How To Configure Message Level Security in SAP XI 3.0

Version 1.00 – May 2005

Applicable Releases:
SAP NetWeaver '04
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1  Scenario</td>
<td>1</td>
</tr>
<tr>
<td>2  Introduction</td>
<td>2</td>
</tr>
<tr>
<td>2.1 Important SAP Notes</td>
<td>2</td>
</tr>
<tr>
<td>2.2 History of Changes</td>
<td>2</td>
</tr>
<tr>
<td>3  The Step By Step Solution</td>
<td>3</td>
</tr>
<tr>
<td>3.1 Configuring Web service security in the ABAP stack</td>
<td>3</td>
</tr>
<tr>
<td>3.2 Configure Web Service Security in the Java Stack</td>
<td>5</td>
</tr>
<tr>
<td>3.3 Configure Business System PCK</td>
<td>8</td>
</tr>
<tr>
<td>3.4 Configure Business System IS</td>
<td>14</td>
</tr>
<tr>
<td>3.5 Configuring Message Archiving for the IS and PCK</td>
<td>19</td>
</tr>
<tr>
<td>4  Appendix</td>
<td>23</td>
</tr>
<tr>
<td>4.1 Apply the JCE Unlimited Strength Jurisdiction Policy</td>
<td>23</td>
</tr>
<tr>
<td>4.2 Deploy the Cryptographic Library IAIK on the IS</td>
<td>23</td>
</tr>
<tr>
<td>4.3 Troubleshooting</td>
<td>23</td>
</tr>
<tr>
<td>4.4 Roundtrip Configuration</td>
<td>24</td>
</tr>
<tr>
<td>4.4.1 Integration Directory</td>
<td>25</td>
</tr>
<tr>
<td>4.4.2 Partner Connectivity Kit</td>
<td>30</td>
</tr>
<tr>
<td>4.5 References</td>
<td>34</td>
</tr>
</tbody>
</table>
1 Scenario

If messages are exchanged between the SAP Partner Connectivity Kit (PCK) and the Integration Server (IS) over unsecured networks, for example the Internet, it should be ensured that the messages can neither be read nor changed by a third party. In addition to communication channel encryption (HTTPS protocol), it is possible to digitally sign and/or encrypt the message. Signing/encryption of messages is known as message level security (MLS).

This guide describes the implementation of MLS between the PCK and the IS – as part of SAP Exchange Infrastructure (XI) 3.0.

Message level security can be used for the XI-XML protocol, that is, for communication between

- PCK and IS
- IS and IS (SAP XI and SAP XI)

Besides the message level security for the XI-XML protocol, it is possible to exchange messages between SAP XI and other components in a secure manner using different adapters, for example the RNIF adapter. For more information, see SAP Help Portal at help.sap.com/nw04 → Process Integration → SAP Exchange Infrastructure → Runtime → Connectivity → Adapters.

The step-by-step example describes how Party A sends messages from the PCK using the XI-XML protocol to the IS, and how message level security is used to sign/encrypt the message. The way the message is forwarded to Party B can be configured accordingly.
2 Introduction

This How-To Guide helps SAP XI and security experts to enable MLS quickly. For more information, see the SAP Exchange Infrastructure Security Guide available on Service Marketplace at service.sap.com/security → Security in Detail → SAP Security Guides.

To set up the example scenario using message level security described in this guide, the following prerequisites must be fulfilled:

- SAP PCK is installed
  Refer to the Installation Guide – SAP Partner Connectivity Kit, available on Service Marketplace at service.sap.com/instguidesNW04 → Installation
- SAP XI 3.0 SP09 or higher is installed
- The JCE file has been applied to the corresponding JRE (see appendix)
- The cryptographic library IAIK has been deployed on the J2EE Engine of the IS and the PCK (see appendix)

For message level security, the transport protocol between the PCK and the IS does not necessarily have to be HTTPS/SSL. To be able to send and receive messages using HTTPS/SSL, the SAP J2EE Engine of the PCK and the ABAP stack of the IS must be configured to support HTTPS. For more information, see SAP Help Portal at help.sap.com/nw04 → Security → Network and Transport Layer Security → Using the Secure Sockets Layer Protocol with the SAP Web AS ABAP → Transport Layer Security on the SAP J2EE Engine.

