SAP Exchange Infrastructure Security Guide

<table>
<thead>
<tr>
<th>Version</th>
<th>Status</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2</td>
<td>reviewed</td>
<td>13-Dec-2002</td>
</tr>
<tr>
<td>1.3</td>
<td>released</td>
<td>31-March-2003</td>
</tr>
<tr>
<td>1.4</td>
<td>updated</td>
<td>09-July-2003</td>
</tr>
</tbody>
</table>
## Contents

1. **Introduction** .......................................................................................................................... 3  
   1.1. Purpose ..................................................................................................................................... 3  
   1.2. Scope ....................................................................................................................................... 3  
   1.3. Glossary .................................................................................................................................. 4  
   1.4. References ................................................................................................................................. 4  

2. **Architecture Overview** ............................................................................................................. 5  
   2.1. Components of an XI Landscape ............................................................................................... 5  
   2.2. Data Exchange ............................................................................................................................ 6  
   2.3. Security Needs ............................................................................................................................ 8  

3. **Authentication and Authorization Concept** ............................................................................. 8  
   3.1. Service Users ............................................................................................................................ 8  
   3.2. Users for Message Exchange ...................................................................................................... 9  
   3.3. Adapters and Service Users ....................................................................................................... 10  
   3.4. Dialog Users ............................................................................................................................. 11  
   3.5. User Data Stores ....................................................................................................................... 11  

4. **Communication** ......................................................................................................................... 12  
   4.1. HTTP and SSL ........................................................................................................................... 12  
   4.1.1. Obtaining Certificates .......................................................................................................... 13  
   4.1.2. Enabling SSL ....................................................................................................................... 13  
   4.2. RFC and SNC ............................................................................................................................ 13  
   4.2.1. Enabling SNC ....................................................................................................................... 13  
   4.3. Network Zones ......................................................................................................................... 13  

5. **Audit** ....................................................................................................................................... 15  

6. **Configuring Security** ............................................................................................................... 16  
   6.1. SAP 6.20 Systems ....................................................................................................................... 16  
   6.2. RFC Adapter .............................................................................................................................. 16  
   6.3. IDoc Adapter .............................................................................................................................. 17  
   6.4. File Adapter ............................................................................................................................... 18  
   6.5. JMS Adapter .............................................................................................................................. 19  
   6.6. JDBC Adapter ............................................................................................................................ 20  
   6.7. SOAP Adapter .......................................................................................................................... 20  
   6.8. Java Proxy ................................................................................................................................. 21
1 Introduction

1.1 Purpose

The SAP Exchange Infrastructure Security Guide explains the security features included in SAP Exchange Infrastructure 2.0 (XI 2.0) and proposes how to apply these features to protect data and to maximize the confidentiality of data passed through the SAP Exchange Infrastructure.

The Security Guide
- describes recommended deployment scenarios
- explains for each component the options for data protection offered by the component
- contains a description of how to configure each component for secure communication to SAP and 3rd party systems.

1.2 Scope

The Security Guide provides a complete picture of XI 2.0 security features. It states the tools that can be used for configuring the various security features. The concrete handling of these tools, however, is not part of this guide. For a detailed description of installation and configuration steps, please refer to [1], [2], and [3] as listed under References below.
1.3 Glossary

CA  Certification Authority
LCR  Landscape Component Repository
RFC  Remote Function Call
SLD  System Landscape Directory
SSL  Secure Sockets Layer
XI  SAP Exchange Infrastructure

1.4 References


[6] Documentation of the Integration Builder as part of the SAP Library online documentation contained on the XI 2.0 documentation CD.

[7] Documentation of the Adapter Engine as part of the SAP Library online documentation contained on the XI 2.0 documentation CD.

