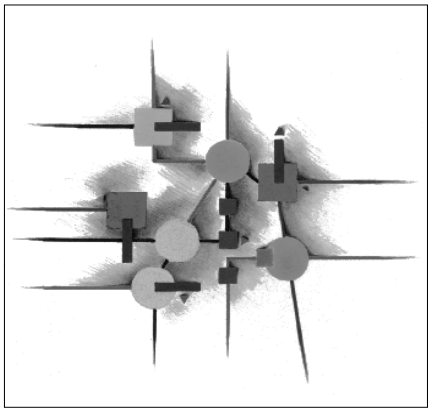
SAP Business Connector Certificate Toolkit Guide



SAP System

Release 4.8

SAP AG - Dietmar-Hopp-Allee 16 - D69190 Walldorf

Copyright

Contents

1

Introduction

Welcome!

This guide describes how to install and use the SAP BC Certificate Toolkit. It contains information for administrators and developers of SAP products about creating and managing digital certificates for use with SAP products.

To use this guide effectively, you should understand the basic concepts described in the *SAP BC Administration Guide* and the *SAP BC Developer Guide*.

Typographical Conventions

This document uses the following typographical conventions:

Convention	Example
Procedures are designated by a blue box in the left column. Procedures are presented as a series of numbered steps.	1 On the **Activity** menu, click **File**.
Terms that identify elements, options, selections, and commands on the screen are shown in bold.	The **Service** field on the **Properties** tab specifies the name of the requested service.
Characters that you must type exactly are shown in a typewriter font.	Type: `setup` and then press ENTER.
Variable information that you must type based on your specific situation or environment is shown in italics.	Type: <*sapbc*>`\setup` and then press ENTER.
Keyboard keys are shown in uppercase.	Press ENTER; then press TAB.
Keys that you must press simultaneously are joined with the "+" symbol.	Press CTRL+ALT+M.
Directory paths are shown with the "\" directory delimiter unless the subject is Linux-specific. In these cases, the "/" is used. If you are working in a Linux environment, substitute a "/" for the "\" shown in the procedures in this book.	<*sapbc*>\server\packages\Default

Convention	Example
Information that you must read before beginning a procedure or that alerts you to negative consequences of certain actions is denoted using this notation.	 **Important!** If the folder is not already open in the Service Browser, open it before you start the following procedure.
Notes that provide related, but non-critical, information are denoted using this notation.	 **Note:** When you start SAP BC Developer, you are prompted to log on to a SAP BC Server.
Helpful information such as shortcuts and alternatives.	 **Tip!** You can also use CTRL+C to copy an object.

Program Code Conventions

For programming code and command syntax, this document uses the following typographical conventions:

Convention	Example
Keywords and values that you must type exactly as printed are shown in typewriter font.	`%CoSymbol%`
Variable values or parameters that you must supply are shown in italics.	`%`*`VarName`*`%`
Keywords or values that are optional are enclosed in [ ]. Do not type the [ ] symbols in your own code.	`%loop` *`LoopVar`* `[null=`*`NullValue`*`]%`

Related Documentation

The following documents are companions to this guide. Some documents are in PDF format and others are in HTML.

Refer to this book...	For...
SAP BC Administration Guide	Information about using the Server Administrator to configure, monitor, and control the SAP BC Server. This book is for server administrators. You will find this book at: <*sapbc*>\server\doc\SAPBCAdministrationGuide.pdf
SAP BC Developer Guide	Information about creating and testing services and client applications. This book is for solution developers. You will find this book at: <*sapbc*>\developer\doc\SAPBCDeveloperGuide.pdf
SAP BC Built-In Services Guide	Descriptions of services that are installed on your SAP BC Server. This book for is for solution developers. You will find this book at: <*sapbc*>\developer\doc\SAPBCBuiltInServicesGuide.pdf
Building Output Templates and DSPs	Information about creating output templates and Dynamic Server Pages (DSPs). This reference is for solution developers. You will find this book at: <*sapbc*>\developer\doc\SAPBCTemplatesAndDSPs.pdf
SAP BC Java API Reference	Descriptions of the Java classes you use to create services. This reference is for developers who build services using Java. You will find this book at: <*sapbc*>\server\doc\api\Java\index.html
SAP BC Administrator's Online Reference	Information about the controls in the SAP BC Server Administrator screens and step-by-step procedures describing how to perform tasks with the Server Administrator. You can access the online reference by clicking the Help tab on a Server Administrator screen.