Note that encryption of messages is only supported with SAP NetWeaver '04 SP 9 or higher.

2.1 Important SAP Notes

<table>
<thead>
<tr>
<th>SAP Note Number</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>713508</td>
<td>SAP XI: Message Security Settings</td>
</tr>
</tbody>
</table>

⚠️ Check regularly which SAP Notes are available.

2.2 History of Changes

⚠️ Make sure you use the current version of this How-To Guide.

You can find the current version of this How-To Guide on SAP Service Marketplace at service.sap.com/nw-howtoguides → SAP NetWeaver → Media Library → How-to Guides → Exchange Infrastructure.

The following table provides an overview of the most important changes in prior versions.

<table>
<thead>
<tr>
<th>Version</th>
<th>Important Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.00</td>
<td>First version of document</td>
</tr>
</tbody>
</table>
3 The Step By Step Solution

Message level security is based on the Web service security services provided by the J2EE Engine. These Web service security services are used by both the PCK and IS for signing/validating and encrypting/decrypting messages.

Therefore, MLS configuration must be done in both the ABAP and the JAVA stack of SAP XI 3.0.

- The IS ABAP stack must be configured as a consumer for the Web service security of the J2EE Engine.
- The J2EE Engine of both the PCK and the IS must be configured for MLS in terms of certificates and authorization.
- Archiving of messages is the last security-relevant topic described in this chapter.

The sender and receiver parties and services definition must be the same in the PCK and the IS. Party mapping is not part of this example configuration.

3.1 Configuring Web service security in the ABAP stack

The Web service security services of each J2EE Engine can be used by the IS ABAP stack for message level security. In this example, the J2EE Engine of the IS is used.

To configure Web service security in the ABAP stack of the SAP Web Application Server (SAP Web AS), follow the steps below:

1. Create and configure an RFC connection for the Web service security services (connects IS and J2EE).

Use transaction SM59 to create a new destination of type HTTP Connections to Ext. Server (connection type G).

Specify the following technical settings:

- Target Host: Host name of the IS.
- Service No.: HTTP/HTTPS port of the IS (Java stack).
- Path Prefix: Path prefix specified in the following step.
- Select the appropriate logon/security settings.

If a different J2EE Engine is used, specify the corresponding host.
name and port.

The user specified in the logon/security settings must exist on the J2EE Engine (see step 4).

2. Specify the path prefix for the destination of the Web service security services.

Depending on the logon procedure or security settings, you must set the path prefix as follows:

- For the logon procedure **Basic Authentication** or **Send SAP log ticket**:
  - With the SSL option deselected, enter the following path prefix:
    `/wssproc/plain?style=document`
  - With the SSL option selected, enter the following path prefix:
    `/wssproc/ssl?style=document`

- For the SSL Client Certificate logon procedure, enter the following path prefix:
  `/wssproc/cert?style=document`

3. Configure the logical port for the Web service security services.

The proxy **CO_WSSEWSSPROCESSOR_VI_DOCUMEN** is used by the Integration Engine to access the Web service security services if message level security is activated in a specific sender or receiver agreement.

Use transaction LPCONFIG to configure the logical port by specifying the following attributes:

- Proxy class: **CO_WSSEWSSPROCESSOR_VI_DOCUMEN**
3.2 Configure Web Service Security in the Java Stack

The Web service security in the Java stack must be configured for the J2EE Engines of both the IS and the PCK by applying the following steps:

- Generate a local keystore hosting the keys/certificates used for MLS and generate the actual keys/certificates as needed (step 5).
- Exchange public key certificates as needed (step 7).

Additionally, in the J2EE engine used by the IS, a user for the RFC connection of the ABAP stack must be created (step 4) and a security role must be assigned to this user (step 6).

Public Key Certificates

- **Message encryption**
  The sender (PCK) encrypts the message for the receiver (IS) using the receiver’s public key certificate (ISmls-cert, see Step 2). The receiver uses its own private key (ISmls) for decrypting the message.

- **Message signature**
  The sender (PCK) signs the message using its own private key (PCKmls). The receiver (IS) verifies the signature using the distinguished name of the private key, which is part of the Signature, and either the CA’s certificate or the public key certificate (PCKmls-cert) in case of self-signed certificates.

