> <ul style="list-style-type: none"> <li>● Y - Users need at least READ access to log on to a library.</li> <li>● N - Access to libraries is controlled by Natural Security according to the Natural Security logon rules.</li> <li>● R - If RACF is used as external security system, you can set this option to "R": The library access level will be checked, but access to libraries not defined in RACF will also be possible. For other security systems, "R" is not possible.</li> </ul>
<b>with Environment</b>	<p>Determines whether the environment alias is to be used as prefix of the resource library for the access-level check (Y/N).</p> <p>See also Environment Profiles below.</p>
<b>Disable Natural Commands</b>	<p>Determines whether the use of Natural system commands is to be controlled by the access level (Y/N).</p> <p>If this option is set to "Y", the access level determines whether the use of Natural system commands is allowed:</p> <ul style="list-style-type: none"> <li>● If the access level is CONTROL or higher, the use of system commands is allowed.</li> <li>● if the access level is lower than CONTROL, the use of system commands is not allowed.</li> </ul> <p>If this option is set to "Y", the Natural profile parameter NC as well as any settings concerning system commands in Natural Security library profiles (Allow System Commands, Command Restrictions and Editing Restrictions) will be ignored.</p>
<b>Set FUSER Read-Only</b>	<p>Determines whether read-only access to the FUSER system file is to be controlled by the access level (Y/N).</p> <p>If this option is set to "Y", the access level determines whether modifications of the data on the FUSER system file are allowed:</p> <ul style="list-style-type: none"> <li>● If the access level is ALTER, modifications on the FUSER file are allowed. This requires the definition of a Natural scratch-pad file (as described in the Natural Operations documentation for mainframes).</li> <li>● If the access level is lower than ALTER, modifications on the FUSER file are not allowed.</li> </ul> <p>If this option is set to "Y", the RO option of the Natural profile parameter FUSER is ignored.</p>

## RPC Options

Option	Explanation
<b>Protect Services</b>	<p>Determines if the Natural RPC service access is to be checked via the SAF server (Y/N/R):</p> <ul style="list-style-type: none"> <li>● N - Access to a service is controlled by the Natural Security library profile of the library containing the subprogram.</li> <li>● Y - Access to a service is controlled by the resource profile. Users need at least READ access to execute a service. In addition, the library profile of the library containing the subprogram.applies.</li> <li>● R - This is the same as "Y"; however, access to services not defined in RACF will also be possible. "R" is only possible if RACF is used as external security system.</li> </ul>
<b>with Environment</b>	<p>Determines whether the environment alias is to be used for the service-access check (Y/N). See also Environment Profiles below.</p>

## User-Resource Options

Option	Explanation
<b>with Environment</b>	<p>Determines whether the environment alias is to be used as prefix to the resource definitions (Y/N).  See also Environment Profiles below.</p>
<b>Allow Undef. Resources</b>	<p>Determines whether access to undefined resources is to be allowed via the Natural SAF Security application interfaces (Y/N).  This option is only relevant if RACF is used as the external security system. With other external security systems, this option will be ignored.</p>

## Environment Profiles

If you wish to protect resources in specific environments, you have to define environment profiles for these environments (that is, security profiles for the individual system-file combinations).

In an environment profile, you specify a one-character alias for the environment. The alias is used to identify the environment to the external security system; the environment-specific resource profiles whose names are prefixed with this alias determine users' access rights, if the "with Environment" option for the resource class in question is set to "Y" in the NSF options (see above).

To define environment profiles, you use the Natural Security function "Environment Profiles", as described under Defining Environment Profiles in the section Protecting Environments of the Natural Security documentation.

For any environment-profile modifications to take effect in Natural SAF Security, you have to restart your Natural session.

## SAF Online Services

SAF Online Services are only available if Natural SAF Security is installed.

SAF Online Services provide several functions for monitoring the SAF server. They are described under SAF Online Services in the Natural Security documentation.

SAF Online Services can be invoked:

- from within the Natural Security library *SYSSEC* by selecting it from the Administrator Services Menu, or
- from anywhere else in Natural by issuing the direct command *SYSSAFOS*.