Refer to this book...	For...
Developer Online Reference	Information about the controls in the SAP BC Server application windows and step-by-step procedures describing how to perform tasks with the SAP BC Server. You can access the online reference by clicking **Help** in an application window or dialog box.

Viewing this Document

To view this document, which is in PDF format, you must have Acrobat Reader™ 4.0 or later installed on your system. If you have an earlier version of Acrobat Reader, you will receive the following error message when you open this document and Acrobat Reader will not display the images in this document:

```
Could not find the ColorSpace named 'Cs8.'
```

If you do not have this software or you do not have the correct version, you can download a free copy from:

http://www.adobe.com/downloads.

Printing this Guide

To produce a hard copy of this guide, print this document from Acrobat Reader.

2

Overview of the SAP BC Certificate Toolkit

What Is the Certificate Toolkit?

The SAP BC Certificate Toolkit is a utility you can use to easily create a digital certificate for your SAP BC Server.

The digital certificate, used during Secure Sockets Layer (SSL) communications, helps ensure that communications between your SAP BC Server and clients are secure. When the server and a client communicate, the server presents its certificate to the client. The certificate attests to the identity of your server. In other words, the client can be sure it is communicating with your organization.

Obtaining the digital certificate is just one step in making communications with your SAP BC Server secure. Once you have obtained a digital certificate for your SAP BC Server, you must configure your SAP BC Server to use SSL. Instructions for doing so are provided in "Managing Server Security" in the *SAP BC Administration Guide*.

In addition, you can control access to the SAP BC Server through access control lists, listening ports, client authentication, and NT Challenge/Response. For a more in-depth explanation of securing your SAP BC Server, refer to "Managing Server Security" in the *SAP BC Administration Guide*.

Starting the Certificate Toolkit

The Certificate Toolkit must be running in order for you to create a digital certificate for your SAP BC Server.

To start theSAP BC Certificate Toolkit on Windows

1 Locate the SAP BC folder on the Programs menu.

2 Click the SAP Business Connector Certificate Toolkit icon.

To start the SAP BC Certificate Toolkit on Linux

1 Locate the ssltoolkit.sh script file that was modified for your environment when you installed the toolkit with SAP BC Developer.

2 Execute this script running an X-Windows environment.

Note: Run this script when logged in as a non-root user. Running the script as root might reduce the security of your system. If you are running a Windows system, do not run this command when logged in as an administrator.

To start the SAP BC Certificate Toolkit from the command-line

1. At a command-line, type the following command to switch to the CertToolkit directory:

   `cd <sapbc>\Developer\certkit`

2. Type the following command to start the toolkit:

   For Windows: `bin\ssltoolkit.bat`

   For Linux: `bin/ssltoolkit.sh`

3

Obtaining a Digital Certificate for the SAP BC Server

Overview

This chapter describes the steps you must follow to set up a digital certificate for your SAP BC Server. The chapter has two parts:

- "Generating a Certificate Signing Request and Sending It to the Certificate Authority"—In this section you use the Certificate Toolkit to generate a Certificate Signing Request and send the request to a Certificate Authority.
- "Saving Your Certificate"—In this section you obtain your certificate and use the Certificate Toolkit to make it available to your SAP BC Server. If necessary, the Certificate Toolkit converts the certificate to Distinguished Encoding Rules (DER) format, which the SAP BC Server requires.

Generating a Certificate Signing Request and Sending It to the Certificate Authority

The following procedure describes how to use the SAP BC Certificate Toolkit to create your private key and a Certificate Signing Request (CSR) and send your request to your Certificate Authority (CA).

Step	Description
Step 1	Generate the private key.
Step 2	Generate the Certificate Signing Request.
Step 3	Send your request to the Certificate Authority.
Step 4	Wait for the response; check with your Certificate Authority on the status of your request.