For message encryption and ease of use in later configuration, the certificates used for message level security must be exchanged between the J2EE Engines of the PCK and the IS (the latter one being the J2EE Engine that the IS ABAP stack is using for MLS).
1. Create a user for the RFC connection
   a. Standalone J2EE Engine
      Select the service Security Provider on the corresponding server.
      Under User Management, choose Create User and enter <RFCUSER> and <Password>.
   b. SAP Web AS double stack
      Create the user in the ABAP stack using transaction SU01.
      The user name must be at least 5 characters long.
      This step must be carried out only for the J2EE Engine that the IS ABAP stack is using for MLS.

2. Generate local keystore and key/certificate
   Root certificates are stored in the keystore of the TrustedCA.
   For private certificates, it is recommended that you create a new keystore view.
   - Select the service Key Storage, choose Create View, and enter the name of the new local keystore view.
   - For the example, create the keystore PCKlocal on the PCK and ISlocal on the IS J2EE Engine.
   - Create private and public keys for the newly created view:
     - Select the view and choose Entry – Create.
     - Make the relevant entries as shown below, select Store certificate and choose Generate.
     - In the example, enter the following common name and
entry name:
  o PCKmls in the PCK
  o ISmls in the IS J2EE Engine

3. Assign security roles

Use the J2EE Visual Administrator on the IS J2EE Engine to assign security roles as follows:

- Select the service Security Provider on the corresponding server.
- Under Policy Configuration select the component sap.com/tc-sec-wssec-app *wssprocess.jar
- Assign the security role WSSecurityProcessing to the user you specified in the above-maintained RFC destination for logging on to the IS.
- Assign the security role KeystoreAdministrator of the newly generated keystore view (for example, ISlocal) to the <RFCUSER> you specified in the above-maintained RFC destination for logging on to the IS:
  - Select the service Security Provider
  - Under Components select keystore view <local keystore view>, for example keystore view ISlocal
  - Select tab page Security Roles
  - Select security role KeystoreAdministrator
  - Select radio button Security
  - Add user <RFCUSER>

If the private key and public root certificate of any keystore view are not contained in the
TrustedCA or DEFAULT view, assign the security role KeystoreAdministrator of this keystore view component to the user you specified in the above-maintained RFC destination.

4. Exchange public key certificates

For message encryption or decryption and signature validation configuration, the public key certificates must be exchanged between the PCK and the IS J2EE Engine. If a message is sent encrypted from the PCK to the IS, the PCK encrypts the message using the public key certificate of the IS.

In the J2EE Visual Administrator navigate to Server Æ Keystore and select the corresponding keystore view.

- Export

   In the Entry section, select the certificate to be exported. Next, choose Export, and save the certificate to the hard disk of your J2EE Engine server.

   For the example, export:
   - PCKmls-cert on the PCK
   - ISmls-cert on the IS J2EE Engine

- Import

   After physically copying the certificates from one server to the other, choose Load and import the certificates.

   For the example, import:
   - ISmls-cert on the PCK
   - PCKmls-cert on the IS J2EE Engine

3.3 Configure Business System PCK

Party A sends files from a file system File System A to its business partner Party XI.

The following configuration objects are required on the PCK:

- Sender
- The sender collaboration profile including party, service, channel (File adapter in this example).
- Sender agreement (SA1)

**Receiver**
- The receiver collaboration profile including party, service, communication channel (XI adapter in this example).
  - Message level security will be activated in the communication channel.
- Receiver Agreement (RA1)
  - Message level security is configured in the sender agreement.

---

For more information about configuring the PCK, see SAP Help Portal at help.sap.com/nw04 → SAP NetWeaver → Process Integration → SAP Exchange Infrastructure → Runtime Connectivity → Partner Connectivity Kit

### 1. Access the PCK configuration tool
- Call the PCK by entering http://<host>:{port}/pck/start in your Web browser.
- Choose *Configuration PCK* (you may need to set the proxy in Java Web Start to NONE).
- Enter *User Name* and *Password* for the SAP J2EE Engine.
2. Configure the communication from the file system to the PCK

To enable the file system to exchange data with the IS, you must create the following objects in the PCK:

Party and service for File System A that sends the files with a communication channel of type Sender and FILE to the PCK.