To be able to access SAF Online Services, a utility security profile for *SYSSAFOS* has to be defined in Natural Security (as described in the section Protecting Utilities of the Natural Security documentation).

# Application Interfaces

This section describes the application interfaces provided by Natural SAF Security. It covers the following topics:

- Overview of Application Interfaces
- Application Interfaces for User and Password Authentication
- Application Interface for Checking Resource Access to Dedicated API Class
- Application Interface for Maintaining Resource Profiles
- Application Interface for Checking Access Rights to a Resource
- Application Interface for Obtaining Information from the SAF Server
- Natural Security Application Interfaces

## Overview of Application Interfaces

Natural SAF Security provides the following application interfaces:

Function	Invoked Subprogram	Example Program of how to Invoke the Subprogram
User and password authentication.	NSFNPAS	PGMSFU01
	NSFNPAZ	PGMSFU02
	NSFNPAX	PGMSFU03
Check resource access to a dedicated API class.	NSFNAPC	PGMSFC $nn$
Maintain resource profiles.	NSFNRES	PGMSFR $nn$
Check access rights to a resource.	NSFNRES	PGMSFX $nn$
Obtain miscellaneous information from the SAF server.	NSFNINF	PGMSFI $nn$

The example programs are provided in the Natural Security library SYSSEC.

## Application Interfaces for User and Password Authentication

- NSFNPAS
- NSFNPASZ
- NSFNPAX

### NSFNPAS

The subprogram NSFNPAS can be called from any Natural library to verify the authentication of a user (\*USER) and, optionally, establish that the user was already logged on.

Five different sub-call are available:

#PAS-FUNC	Action
INDQVER	Verify user ID (not password) and create ACEE.
INDQVPW	Verify user ID and password, creating new ACEE.
INDQVPO	Verify user ID and password without creating new ACEE (CA Top Secret only).
INDQVPT	Verify user ID and password without creating ACEE (CA Top Secret only).
INDQVPC	Verify user ID and password and change password creating new ACEE.

The parameter data area NSFAPAS is available to invoke this subprogram. Its fields are:

Field	Format/Length	Description
#PAS-FUNC	B1	Indicates type of verification check required.
#PAS-RETC	B1	Return code: 8 = error; 16 = severe error.
#PAS-POLD	A8	Existing (old) password.
#PAS-PNEW	A8	New password.
#PAS-ACCN	A8	Accounting information - <i>for future use</i> .
#PAS-SERR	B8	Return code (as described in the SAF Security Kernel documentation).

## NSFNPASZ

To verify the password of any other user ID, the subprogram NSFNPASZ is provided.

The parameters are the same as described for subprogram NSFNPAS above.

In addition, the parameter data area NSFAPAS contains the following fields for NSFNPASZ:

Field	Format/Length	Description
#PAS-PUSER	A8	User ID of user whose password is to be changed.
#PAS-PMSG	A40	Message text returned from the SAF server.

## NSFNPAX

To verify and change the password of \*USER, the subprogram NSFNPAX is provided.

The parameters are the same as described for subprogram NSFNPAS above.

In addition, the parameter data area NSFAPAS contains the following fields for NSFNPAX:

Field	Format/Length	Description
#PAS-PUSER	A8	<i>Not used.</i>
#PAS-PMSG	A40	Message text returned from the SAF server.

## Application Interface for Checking Resource Access to Dedicated API Class

The subprogram NSFNAPC can be called from any Natural library to check the access to a general resource profile.

### Input Parameters:

Parameter	Content
#RES-PROF	Name of desired profile.
#RES-CLAS	Name of desired class.
#RES-ATTR	Access level to be checked: H'02' = READ access, H'04' = UPDATE access; H'08' = CTL access, H'80' = ALTER access.  If you specify H'00', the highest access level will be returned.

### Output Parameters:

Parameter	Content
#RES-ATTR	If H'00' was specified as input, this field returns the highest acceptable access level.
#RES-RETC	Return code: 0 = Profile allowed for given access level. 8 = Error (in this case, the field #RES-SERR contains the SAF error code).