Step 1 Generating a Private Key

1 Start the Certificate Toolkit.

2 From the **Certificate Toolkit** menu, select **Generate a private key** and click **Next**.

3 From the Generate a Private Key screen, specify the following:

For this parameter...	Specify...
Key size	A key size or accept the default of 1024. 2048 is more secure than 1024, but might slow processing. Use 1024 for ordinary transactions and 2048 for high-value transactions.
Algorithm	The SAP BC Certificate Toolkit uses the RSA Public-Key algorithm.
Enter file name	Name of the file that you want to hold the private key you are about to create. Specifying the file name is mandatory for the private key generation.
Select a location for private key	The directory path of the file to which you want the toolkit to write your server's private key.

4 Click Next.

Note: Depending on your machine and the key size you selected, key generation can take several minutes.

When the Certificate Toolkit has successfully generated the key, a dialog displays stating the key has been generated. Click OK.

The Create a Certificate Signing Request (CSR) including the Public Key screen displays. If you want to continue and create the CSR, follow the instructions under "Generate the Certificate Signing Request" below. If you do not want to create the request now, click Back to return to the Certificate Toolkit menu.

Note: In the next step, the toolkit creates a *public* key from the private key just created.

Step 2 Generating the Certificate Signing Request

1 If it is not already started, start the Certificate Toolkit and select Generate a Certificate Signing Request (CSR) including Public Key. See "Starting the Certificate Toolkit" on page 12 for instructions.

2 Specify the following information.

For this parameter...	Specify...
Select the file that contains the private key	The directory path and file name of the file that contains the private key you created earlier.

For this parameter...	Specify...
Enter CSR file name	The name of the file to which the Certificate Toolkit is to write the request. Later, you will send the information in this file to your CA. The toolkit uses the PEM encoding format (creates header information that includes the version number and the encryption algorithm used to encrypt the private key) and adds `pem` as the file extension. For example, if you specify `csrfile`, the toolkit names the file `csrfile.pem`.

Note: The toolkit creates a *public* key from the private key you created earlier. The toolkit attaches the public key to the certificate Id information (name, organization, etc.) and sends it as part of the Certificate Signing Request.

3 In the Server Information portion of the screen, specify the following information:

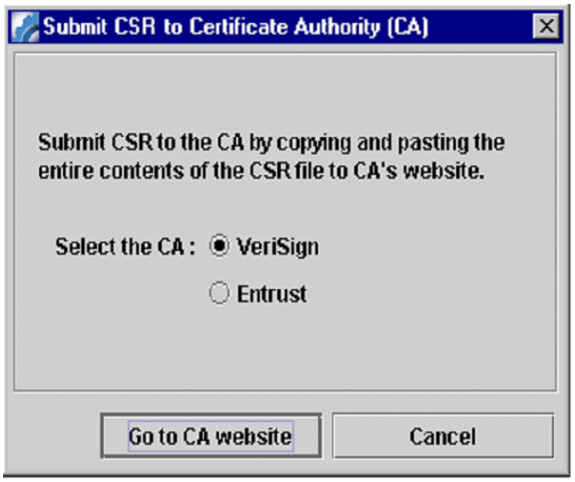
For this parameter...	Specify...
Host name	Name of the host server on which the certificate will reside, for example, BusinessConnector.yourcompany.com.
Department	Your department within your company or organization. This field is optional.
Organization	Your company or organization.
City	City in which your company is physically located.
State	State in which your company is physically located. For example, if your company is incorporated in Delaware but located in California, specify California. This field is optional.
Country	Country in which your company is physically located.
Contact E-Mail	E-mail address of the person to receive the response from the CA.
Revocation Password	A password you can give to your CA later if you decide to revoke your certificate. For example, if you think someone has stolen your private key, you must supply this password to your CA before they can revoke your certificate. This field is optional.

4 Click Next.

After the toolkit has successfully created your CSR, it displays a dialog to that effect.

5 Click OK.

The toolkit displays the following dialog:



6 Select VeriSign or Entrust and click Go to CA website.

If you want to use a different CA, click Cancel to go back to the toolkit menu, then Exit to exit the toolkit. Use the method required by your CA to submit your CSR to them.