- Create a Communication Party → Party, for example PartnerA
- Create the corresponding Service, for example FileService
- Create a Sender Communication Channel to configure the File adapter:
  - Enter the corresponding Party and Service.
  - Enter a name for the Communication Channel, for example FileIn, and choose Create.
  - Select File as adapter type.
  - Select Sender.
  - Enter the appropriate data to configure the File adapter, for example, Source Directory, Filename and so on.
3. Create the receiver communication party
   - Create a Communication Party → Party, for example PartnerXI.
   - Create the corresponding Service, for example SR4.
   - Create a Receiver Communication Channel of type XI to configure the connection between the PCK and the IS.
     - Enter the corresponding Party and Service.
     - Enter a name for the Communication Channel, for example XI, and choose Create.
     - Select XI as the adapter type.
     - Enter the appropriate data to configure the XI adapter.
       - Select Receiver.
       - Transport Protocol.
- Select the XI as the message protocol.
- Under URL, enter the IS target URL: 
  http(s)://<IShost>:<port>/sap/xi/engine?type=entry
- User Name
- Password
- Language
- Client
- To enable message level security, select Message Security.
4. Create the sender agreement
   Define a **Sender Agreement** for the above-specified sender and receiver parties.
   - Enter appropriate values for **Interface** and **Namespace**.
   - Select the File adapter communication channel, for example FileIn, as the **Sender Communication Channel**.
5. Define the receiver agreement and configure message level security

Define a **Receiver Agreement** for the above-specified sender and receiver parties.

- Specify **Interface** and **Namespace**. Asterisks (*) can be used for the **Receiver Agreement**.

- Select the XI adapter as the **Receiver Communication Channel**, for example XI.

- If **Message Security** is chosen in the communication channel configuration, message level security must be configured.
  - In the **Security Profile** field, select whether the message should be signed or encrypted or signed and encrypted.
  - **Certificate for Signature**
    Select the keystore, for example PCKlocal, and the certificate, for example PCKmls-cert, created for the PCK.
  - **Certificate for Encryption**
    Choose the keystore, for example PCKlocal and the imported certificate, for example ISmls-cert, from the receiver.

### 3.4 Configure Business System IS

The message from Party A is transferred to the IS of Party XI. Party XI might forward the message to Party B (not part of this guide).
To receive the message, the following objects are required in the IS:

- Party and service of Party A, which sends the message. If there is a signature and you want it to be validated or if the message needs to be decrypted, you must also define a communication channel of type *Sender and XI* and a corresponding sender agreement (SA2).

To forward the message to a receiver, the following objects need to be created in the IS. These objects are not part of this guide. Refer to the appendix for the roundtrip configuration.

- Party and service of Party B, which receives the message. You must define a communication channel of type *Receiver and XI*.
- A receiver determination (RD) to determine the receiver of the message.
- An interface determination (ID) to define the inbound interface for the outbound interface of the sender.
- A receiver agreement (RA3) to transfer the message from the IS to the PCK of Party B.
1. Access the Integration Directory (on the IS)
   - Call the IS by entering http://<host>:<port>/rep in your Web browser.
   - Choose Integration Directory (you may need to set the proxy in Java Web Start to NONE).
   - Enter User Name and Password for the SAP J2EE Engine or ABAP stack.

2. Create and configure a new scenario (optional)
   - Choose Object → New from the menu.
   - Choose Scenario.
   - Enter the relevant scenario name and description.
   - Choose Create.
   - Save the scenario.

3. Create a sender collaboration profile
   - Choose Create Object.
   - Create a new Party, for example PartnerA.
   - Create a Business Service for this party, for example FileService.
   - Create a sender Communication Channel, for example FromPCK, with the following specifications:
     - Adapter type: XI
     - Select Sender
     - Message Protocol: XI 3.0
     - Select Message Security

You only have to create the
communication channel if you want to apply message level security.
4. Create sender agreement

The sender agreement is necessary if the message signature must be validated or if the message must be decrypted.

- Define Sender Party, Service, Namespace and Interface.

- For message level security, the checkbox Sender Uses Virtual Receiver must be selected.

- For receiver party and service, enter at least an asterisk (*) or specify the virtual receiver.

If a message is received from the PCK or from another SAP XI system, the receiver party and service is set. If the checkbox Sender Uses Virtual Receiver is not selected, the sender agreement will not be taken into account.

