SIS264
Securing Remote Access within SAP NetWeaver AS ABAP including SNC and SSL
Birger Toedtmann, Frank Buchholz, Michael Kraemer
October / November 2012
Disclaimer

This presentation outlines our general product direction and should not be relied on in making a purchase decision. This presentation is not subject to your license agreement or any other agreement with SAP. SAP has no obligation to pursue any course of business outlined in this presentation or to develop or release any functionality mentioned in this presentation. This presentation and SAP's strategy and possible future developments are subject to change and may be changed by SAP at any time for any reason without notice. This document is provided without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. SAP assumes no responsibility for errors or omissions in this document, except if such damages were caused by SAP intentionally or grossly negligent.
Agenda

1. Overview

2. Access Control for ABAP Remote Requests
   - Access Control for ABAP-ABAP Connections
   - Access Control for RFC Execution
   - Use Workload Analysis to Build Authorizations
   - Exercises

3. Trusted Connections
   - Trust Relationship Maintenance
   - Trusted Connection Access Control
   - Security Level of Trust Relationships
   - Exercises

4. Secure RFC Programming
   - Authority Checks
   - Input Validation
   - Exercises

5. Secure Network Communication (SNC) for RFC
   - Setup And Certificate Exchange
   - Demo

6. Secure Socket Layer (SSL) for HTTP
   - Setup And Certificate Exchange
   - Demo

7. Recent Improvements
Overview

RFC And HTTP Based Communication Between Two Application Servers
Communications Between Two ABAP Systems

RFC Call / HTTP Request
Communications Between Two ABAP Systems: RFC

All incoming RFC requests are handled by the SAP Gateway.

Find error messages in trace files dev_w*. 
Communications Between Two ABAP Systems: HTTP

All incoming and outgoing HTTP requests are handled by the Internet Communications Manager (ICM).

ABAP System

Server System

HTTP Call

Find error messages in ICM trace file
Access Control for Connections

S_ICF Authority Check on Client-Side
Access Control for RFC/HTTP Connections In Source System

ABAP System

Client System

S_ICF authority check

RFC Call or HTTP Request

Server System

Find error messages in ST01 trace
Access Control for Connections
Step 1: Maintain authorization field in connection (transaction SM59).

- Specify a literal in “Authorization for Destination” field.
Access Control for Connections
Step 2: Maintain S_ICF authorization (transaction PFCG).

PFCG Role Maintenance
- Assign S_ICF authorization to the role with following field values:
- ICF_FIELD: DEST,
Access Control for RFC Execution

S_RFC Authority Check in Target System
Access Control for RFC Connections In Target System

ABAP System

RFC Call

Server System

Find error messages in ST01 trace
Access Control for RFC Execution
Maintain S_RFC authorization (transaction PFCG).

S_RFC authorization with 3 fields:

**ACTVT:** Activity
- Value 16 (Execute)

**RFC_NAME:** Names of RFC objects to which access is allowed (white list).

**RFC_TYPE:** Type of RFC object to which access is to be allowed.
- ‘FUGR’ for Function Group (since 3.1I Release).
- ‘FUNC’ for function module (since 7.02 Release).
## SAP Note 931252: Profile Parameter auth/rfc_authority_check

<table>
<thead>
<tr>
<th>Parameter value</th>
<th>Restrictions to full S_RFC authority check</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>No authority check.</td>
</tr>
<tr>
<td>1</td>
<td>No authority check for same user scenario. No authority check for SRFC function group.</td>
</tr>
<tr>
<td>2</td>
<td>No authority check for SRFC function group.</td>
</tr>
<tr>
<td>9</td>
<td>Unrestricted authority check.</td>
</tr>
</tbody>
</table>

**RFC Server System**
Authorization Test for ABAP RFC Connection

1. Navigate to ABAP connection in transaction SM59.

2. Execute menu path “Utilities → Test → Authorization Test”.

3. This checks:
   - logon in target system,
   - Authorization S_RFC for the logon user of the RFC.
Using Workload Analysis to Build S_RFC and S_ICF Authorizations

1. Call transaction ST03N (“Workload in System …”).

2. Select (and double-click) an application server or TOTAL (for all servers).

3. To analyze incoming RFC calls choose “RFC Server Profile” and “Function Module” tab. Use the function module list to build S_RFC authorizations.