2 Architecture Overview

2.1 Components of an XI Landscape

The principle architecture of an XI landscape is depicted in figure 1. An XI landscape may consist of the following components (see also [2]):

- **Integration Server**: An XI 2.0 implementation based on SAP Web AS 6.20. Integration Servers act as a hub for a set of sender and receiver business systems.
- **SAP business systems residing on SAP Web AS 6.20 or higher**: Incorporate an XI 2.0 Integration Engine which enables them to send and receive XML messages in the XI 2.0 message format.
- **SAP business systems residing on SAP Web AS 6.10 or lower**: Do not contain an XI Integration Engine, thus have to communicate with the Integration Server using RFC and IDoc adapters.
- **Business systems connected using a Java proxy**: The Java proxy may be used for Java applications that are to communicate through XI by sender and receiver XML messages.
- **Non-SAP business systems**: Any systems that exchange XML messages using the XI Integration Server. They are connected to the Exchange Infrastructure using technical adapters.
- **RFC and IDoc adapters**: Built-in components of the XI 2.0 Integration Engine. The RFC adapter consists of an ABAP and a Java part. The Java part is typically installed on the Integration Server host.
- **Adapter Engines**: Offer connectivity via files, JDBC, JMS and SOAP. They are typically installed as stand-alone entities, and not on the SAP Web AS.
- **Market Set adapters**: Provide connectivity with SAP Market Set.
- **Integration Repository**: Contains interfaces and mappings available across several landscapes. The Integration Repository runs on the SAP J2EE Engine.
- **Integration Directory**: Contains meta data for a given landscape, such as routing relations, end points and security settings. The Integration Directory runs on the SAP J2EE Engine.
- **System Landscape Directory**: Describes the components that make up the given landscape. The System Landscape Directory runs on the SAP J2EE Engine.
- **Integration Builder**: Comprises a set of user interfaces, implemented as Java clients and Web browser UIs, to be used for designing, configuring and administrating an Exchange Infrastructure.
2.2 Data Exchange

The components of an XI 2.0 landscape communicate with each other for different purposes. The primary purpose of an XI landscape is to enable business systems to exchange XML messages (business documents). This implies communication between business systems and Integration Servers. But communication between components is also necessary to keep XI itself running and up-to-date.

Business Communication

Each business system has an associated Integration Server to which it sends, and from which it receives XML messages. Business systems are described in the SLD. The SLD also contains the information as to which Integration Server is associated with which business system.

Business systems communicate with an Integration Server as follows (see also figure 1):
Direct message exchange using HTTP(S). This is the case if the business system supports the sender and receiver of XML documents using HTTP(S), for example, by using a Java or ABAP proxy.

Communication using adapters. If a business system does not directly support HTTP(S), it connects to the Integration Server using an adapter. Different protocols are used depending on the type of adapter, for example, HTTP, RFC, or JMS.

Technical Communication

In order for messages to be exchanged between business systems, the Exchange Infrastructure components need to communicate with each other at development time, configuration time and runtime (see figure 2).

For example, the content of the Integration Directory (mapping relations, routing relations) controls the behavior of the Integration Engine. For performance and high availability rea-
sons, the directory content is partially cached on the Integration Server. Cache supply and update require the Integration Directory to communicate with the Integration Server.

Furthermore, many XI components need to communicate with the Landscape Component Repository and the System Landscape Directory, as these are the central locations for describing a given XI landscape.

HTTP and RFC protocols are used for this type of technical communication.

### 2.3 Security Needs

As the central infrastructure for exchanging business documents, XI has to make sure that business processes can be executed in a secure manner. Particular security requirements have to be considered if business partners communicate over the Internet. The Internet as a public realm is more susceptible to security attacks than intra-enterprise networks.

XML messages may contain confidential business data. In order to protect them against eavesdropping and unauthorized access, the communication lines as well as the storage locations of XML messages need to be made secure.

In addition to the business data exchanged using XI, the various components of XI need to communicate with each other on a technical level in order to keep the infrastructure running. Security requirements apply to these technical communications as well, because confidential information such as user names and passwords may have to be sent or stored or both.

### 3 Authentication and Authorization Concept

With regard to authentication and authorization, two major scenarios are distinguished between. During design and configuration, *dialog users* communicate with XI using the Integration Builder. At runtime, the participants are computer systems rather than humans. Each system is represented by a dedicated *service user*. All users are SAP standard users.

#### 3.1 Service Users

Service users provide dialog-free access to XI components. They have SAP user roles on the ABAP part of the SAP Web AS that are available on the J2EE part as groups.

General principles for inter-system communication:

*Each XI component that communicates with other XI components identifies itself by means of a dedicated service user.*

*This service user has all the necessary authorizations to access the required services on the addressed XI components.*
Table 1: Service Users Created at Installation Time.