- Certificate for Signature Validation

The Issuer and the Subject of the certificate used for signing the message on the sender system are required. If the certificate is imported into a J2EE Engine keystore, you could use the input help to select the correct certificate.

For the example, select the PCKmls-cert in keystore ISlocal.

- Certification Authority

Enter the keystore view that contains the trusted root certificate for the certificate used for signing the message. If the message is signed with a self-signed certificate, enter the keystore which contains the imported certificate.

For the example, enter keystore
ISlocal.

- **Certificate for Decryption**

  Select the private key of the certificate which was used in the sender system to encrypt the message (note that this certificate must be imported into the PCK's J2EE Engine).

  For the example, select the keystore ISlocal and the private key ISmls.

5. **Create a receiver collaboration profile**

   For a complete scenario, it is necessary to configure the receiver collaboration profile, the interface determination, the receiver determination, and the receiver agreement.

   However, the IS is able to accept the message sent by the PCK if only the sender collaboration profile and the sender agreement is defined as shown in the previous step.

   If you send messages to the IS without a receiver, configured message level security is applied to the message, but you will receive the error OUTBOUND_BINDING_NOT_FOUND.

   You find the receiver configuration in the appendix.

3.5 **Configuring Message Archiving for the IS and PCK**

   To enable message archiving for the PCK, the following post-installation steps are required for the SAP XML Data Archiving Service (DAS) of the SAP J2EE Engine:

   - Configuration of the XML DAS administration destination
   - Definition of the archive store
   - Synchronization and display of the home path of archiving objects
1. Configuration of the XML DAS administration destination

Use the Destinations service of the J2EE Visual Administrator of the PCK to configure an HTTP destination for the XML DAS administration by specifying the following values:

- **Name:** DASdefault
- **URL:** http://<host>:<port>/DataArchivingService/DAS
- **Authentication:** BASIC
- **User name:** XMLDAS
- **Password:** XMLDAS

You must use this user and password combination at present.

Save and check that the Destinations service is activated.

2. Definition of an archive store

To define an archive store, perform the following steps:

- Launch the XML DAS using the URL and logon data maintained for the HTTP destination above.
- Choose Define Archive Stores and then choose New and specify the following parameters:
  - **Archive Store**
    - Name of your archive store, for example, Archive Stores.
  - **Storage System**
    - Name of your storage system, for example AS1.
  - **Store Type**
    - Select File System.
  - **WebDAV Root or Win Root**
    - If your SAP J2EE Engine runs on a Windows operating system, enter the archive file path as, for example, C:\Archive. This folder must
have been created on the file system beforehand.

- **Unix Root**
  If your SAP J2EE Engine runs on a Unix or Linux operating system, enter the archive file path as, for example, `/usr/sap/Y6D/home/archive`. This folder must have been created on the file system beforehand.

- **Proxy Host**
  Leave this parameter empty.

- **Proxy Port**
  Leave this parameter empty.

- Choose **Insert Archive Store**, return to **Home**, and test your new archive store by choosing **Test Archive Stores**.

### 3. Synchronization and display of the home path of archiving objects

To synchronize and display the home path of archiving objects, perform the following steps:

- Choose **Synchronize Home Path** and enter the following parameters:
  - **Home Path**
    Enter the archive path.
  - **Action**
    Select **Insert New Home Collection**.
  - **Context**
    Enter any context name.
  - **Archive Store**
Select the archive store created above.

- Choose *Execute*. A success message will appear.
- Choose *List Archive Paths* to verify that your home path is assigned to your archive store.
- Call the Message Display Tool at `http://<host>:<port>/mdt` and authenticate with user *Administrator* for the SAP J2EE Engine of the PCK.
- Choose *Security Archiving*.
- Set the archiving settings (for example, the archiving Interval) according to your efforts.
4 Appendix

4.1 Apply the JCE Unlimited Strength Jurisdiction Policy
The JCE file has been applied to the corresponding JRE. Therefore, exchange the following files in directory `<jdk_home>/jre/lib/security` with the respective files you can download from http://java.sun.com.

- US_export_policy.jar
- local_policy.jar

4.2 Deploy the Cryptographic Library IAIK on the IS
The IAIK software can be downloaded from the SAP Service Marketplace at service.sap.com/swdc → Download → SAP Cryptographic Software.

- Extract the included car file.
- Deploy the _sec_java_crypto_signed_fs_lib_630SP1.sda file with the Software Deployment Manager (SDM).