4. To analyze destinations of outgoing RFC calls choose “RFC Destination Client Profile” and “Remote Destinations” tab. Use the destination list to build S_ICF authorizations.

See SCN Blog about report ZRFC_STATRECS_SUMMARY: How to get RFC call traces to build authorizations for S_RFC for free!
Using STAUTHTRACE to Build S_RFC and S_ICF Authorizations

STAUTHTRACE:
Advanced version of ST01 for tracing user authorization checks

1. Call transaction STAUTHTRACE (“System Trace for Authorization …”).

2. Select user and S_RFC / S_ICF object

3. Check “Filter Duplicate Entries”.

STAUTHTRACE is available since SAP_BASIS 7.00 SP26.
RFC (or HTTP) Trusted Connections
Transaction SMT1 and S_RFCACL Authority Check
Trust Relationships Between Two ABAP Systems

Trusted ABAP System (SID + license number)

RFC Call / HTTP Request

S_RFCACL Authority Check

Server System

Client System

Trusting ABAP System (SID + license number)
Security Benefits of Trust Relationships

1. No passwords are transmitted in network or stored in SM59 connection.

2. Uni-Directional Trust (Trusting System trusts Trusted System).

3. User and client specific access control via S_RFCACL authority check.
## Trusted RFC Logon: S_RFCACL Authority Check

<table>
<thead>
<tr>
<th>Authorization Field</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACTVT</td>
<td>Activity: 16=Execute</td>
</tr>
<tr>
<td>RFC_SYSID</td>
<td>Caller system id (SID)</td>
</tr>
<tr>
<td>RFC_INFO</td>
<td>Caller license number (provided both communication partners are at least 7.02 SAP_BASIS Release)</td>
</tr>
<tr>
<td>RFC_CLIENT</td>
<td>Caller client. Avoid * entry!</td>
</tr>
<tr>
<td>RFC_USER</td>
<td>Caller user. Avoid * entry!</td>
</tr>
<tr>
<td>RFC_EQUSER</td>
<td>Same caller user and target user (RFC_USER not considered!)</td>
</tr>
<tr>
<td>RFC_TCODE</td>
<td>Caller transaction code, checked if „Use transaction code“ is activated in SMT1 (Trust Configuration).</td>
</tr>
</tbody>
</table>

Note that due to its highly critical nature, S_RFCACL is **not** part of SAP_ALL.
Trust Relation Configuration

**Use transaction code:**

- Activate caller side transaction code check against S_RFCACL authorization field TCODE.
- Default: inactive.

Server System (Trusting) Transaction SMT1
For failed trusted logon read shortdump in target system.

<table>
<thead>
<tr>
<th>Trusted Error Code (T-RC)</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>0: Invalid logon data</td>
<td>Provide valid logon data (see logon error code L-RC in shortdump!).</td>
</tr>
<tr>
<td>1: Invalid trust relation</td>
<td>Re-create trust relationship (transaction SMT1 in target system).</td>
</tr>
<tr>
<td>2: Insufficient authorization</td>
<td>Maintain S_RFCACL authorization in logon client in target system.</td>
</tr>
<tr>
<td>3: Invalid timestamp</td>
<td>Check system time in caller and target system. Suspect replay attack.</td>
</tr>
</tbody>
</table>
Security of Trust Relationships

Trusted ABAP System
(SID + license number)

Original Client System

Rogue Client System

Trusting ABAP System
(SID + license number)

Server System

Trusted RFC Call
SAP Notes 1491645, 1498973: Security of Trust Relationships

Purpose: Protect against Unauthenticated System Access via Trusted Connections (RFC or HTTP), see SAP Note 1491645.

1. Check security level of Trust Relationships:
   • Report RS_SECURITY_TRUST_RELATIONS, see SAP Note 1498973, see screenshot.