Example

The Integration Directory is associated with service user XIDIRUSER. Since the Integration Directory needs to communicate with the Integration Repository (to obtain interface descriptions), the System Landscape Directory (to obtain physical end point data) and the Integration Server (for the cache update), the user XIDIRUSER needs to be known by each of these components.

The service users in table 1 are automatically created during installation. Name, password and language are defined in the exchange profile. The associated roles are shown in table 2.

3.2 Users for Message Exchange

In general, the message exchange between business systems can be separated into two communication segments that are treated differently from an authentication and authorization point of view:


<table>
<thead>
<tr>
<th>Service User Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP_XI_IR_SERV_USER</td>
<td>User role for the Integration Repository</td>
</tr>
<tr>
<td>SAP_XI_ID_SERV_USER</td>
<td>User role for the Integration Directory</td>
</tr>
<tr>
<td>SAP_XI_APPL_SERV_USER</td>
<td>Generic user role for sender business systems</td>
</tr>
<tr>
<td>SAP_XI_IS_SERV_USER</td>
<td>User role for the Integration Server</td>
</tr>
<tr>
<td>SAP_XI_IRWB_SERV_USER</td>
<td>User role for the Runtime Workbench</td>
</tr>
<tr>
<td>SAP_BC_AI_LANDSCAPE_DB_RFC</td>
<td>User role for the System Landscape Directory</td>
</tr>
</tbody>
</table>

Table 2: Service User Roles.
The sender system is authenticated on the Integration Server by its associated service user. This service user has to be defined on the Integration Server.

2. **Integration Server → Business System.**

   In this case the Integration Server logs on (on behalf of the sender application) to the receiver system. User, password, log-on language as well as authentication method are application-specific and have to be defined in the Integration Builder (Configuration). See [1] and [5] for concepts and configuration in detail.

**Sender Business System → Integration Server**

For the first communication segment, SAP recommends that you define a dedicated service user for each sender business system instead of using the generic user XIAPPLUSER for any business system.

Each service user has to be defined on the Integration Server; it needs the role SAP_XI_APPL_SERV_USER to be able to access the Integration Engine.

On the sender business system, a SM59 destination for this user and the Integration Server has to be created in order to instruct the local integration engine to use the designated service user.

See the chapter Communication and Security in [1] for the detailed configuration steps.

**Integration Server → Receiver Business System**

The Integration Server needs a user with appropriate authorizations to access receiver business systems. These are stored in the Integration Directory as part of end points.

The role SAP_XI_IS_SERV_USER is available in all business systems based on SAP Web AS 6.20 and higher. It provides all authorizations required to access the Integration Engine of the receiver business systems and the ALE entry (integration layer).

Note, however, that no default user is defined with this role, because additional application-specific authorizations will generally be required.

### 3.3 Adapters and Service Users

IDoc, RFC, MarketSet and Plain HTTP adapters are installed on the Integration Server. The receiver (inbound) parts are accessible from business systems by logging in with users that have the role SAP_XI_APPL_SERV_USER. The sender (outbound) parts access the respective business systems as defined in the Integration Directory (end points, no generic user roles).

File, JDBC, JMS and SOAP adapters represent business systems. The sender parts access the Integration Server by logging in with users that have the role SAP_XI_APPL_SERV_USER (XIAPPLUSER). The receiver parts are accessible from the Integration Server as defined in the Integration Directory (end points, no generic user roles).
### Table 3: Dialog User Roles

<table>
<thead>
<tr>
<th>Dialog User Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP_XI_DISPLAY_USER</td>
<td>Read-only access to Integration Directory and Repository</td>
</tr>
<tr>
<td>SAP_XI_DEVELOPER</td>
<td>Design and development of business processes</td>
</tr>
<tr>
<td>SAP_XI_CONFIGURATOR</td>
<td>Configuration of business integration content</td>
</tr>
<tr>
<td>SAP_XI_CONTENT_ORGANIZER</td>
<td>Maintaining the content of the System Landscape Directory</td>
</tr>
<tr>
<td>SAP_XI_MONITOR</td>
<td>Monitoring of XI components</td>
</tr>
<tr>
<td>SAP_XI_ADMINISTRATOR</td>
<td>Technical configuration and administration of XI</td>
</tr>
</tbody>
</table>

#### 3.4 Dialog Users

Dialog users represent *human* users (as opposed to service users) that log-on through the various UIs of the Integration Builder. As with service users, dialog users are generally maintained in the ABAP part of the SAP Web AS.