4.3 Troubleshooting
Basically the following monitoring tools and log files are of interest for troubleshooting message level security:

- PCK
  - Message Monitoring Tool
    - For messages in state WAIT, see Chapter 3.2. These are messages that are rejected by the IS, for example, because of missing authorization for the Web service security services or for the keystore on the J2EE Engine.
    - Choose Error Log to show errors for messages that have not yet been processed by the messaging system and therefore not yet shown in the message monitor directly.
  - Default Trace
    - If errors occur during the message level security processing, they are traced in the default trace file. Use the J2EE Visual Administrator Log Viewer service to access the default trace.

- Integration Engine’s J2EE Server
  - Message monitoring tool, transaction SXMB_MONI
    - Verify that the sender agreement was taken into account that contains the message level security configuration. For an inbound message, two additional attachments are created:
      - MessageLevelSecurityBinaryStream
MessageLevelSecurityXML

If these attachments are missing, the sender agreement has not been found by the IS.

- Security Log
  - All security-relevant logs and traces are written into the security log. Access the security log by using the J2EE Visual Administrator’s Log Viewer.

1. Missing authorization for <RFC user>

As described in Step 3, the user specified in the ABAP RFC destination that points to the J2EE Engine’s Web security services needs authorization for the Web service security itself and for the keystore.

If the keystore authorization is not sufficient, the message sent from the PCK with MSL is rejected by the IS.

In the message monitoring tool of the PCK, you find a corresponding entry Received Response Code 500.

In the J2EE security log of the Integration Engine you find the exception shown here. Access the log file by using the log viewer (which is part of the J2EE Visual Administrator), section Cluster → Server → <Path> → <SID>/JC<SysNr> → j2ee/cluster/server0 → log → system → security.log.

4.4 Roundtrip Configuration

To complete the roundtrip, the message is sent from the IS to the PartnerB business service PCK. On the PCK, the message is then routed to the File adapter.

For this purpose, several configuration objects have to be created in the Integration Directory and in the receiving PCK:

- Integration Directory
  - Collaboration profile for PartnerXI and PartnerB
  - Logical routing objects
- 25 -

<table>
<thead>
<tr>
<th>Collaboration agreement</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCK</td>
</tr>
<tr>
<td>Collaboration profile for PartnerA and PartnerB</td>
</tr>
<tr>
<td>Collaboration agreement</td>
</tr>
</tbody>
</table>

## 4.4.1 Integration Directory

### 2. Access the Integration Directory
- Call the PCK by entering `http://<host>:<port>/rep/start` in your Web browser.
- Choose **Integration Directory**.
- Enter your user name and password.

### 3. Collaboration profile PartnerXI
Since PartnerXI is configured as receiver in the sender PCK, the collaboration profile of PartnerXI must be created in the Integration Directory.
- Create **Party**, for example PartnerXI.
- Create **Business Service**, for example SR4.
- Assign **Inbound Interface** to the business service, for example, `http://test.as/simpleTests`, SimpleInterfaceIn.

The interface can be created in the Integration Repository beforehand.
4. Collaboration profile PartnerB
   The receiver should be PartnerB rather than PartnerXI. The IS should only route the message to the correct receiver.
   - Create Party, for example PartnerB.
   - Create Business Service, for example PCK.
   - Assign Inbound Interface to the business service, for example, http://test.as/simpleTests, SimpleInterfaceIn.
   - Create a sender Communication Channel of type XI, for example ToPCK.
     - Adapter Type XI
     - Select Receiver
     - Transport Protocol can be either HTTP or HTTPS
     - Message Protocol XI 3.0
     - Addressing Type can be either URL Address or HTTP Destination.

   If you choose URL Address, enter Target Host, Service Number, and Path accordingly.

   If you choose URL Address, select Use Logon Data for Non-SAP System for the
Authentication Type.

- **User Name**
  User configured in PCK as receiver user, normally pckreceiver.

- **Password**
  - If you want to use message level security between the IS and the PCK, select *Message Security*. 