2. Elevate old trust relationships to recommended security level:
   • Report RS_UPDATE_TRUST_RELATIONS, see SAP Note 1498973.
Excursion: Gateway Security

Protect Gateway With Access Control Files

SAP Gateway – Normal use

» Register external RFC server

Register with SWIFT
SAP Gateway – Normal use

» **Consume:**
  Execute OS commands, upload/download files, perform transports

Requests address platform independent ABAP layer of the Application Server

If platform dependent tasks need to performed, ABAP layer calls RFC servers via SAP Gateway to execute
Register external RFC server

In terms of dynamic load sharing, SAP Gateway may pass requests to the hacker’s RFC server.
» **Execute OS commands, upload/download files, perform transports**

Requests address platform independent ABAP layer of the Application Server.

If platform dependent tasks need to performed, ABAP layer calls RFC servers via SAP Gateway to execute.

Hacker tries to addresses RFC servers directly via SAP Gateway for platform / OS dependent actions bypassing the authentication in the ABAP layer.
SAP Gateway Protection – Further Information

See also


   → Whitepapers → “Secure Configuration SAP NetWeaver Application Server ABAP ”
Secure RFC Programming

Authority Checks and Input Validation
Restricting User Activities by Authority Checks

1. Introduce Authority Check in each remotely called function module.

2. Specify permitted activity (display, change, delete,…).

3. If necessary, restrict access to certain data.

4. In error messages, avoid giving information that a potential attacker can benefit from.
Guard against Injection Attacks by Input Validation

1. Best: Use whitelist.
   • Case statement in program code.
   • Persisted whitelist (e.g. database table).

2. Other means:
   • String comparison using regular expressions.
   • Use blacklist.

3. In error messages, avoid giving information that a potential attacker can benefit from.
Secure Network Communications (SNC)
Making RFC (and DIAG) More Secure
Recap: Why Trust Relationships Might Not Be Sufficient

A malicious user can still eavesdrop on the transmitted information.

A malicious user can still manipulate the transmitted information.
Communications Between Two ABAP Systems: RFC over SNC

SNC Certificate Exchange

SNC Secured RFC Call
Secure Network Communications (SNC) integrates an external security product with SAP systems, providing certain levels of protection of:

- identity of the communication partners,
- data communication.

SNC is available for the following protocols:

- RFC,
- DIAG (for communication between ABAP system with frontend using SAPGUI).

The SAP Cryptographic Library is a product that is available free-of-charge to customers to use for SNC connections between system components (ABAP systems and frontend).
SNC: Initial System Wide Configuration

1. Adjust profile parameters via RZ10.
   Important:
   - snc/identity/as = <ID used by partner system>
   - snc/enable = 1
   Set accept_insecure* = 1 for testing

2. Save profile, restart system.

3. If the system does not come up, there is typically an issue with the SNC library.
   Debug looking into trace files dev_w*.

---

RFC Client And Server Systems

snc/enable = 1
snc/gssapi_lib = <path to SNC lib>
snc/identity/as = <system ID>
snc/r3int_rfc_secure = 0
snc/accept_insecure_cpic = 1
snc/accept_insecure_gui = 1
snc/accept_insecure_r3int_rfc = 1
snc/accept_insecure_rfc = 1
SNC: Establish Mutual Trust By Exchanging Keys

In both (!) systems:

1. Start the Trust Manager using transaction STRUST

2. Verify that there exists a valid SNC PSE with respective certificates (private and public key)

3. If not, create one. It will carry the snc/identity/as name in its certificate DN

4. Export the certificate and import in partner system.

5. Save.
1. Maintain entries in SNC0 for all systems connecting to this one via SNC

2. Entries must match the respective snc/identity/as parameters of the initiating (client) systems

2. Authentication will be done using standard mechanisms (e.g. password or token)

2. Select QoP (Quality of protection) and enter SNC name of communication partner (parameter snc/identity/as of other system)