The roles in table 3 for the different dialog users are predefined and shipped. See [1] for a more detailed description. Each role implies at least display authorizations for all XI components.

#### 3.5 User Data Stores

Users that are needed by XI components running on a SAP Web AS are in general maintained on the ABAP part of this SAP Web AS. This applies both to service users and dialog users. For instance, if you want a user MILLER to be entitled to define interfaces, you have to create this user on the ABAP part of the SAP Web AS on which the Integration Repository is deployed, and assign the role SAP_XI_DEVELOPER to this user. After logging on to the Integration Builder (which is implemented in Java), the J2EE part of the SAP Web AS authenticates user MILLER against the ABAP part.

By relying on the proven user administration of SAP Web AS, all basis tools and solutions that have emerged around this user administration over years, are immediately available for XI users as well.

General principle for user administration:

> *Each XI component that resides on an SAP Web AS refers to the user management of the ABAP part of this SAP Web AS. XI Java applications running on an SAP Web AS authenticate against the users maintained in the ABAP part.*

There are two exceptions to this rule in which SAP user administration cannot be used:

- **Stand-alone components.** For XI components that do *not* reside on a SAP Web AS, for example, stand-alone adapters or stand-alone Java applications based on
the XI Java proxy, user information is kept in property files. Although sensitive data such as passwords are stored in an obfuscated form, SAP recommends that you also secure these property files by using the functions of your operating system.

- **Users for logging on to receiver systems.** In order to deliver an XML message to a receiver business system, the Integration Server has to log on to the receiver system. The Integration Directory informs the Integration Server about which user and password to use for logging on (see also chapter 3.2). Back-end users are kept in the database of the Integration Directory and are occasionally transferred to the directory cache of the Integration Server (see also figure 2). Confidential data such as passwords are stored obfuscated both in the directory database and in the persistent cache on the Integration Server. In order to also secure the communication between the directory and the Integration Server, SAP recommends that you configure SNC for this communication¹.

### 4 Communication

Depending on the protocol used, all data (including passwords) is usually transmitted through the network (intra/internet) in plain text. To maintain the confidentiality of this data, you can apply transport layer encryption to the connection between the business systems, the Integration Server, the adapters, and the Web browser. SAP especially recommends using encryption when you transmit passwords, orders, company-specific information or any other data that you consider sensitive.

You can use SSL or SNC to increase the security of the following connections:

- Between adapters and Integration Server
- Between business systems and Integration Server
- Between business systems and adapters

Adapters, business systems, and Integration Servers communicate with each other using the RFC or HTTP protocols, which can be secured by SNC or SSL respectively.

#### 4.1 HTTP and SSL

All XI components using the HTTP protocol support the encryption of the HTTP data stream by means of the Secure Sockets Layer protocol (SSL), also known as HTTPS. HTTPS data streams are completely transparent to the Exchange Infrastructure.

In order to use SSL encryption, each server component supporting SSL must obtain an X.509 certificate that has been issued by a Certification Authority (CA). The server certificate is used to authenticate the server. If the HTTP client receives a server certificate issued by a trusted CA, then the client can verify that it is connected to the intended server.

---

¹ The directory server and the Integration Server communicate using the RFC protocol.
4.1.1 Obtaining Certificates

Server certificates are issued by a company internal Certificate Authority, or by a CA such as Thawte, Verisign, TC Trustcenter and so on. SAP customers can also obtain server certificates from the SAP Trustcenter Service [http://service.sap.com/tcs](http://service.sap.com/tcs).

4.1.2 Enabling SSL

To enable HTTPS for the server, a certificate must be installed on the server. For instructions on how to install the certificates and on how to activate SSL, see the following documents:

- Configuring the SAP Web AS for Using SSL [5]

4.2 RFC and SNC

All connections between SAP system components that communicate using RFC can be secured with SNC, which secures the data communication paths between the various SAP system components. There are well-known cryptographic algorithms that have been implemented by the external security products supported by SAP systems. With SNC, you can apply these algorithms to your data for increased protection. SNC supports three levels of security protection: authentication only, integrity protection, and confidentiality protection.