  ![Authentication Type Diagram](image-url)
5. Logical routing objects

### Interface determination

- **Sender Party**, for example PartnerA
- **Sender Service**, for example FileService
- **Interface**, for example SimpleInterfaceOut
- **Namespace**, for example http://test.as/simpleTests
- **Receiver Party**, for example PartnerB
- **Receiver Service**, for example PCK
- **Configured Inbound Interface**, for example http://test.as/simpleTests, SimpleInterfaceIn

### Receiver determination

- **Sender Party**, for example PartnerA
- **Sender Service**, for example FileService
- **Interface**, for example SimpleInterfaceOut
- **Namespace**, for example http://test.as/simpleTests
- **Check Sender uses virtual Receiver**
- **Receiver Party**, for example PartnerXI
- **Receiver Service**, for example SR4
- **Configured Receivers**, for example PartnerB, PCK
6. Collaboration agreement

Create a receiver agreement

- **Sender Party**, for example PartnerA
- **Sender Service**, for example FileService
- **Receiver Party**, for example PartnerB
- **Receiver Service**, for example PCK
- **Interface**, for example SimpleInterfaceIn
- **Namespace**, for example http://test.as/simpleTests
4.4.2 Partner Connectivity Kit

Ensure that the JCE Unlimited Strength Jurisdiction and the SAP Cryptographic library IAIK are deployed on the receiver PCK; refer to the appendix for more details.

Exchange the Public Key Certificates used for Signing and Encrypting Messages between the IS’s J2EE Engine and the PCK as described in Step 4.

7. Access the PCK Configuration Tool
   - Call the PCK by entering http://<host>:<port>/pck/start in your Web browser.
   - Choose Configuration PCK (you may need to set the proxy in Java Web Start to NONE).
   - Enter User Name and Password for SAP J2EE Engine.
8. Collaboration Profile PartnerA

If message level security is configured between the IS and the receiving PCK, the collaboration profile of PartnerA must be configured in the receiving PCK as well, because MLS is activated in the communication channel and configured in the sender agreement.

- Create Party, for example PartnerA.
- Create Service, for example FileService.
- Create a sender Communication Channel of type XI.
  - Select Sender.
  - Select Message Security.
9. Collaboration profile PartnerB

PartnerB is the receiver of the message; the message should be routed to the File adapter.

- Create Party, for example PartnerB.
- Create Service, for example PCK.

The service name must be the same as configured in the Integration Directory.

- Create a receiver Communication Channel of type File Adapter.
  - Select Receiver
  - Configure File Adapter
    - Target Directory
    - File Name Schema
    - Construction Mode
    - File Type
10. Collaboration agreement

The sender agreement is necessary to configure message level security. The receiver agreement assigns the File adapter communication channel to the logical routing.

**Sender agreement**

- **Sender Party**, for example PartnerA.
- **Sender Service**, for example FileService.
- **Interface**: Enter at least an asterisk (*).
- **Namespace**: Enter at least an asterisk (*).
- **Sender Communication**
Channel: Select the XI channel created before, for example From XI.

- Specify the Security Settings, for example Validate
- Certificate for Signature Validation: Select the imported public key certificate of the IS, for example ISmls-cert in Keystore PCKlocal.
- Certification Authority: Select the keystore that contains the trusted root certificate of the certificate used for the signature. In case of self-signed certificates, as used during the example, select the keystore which contains the imported public key certificate of the IS, for example PCKlocal.

Receiver agreement

- Receiver Party: Enter at least an asterisk (*).
- Receiver Service: Enter at least an asterisk (*).
- Interface: Enter at least an asterisk (*).
- Namespace: Enter at least an asterisk (*).
- Sender Party, for example PartnerB.
- Sender Service: PCK
- Receiver Communication Channel: Select the File adapter communication channel created before, for example ToFile.

4.5 References

SAP Exchange Infrastructure
SAP Partner Connectivity Kit

service.sap.com/xi
help.sap.com/nw04 → SAP NetWeaver → Process Integration → SAP Exchange Infrastructure → Runtime
Connectivity → Partner Connectivity Kit

SAP XI Configuration Guide

service.sap.com/instguidesNW04 → Installation → SAP XI

SAP Security Guide

service.sap.com/security → Security in Detail → SAP Security Guides

SAP Security Guide XI


Digital Signatures and Encryption

help.sap.com/nw04 → Security → Digital Signatures and Encryption

Network and Transport Layer Security

help.sap.com/nw04 → Security → Network and Transport Layer Security

SAP Network Integration Guide

service.sap.com/network