3. Save SNC configuration (SAVE icon in dialog box).

4. Select “Active” Radiobutton to the right of “SNC” button.

5. Save connection.
SNC: Libraries And Their Use Cases

The SAP Cryptographic Library (Subject to German Export Regulations)
- SNC for RFC (server to server connections)
- SNC for DIAG (SAP GUI to server connection): Authentication and encryption in pure Windows environments only, utilizing Kerberos
- SSL (HTTP based communications)

SNC Client Encryption (new product, free of charge)
- SNC for DIAG (SAP GUI to server connection): Encryption only, utilizing Kerberos, no authentication

SAP NetWeaver Single Sign-on: Secure Login Client (SLC) & Secure Login Library (SLL)
- SNC for RFC (server to server connections),
- SNC for DIAG (SAP GUI to server connection) Authentication and encryption in many different environments
- Related TechEd Session: „SIS101 - SAP NetWeaver Single Sign-On - Overview and Business Scenarios”.

Other 3rd Party SNC Libraries
- SNC for RFC (server to server connections),
- SNC for DIAG (SAP GUI to server connection) – including authentication
Secure Socket Layer (SSL)
Making TCP Based Communications More Secure
Communications Between Two ABAP Systems: HTTP over SSL

SSL Certificate Exchange

SSL Secured HTTP Call
SSL (with HTTP): Initial System Wide Configuration

1. Adjust profile parameters via RZ10:
   - `ssl/ssl_lib`: is required to point to a valid cryptographic library
   - `icm/server_port_<X>` must be set for HTTPS
   - `icm/verify_client`:
     0: client certificates are not requested by the server
     1: client certificates are requested by the server, but not required
     2: client certificates are requested by the server and required

2. Save profile, restart system. For ICM parameters, only ICM restart is required

3. Check whether everything is loaded properly in ICM trace file (dev_icm).
SSL for HTTP connection: Configuration in STRUST (Client)

1. Check SSL Client Entries
   - At least one entry for either anonymous or authenticated access must exist.
   - SSL Client (Anonymous): No client certificate is used for logon; SSL protocol ensures only the encryption of the HTTP connection.
   - SSL Client (Standard): Certificate is used to authenticate itself to other Web servers.

2. Create entry if not existing

3. Export certificate for import into receiver system (server).

4. Import server certificate from partner system (see next slide).
SSL for HTTP connection: Configuration in STRUST (Server)

1. Check SSL Server Entries
   • One entry per server node should exist

2. Create entry if not existing.

3. Export certificate for import into requesting system (client).

4. Import client certificate from partner system (see previous slide).
   • ANONYM: No client certificate is used for logon; SSL protocol ensures only the encryption of the HTTP connection.
   • DEFAULT: SAP Web AS uses Standard SSL client PSE to authenticate itself on other Web servers.
   • Others: SAP Web AS uses SSL client PSE as configured in transaction STRUST.

2. Select “SSL Active” radiobutton.

3. Save connection.
Latest Improvements
Latest Improvements

Input Help for Maintenance of S_RFC Authorization
• Search for function groups and function modules using filter criteria.
• Multiple selection supported.
• See SAP Note 1693446.

Improved Documentation of S_RFC Authorization
• Function group / function module entries in authorization field RFC_NAME constitute a whitelist.
• See SAP Note 1664340.

Deleting Trust Relationships Despite Connection Error
• Delete trust relationship in the trusting system (using transaction SMT1), even if trusted system is no longer reachable.
• See SAP Note 1744698.
Further Information

Related SAP TechEd Sessions
SIS101: SAP NetWeaver Single Sign-On – Overview and Business Scenarios
SIS203: SAP Runs SAP – Remote Function Call: Gateway Hacking and Defense
SIS263: SAP NetWeaver Single Sign-On – SSO for GUI for Microsoft Windows

SAP Security Whitepapers and SAP Public Web
http://service.sap.com/securitynotes (“Whitepapers”)
http://scn.sap.com/community/security
http://scn.sap.com/docs/DOC-17127 (SPJ Article “Secure the RFC Connections in Your SAP System Landscape”)  

SAP Education and Certification Opportunities
www.sap.com/education

Watch SAP TechEd Online
www.sapteched.com/online