4.2.1 Enabling SNC

To enable SNC for the RFC adapter and SAP R/3 systems, a certificate must be installed on the server. For instructions on how to install the certificates and on how to activate SNC see the following documents:


4.3 Network Zones

The SAP Exchange Infrastructure is implemented as client-server frameworks using HTTP to exchange business documents between business systems. To connect the business systems, adapters (i.e. File adapter, JMS adapter) for sender or receiver documents to other systems are used.

The partners exchanging business documents can use firewalls to establish different network zones with different levels of security. These network zones use firewalls to shield a business system, which contains sensitive information, by allowing only connections between a defined set of servers and disallowing any other connection.
Application-level gateways or proxies implement application-dependent protocols such as HTTP and transfer data between networks (for example, between internal and external networks).

SAP highly recommends that you install your business system and adapters in a trusted network zone (server LAN) and not to place them in the DMZ since the configuration files of the adapters may contain sensitive information (names of service users, scrambled passwords). This is indicated in the figure 3. The installation uses two different network zones. Data is exchanged between these network zones using the HTTP protocol (possibly with SSL). Business systems on the left connect to an adapter (i.e. JMS adapter). The adapter and the business system may be placed in a separate network zone (see figure 4).
The adapters may connect to an HTTP proxy for outgoing connections, to send requests via a reverse proxy (i.e. SAP Web Dispatcher) to the Integration Server. The Integration Server is placed in the server LAN and connects to one or more business systems. Depending on the security needs, the business systems may be placed in another network zone. Refer to the recommendations given in the SAP Security Guide [4] and Web Infrastructure Concepts for SAP Web Application Server [8] for the protection of the Integration Server and the business systems themselves.

5 Audit

Auditors must be able to analyze and track the messages that have been processed by SAP Exchange Infrastructure. Business processes that include booking events are typically implemented using asynchronous messages. SAP Exchange Infrastructure persists asynchronous messages and allows you to mark messages that have been correctly processed for deletion or archiving. Faulty messages are never automatically deleted by the system, but only manually by administrators. Synchronous messages are never persisted within XI and have to be audited by the applications involved.

To archive XML messages, you first have to define the interfaces of the messages you want to archive, and then schedule the archiving jobs.

Multiple jobs have to be executed to archive XML messages:

- Preparation job: Determines messages to be archived
- Archiving job: Writes messages to archive
- Deletion job: Remove messages from persistence layer (database) of the Integration Engine

Two jobs have to run to delete messages:

- Determine messages to be deleted
- Delete archived messages from the database

You can reschedule all jobs periodically, but you should maintain the job sequence.

See transaction SXMB_ADM and the corresponding online documentation for a detailed description of how to configure the archiving of messages.

Using transaction SXMB_MONI, you can select and display archived XML messages. There are two ways you can search for archived XML messages:

- using an archive
- using a message GUID

In both cases the system displays a list of archived XML messages. You can switch from the list to display individual archived XML messages or to compare message versions.

See transaction SXMB_MONI and the corresponding online documentation for a more detailed description of how to select and display archived messages.
6 Configuring Security

This chapter describes the configuration steps for establishing secure communication between business systems and the relevant Integration Server. A business system either communicates directly with the SAP Exchange Infrastructure or indirectly by means of adapters. The following sections describe how to configure secure communication for the different connection types.

6.1 SAP 6.20 Systems

Purpose

Exchange data between SAP 6.20 systems. Requires that the business system runs on SAP Web AS release 6.20 or higher.

Supported Protocols/APIs

HTTP, HTTPS to and from the Integration Server

Maintained User Accounts

- From Business System to Integration Server: Service user dedicated to the business system has to be maintained. The credentials of the service user are stored inside a destination on the sender business system. Tool for user maintenance: Transaction SM59, or the connection wizard of the Runtime Workbench
- From Integration Server to Business System: The users for logging on to a business system can be configured for each message interface. The credentials of these users are stored in the Integration Directory. Tool for user maintenance: Integration Builder.

Recommendation

Use HTTPS to avoid eavesdropping of passwords or other confidential information that may be part of your messages.