Step 3 Sending the Certificate Signing Request to the CA

The method you use to send your CSR to the CA depends on your CA. If you just used the Certificate Toolkit to create a CSR and chose VeriSign or Entrust as your CA, you will be at VeriSign's or Entrust's website and will be asked to copy your CSR from the file it is stored in and paste it into a field on the website. Other CAs might have you send the request in an e-mail.

When you have finished submitting your request, you are returned to the Certificate Toolkit.

After your CA approves your request (this can take an hour for a test certificate or a number of days for a permanent certificate) they will send you a response. The form of the response depends on the CA, but typically they will send it in an e-mail or they will require you to go to their website and obtain the response from there.

Step 4 Waiting for a Response and Checking the Status

Typically the CA will give you a PIN and a link to Web site so that you can check the status of your request. Monitor the status periodically. If the request seems to be taking too long, contact your CA.

Saving Your Certificate

Eventually, your CA will send you a response, either through e-mail or their website. The response might contain just your digital certificate with your public key, or it could contain a chain of certificates consisting of your certificate (with your public key) and the CA's own certificate. Typically, you will copy the response to a file of your choice, for example `Certificate.txt`.

The following procedure describes how to install the certificate or certificates on your SAP BC Server.

Note: The toolkit automatically converts certificates that are in a non-DER format to DER format.

Making the Certificates Available to Your SAP BC Server

1 Start the Certificate Toolkit. See "Starting the Certificate Toolkit" on page 12 for instructions.

2 Select Convert and Save Certificates for use with SAP Business Connector.

3 Supply the following information:

For this parameter...	Specify...
Select the file that contains the CA's response	The directory path and name of the file that contains the response from the CA.

4 Click Next.

5 Enter information in the following fields:

For this parameter...	Specify...
Enter certificate file name	Name of the file to which you want the toolkit to write the converted version of your server's certificate, for example: `MyServerCert`. The toolkit automatically appends the `der` extension.
Select a location for the certificate	The directory path of the file to which you want the toolkit to write your server's certificate. Make sure the directory is in a location the SAP BC Server can access, such as <*sapbc*>\server\config

If the CA's response contains their certificate as well, you will see these fields:

For this parameter…	Specify…
Enter CA certificate file name	The name of the file to which you want the toolkit to write the converted version of the CA's digitial certificate. Typically you will have a directory set aside just for CA certificates.
Select a location for the CA's certificate	The directory path of the file to which you want the SAP BC Certificate Toolkit to write the converted version of the CA's certificate. Make sure the directory is in a location the SAP BC Server can access, such as <*sapbc*>\server\config.

6 Click OK.

If you did not receive the CA's certificate, see "What to Do if the Certificate Authority Does Not Send You Their Own Certificate" below.

Now you are ready to configure your SAP BC Server to use SSL. Refer to the section "Configuring the Server to Use SSL" in the chapter "Managing Server Security" in the *SAP BC Administration Guide*.

What to Do if the Certificate Authority Does Not Send You Their Own Certificate

Sometimes a CA will send a signed version of the certificate for your Business Connector without including a copy of the CA's certificate. You need a copy of the CA's certificate to ensure secure communication; therefore if you did not receive one, try one of the following methods to obtain one:

- Contact the Certificate Authority—some Certificate Authorities allow you to copy their certificate from their website. If that option is not available, get in touch with your CA through their website, e-mail, or by phone and ask them to send you the certificate.
- Export it from your browser—most Web browsers that support SSL are shipped with the certificates of well-known Certificate Authorities. Some browsers provide a method for you to export the certificate from the browser to a file. The method you use to obtain the certificate depends on your browser.
- Import it from the SAP BC Server's certificate—You might be able to obtain the CA's certificate by following the certificate path from your Business Connector's certificate. On a Windows machine, double click your converted certificate file, for example `certificate.der`. Select the Certification Path tab. If the CA certificate is available, it will appear above your certificate in the path. Double click this certificate entry and select the Details tab. There you can copy the CA certificate to a file with the der extension, for example `cacert.der`. Place the file in the directory where you store CA certificates for the Business Connector.

Index

T

V

W