## Application Interface for Maintaining Resource Profiles

The subprogram NSFNRES can be called from any Natural library to read and maintain security-profile information.

RACF, CA Top Secret and CA-ACF2 enable different levels of functionality to be achieved. The different functions are shown below:

#RES-FUNC	Action
INDQRTV	Retrieve field(s) from user, group, and general profiles of the security system. CA Top Secret and CA-ACF2 allow fields such as PGMNAME to be read from a base segment.
INDQRDN	Retrieve next resource profile in collating sequence. The name of the resource and selected field(s) can be retrieved. CA Top Secret permits only the USER class to be retrieved in this way. This functionality is currently not available with CA-ACF2.

The parameter data area NSFARES available to invoke this subprogram. Its fields are:

Field	Format/Length	Description
#RES-FUNC	B1	Indicates function type required.
#RES-ATTR	B1	<i>Not used for this call.</i>
#RES-RETC	B1	Return code: 0 = call successful ; 4 = profile not found/EOL; 8 = error.
#RES-CLAS	A8	Required resource class/type.
#RES-GRUP	A8	Default user group - returned.
#RES-PROF	A32	Name of resource profile.
#RES-FLDA	A8 * 4	Profile field names (array).
#RES-SERR	B8	8-byte return code (as described in the SAF Security Kernel documentation).
#RES-SLOG	A4	<i>Reserved for future use.</i>
#RES-DATA	A16 * 16	Profile data input/output area. The data layout is described in detail in the IBM RACROUTE documentation.

## Application Interfaces for Checking Access Rights to a Resource

The subprogram NSFNRES can be called from any Natural library to test a user's authorization to any resource profile, including those used to protect Natural objects.

#RES-FUNC	Action
INDQCHK (#RES-ATTR supplied)	Check authorization at given level of access.
INDQCHK (#RES-ATTR zero)	Determine user's maximum access level.

The parameter data area NSFARES is provided to invoke this subprogram. Its fields are:

Field	Format/Length	Description
#RES-FUNC	B1	Indicates function type required
#RES-ATTR	B1	Access level to be tested; either zero or determine highest level (as described in the IBM RACROUTE documentation).
#RES-RETC	B1	Return code: 0 = success; 8 = error.
#RES-CLAS	A8	Resource class/type.
#RES-PROF	A32	Name of resource profile.
#RES-SERR	B8	8-byte return code (as described in SAF Security Kernel documentation).

## Application Interface for Obtaining Information from the SAF Server

The subprogram NSFNINF is provided to perform a number of functions which may be useful when using Natural SAF Security.

The different functions provided are:

#INFFUNC	Action
INF-1	Determine last "access denied" message for this user.
INF-2	Determine last "access denied" message - internal format.
INF-3	Return invocation count.
INF-4	Return environment code.
INF-5	Read user name and group from values stored.
INF-6	Update user-name/group values; for example, if these are to be reformatted.
INF-7	<i>Currently not available.</i>
INF-8	<i>Currently not available.</i>
INF-9	Write SMF record.

The parameter data area NSFAINF is provided to invoke this subprogram. The local data area NSFLEQU defines the necessary equate values.

Field	Format/Length	Description
#INFFUNC	B2	Indicates function type required.
#INFRETC	I2	Return code: zero = success.
#INFDATA-SUBR	I4	Error - sub-response.
#INFDATA-TEXT	A72	Last error message.
#INF-COUNT	I4	Invocation count.
#INF-ENV	A1	Current environment code.
#INF-GROUP	A8	Group.
#INF-NAME	A32	User name.
#INF-SMFLLEN	B1	Length of SMF data to be written.
#INF-SMFTXT	B255	Data to be written - A15 * 17.

## Natural Security Application Interfaces

When Natural SAF Security is active, the evaluations made by some Natural Security application interfaces will be based not only on user data defined in Natural Security, but also on user data as defined in the external security system. This affects the following application interfaces:

- subprogram NSC---L,
- subprogram NSCXR with parameters POBJ-TYPE='US' and SUB-TYPE='GR', 'GP' and 'GM'.