Configuration of HTTPS

- Enable SSL for the SAP Web AS running the Integration Server and the business system. See note 510007 and the document SAP Web Application Server Security (Release 6.20) [5].
- Configure the destinations on the business system and the end points in the Integration Builder to use SSL.
- See Configuration Guide – SAP Exchange Infrastructure 2.0 [1]

6.2 RFC Adapter

Purpose

Route RFCs from existing SAP applications through the Exchange Infrastructure.

Supported Protocols/APIs
RFC, SNC to and from the Integration Server.

Maintained User Accounts

- **From RFC Adapter (Java Part) to Integration Server**: Service user has to be maintained in the configuration file of the RFC adapter. Passwords are stored in an obfuscated form on the file system. Tool for user maintenance: Configuration UI of Adapter Engine.

- **From RFC Adapter (Java Part) to Receiver System**: The users for logging on to a business system can be configured for each message interface. The credentials of these users are stored in the Integration Directory. Tool for user maintenance: Integration Builder.

- **User for Reading Metadata from Sender System**: This user has to be maintained in the configuration file of the RFC adapter. To retrieve the necessary information from the SAP Data Dictionary, the RFC adapter needs to call a number of remote function modules, for which the access rights have to be granted.

- **User for Reading Metadata from Receiver System**: This user has to be maintained in the configuration file of the RFC adapter, and needs authorizations to read metadata from this system.

Recommendation

Use SNC to avoid eavesdropping of passwords or other confidential information that may be part of your messages.

Configuration of SNC

- Enable SNC for the SAP systems running the Integration Server and the business system. See document *SAP Web Application Server Security (Release 6.20)* [5].

- Configure the SNC options of the used destination on the sender system by means of transaction SM59. The security name of the user under which the RFC adapter is running has to be entered as a partner.

- Activate SNC for the inbound connections of the RFC adapter in the configuration file. See document *Configuration Guide – SAP Exchange Infrastructure 2.0, chapter 10* [1].

- In the Integration Builder, configure end points to use SNC authentication.

- See *Configuration Guide – SAP Exchange Infrastructure 2.0, chapter 6* [1].

### 6.3 IDoc Adapter

**Purpose**

Route IDocs from existing SAP applications through the Exchange Infrastructure.

**Supported Protocols/APIs**

RFC, SNC to and from the Integration Server.

**Maintained User Accounts**
From Sender System to IDoc Adapter: User for logging on to the Integration Server has to be maintained with the RFC destinations used for sender IDocs to the Integration Server: Tool for user maintenance: Transaction SM59.

From IDOC Adapter to Receiver System: Users for logging on to the receiver system have to be maintained with RFC destinations on the Integration Server that are to be used by the outbound part of the IDoc adapter. These destinations have to be assigned to end points in the Integration Builder. Tools for user maintenance: Transaction SM59 and Integration Builder.

Recommendation

Use SNC to avoid eavesdropping of passwords or other confidential information that may be part of your messages.

Configuration of SNC

- Enable SNC for the SAP systems running the Integration Server and the business system. See document SAP Web Application Server Security (Release 6.20) [5].
- Configure the SNC options of the destination used for IDoc communication on the sender system and on the Integration Server by means of transaction SM59.
- See Configuration Guide – SAP Exchange Infrastructure 2.0, chapter 6 [1].

6.4 File Adapter

Purpose

The File adapter is used to exchange data with other systems using files.

Supported Protocols/APIs

HTTP, HTTPS to and from Integration Server.

Maintained User Accounts:

- From Integration Server to File Adapter. The users for logging on to an adapter are defined and assigned to an adapter end point in the Integration Builder. In the Integration Directory, the credentials of theses users are stored on a database in a secure store. This user data also has to be maintained with the file adapter in the configuration file of the Adapter Engine. Passwords can be optionally stored in an obfuscated manner. The configuration file must only be accessible to the operating user running the adapter process.
  Tools for user maintenance:
  - Integration Builder
  - Configuration UI of the Adapter Engine
- From File Adapter to Integration Server. The user for logging on to the Integration Server can be defined for each adapter module, in other words a dedicated user can be defined for each instance of the File adapter. The credentials of theses us-

---

Note: The IDoc adapter is a built-in part of the Integration Server.
ers are stored in the configuration file of the Adapter Engine. They can also be obfuscated if required.

Tools for user maintenance:
- Transaction SU01 on the Integration Server
- Configuration UI of the Adapter Engine

Recommendation

Use HTTPS for communication between the Integration Server and the adapter. Ensure that only the operating system user running the adapter process is able to read the properties file with the obfuscated credentials. The same applies for the data file sent to or received from the Integration Server.

Configuration

- Enable SSL for the adapter as described in [1], [7].
- Enable SSL for the SAP Web AS running the Integration Server. See note 510007 and [4].
- Protect the properties file. Ensure that it can only be read by the operating system user running the adapter\(^3\) (use chmod 600 under Unix; use the Properties/Security tab page to set permissions under Windows).
- Set the access rights for the directories used for data exchange so only the operating system user running the adapter can access the files in the directory.
- See document *Adapter Engine Configuration* [7]

### 6.5 JMS Adapter

**Purpose**

The JMS adapter connects the Integration Server to a messaging system using the JMS interface.

**Supported Protocols/APIs**

HTTP, HTTPS to and from the Integration Server.

JMS to the messaging system.

**Maintained User Accounts**

- *For Communication with the Integration Server*: As for the File adapter, see chapter 6.4.
- *For Communication with the Messaging System*: For logging on to the messaging system, user credentials can be maintained in the configuration file of the Adapter Engine. They can also be obfuscated if required.

\(^3\) Under Unix use chmod 600; under Windows use the Properties/Security tab page to set the permissions.
Recommendation

Use HTTPS for communication between the Integration Server and the adapter. Ensure that only the operating system user running the adapter process can access the properties file with the obfuscated credentials.

Note: If possible, the connection between the JMS server and the adapter should also be encrypted if this is supported by the JMS client library. This depends on the messaging provider and client library used and is not part of this guide.

Configuration

As for the File adapter, see chapter 6.4.

6.6 JDBC Adapter

Purpose

The JDBC adapter connects the Integration Server to a database server using the JDBC interface.

Supported Protocols/APIs

HTTP, HTTPS to and from the Integration Server.

JDBC to the database.

Maintained User Accounts

For Communication with Integration Server: As for the File adapter, see chapter 6.4.

Database User: The credentials for the database are stored in the adapter configuration file and can also be obfuscated if required.

Recommendation

As for the File adapter, see chapter 6.4.

Configuration

As for the File adapter, see chapter 6.4.

6.7 SOAP Adapter

Purpose

The SOAP adapter enables communication with clients and providers of Web Services.

Supported Protocols/APIs

HTTP, HTTPS to and from the Integration Server.

Maintained User Accounts

For Communication with Integration Server: As for the File adapter, see chapter 6.4.
For Communication with Web Service Client or Provider: For logging on to the Web service provider, user credentials can be maintained in the configuration file of the Adapter Engine. They can also be obfuscated if required.

Recommendation

Use HTTPS for communication between the Integration Server and the adapter, as well as between the adapter and the Web service client or provider. Ensure that only the operating system user running the adapter process can access the properties file with the obfuscated credentials.

Configuration

As for the File adapter, see chapter 6.4.

6.8 Java Proxy

Purpose

A Java proxy enables applications written in Java to be connected to SAP Exchange Infrastructure.

Supported Protocols/APIs

- HTTP to and from the Integration Server.
- HTTPS to the Integration Server.
- HTTPS as client if the application runs on the SAP Web AS (J2EE stack).

Maintained User Accounts

- From Java Proxy to Integration Server: The user for logging on to the Integration Server is defined in the exchange profile. The credentials are kept in the properties
  
  com.sap.aii.applicationsystem.serviceuser.name
  com.sap.aii.applicationsystem.serviceuser.pwd

- From Integration Server to Java Proxy: The user for logging on to the Java proxy has to be maintained in the Integration Directory as part of an end point definition (tool: Integration Builder). The application may implement authorization checks for these users.

Recommendation

Use HTTPS for communication between the Integration Server and the Java proxy. Ensure that only the operating system user running the adapter process can access the properties file with the obfuscated credentials.

Configuration

- If the Java application runs on SAP Web AS: Enable SSL for the SAP Web AS running the Integration Server. See note 510007 and [4].
- Protect the properties file. Ensure that it can only be read by the operating system user running the application.
- See the online documentation for the Java Proxy Runtime.