SAP Custom Development

SAP Corporate Connectivity for Banking

Security Configuration information

Version	Status	Date
1.0	Customer	January 25, 2013

Customer



© 2013 SAP AG

Dietmar-Hopp-Allee 16 D-69190 Walldorf



Typographic Conventions

Type Style	Description
Example Text	Words or characters quoted from the screen. These include field names, screen titles, pushbuttons labels, menu names, menu paths, and menu options. Cross-references to other documentation
Example text	Emphasized words or phrases in body text, graphic titles, and table titles
EXAMPLE TEXT	Technical names of system objects. These include report names, program names, transaction codes, table names, and key concepts of a programming language when they are surrounded by body text, for example, SELECT and INCLUDE.
Example text	Output on the screen. This includes file and directory

Icons

lcon	Meaning
\mathbb{A}	Caution
~ <u>~</u>	Example
	Note
	Recommendation
$\langle \rangle$	Syntax

Additional icons are used in SAP Library documentation to help you identify different types of information at a glance. For more information, see *Help on Help* \rightarrow *General Information Classes and Information Classes for Business Information Warehouse* on the first page of any version of *SAP Library*.

names and their paths,

- **Example text** Exact user entry. These are words or characters that you enter in the system exactly as they appear in the documentation.
- <Example Variable user entry. Angle
 text> brackets indicate that you
 replace these words and
 characters with appropriate
 entries to make entries in the
 system.
- EXAMPLE TEXT Keys on the keyboard, for example, F2 or ENTER.

© 2013 SAP AG	Title: SAP Corporate Connectivity for Banking	Page 2 of 23
Dietmar-Hopp-Allee 16	Version: 1.0	
D-69190 Walldorf	Date: January 25, 2013	



Contents

1	Orga	Organization4			
	1.1	Document Administration	.4		
	1.1.1	Authors	.4		
	1.1.2	History	.4		
	1.1.3	Intended Audience	. 4		
	1.1.4	Related Documentation	. 4		
	1.2	Purpose and Scope	. 4		
	1.3	Glossary	. 5		
2	Use	r Administration and Authorization	.5		
	2.1	Authorization Object for the Payment Cockpit	. 5		
3	Cert	ificate Implementation	.6		
	3.1	Overview	. 6		
	3.2	Security Mechanisms	. 6		
	3.3	Step-by-Step Instructions	. 6		
	3.3.1	Transaction STRUST	. 6		
	3.3.2	Certificates Used – Scenario Information	. 8		
	3.3.3	Security Configurations in the Customer's ERP	. 9		

3.3.4	Steps after Certificate-Installation in SAP ERP	15
3.4	Generic Steps – Creating a PSE (If required)	16
3.5	Installing a Root Certificate – Generic Procedure	20
_		

4	Security Issues	23
---	-----------------	----

© 2013 SAP AG	Title: SAP Corporate Connectivity for Banking	Page 3 of 23
Dietmar-Hopp-Allee 16	Version: 1.0	
D-69190 Walldorf	Date: January 25, 2013	



1 Organization

1.1 Document Administration

1.1.1 Authors

Name	Company	Project Role or Comment
Vivek Vishal	SAP Custom Development	Author
Viswanath Natesan	SAP Custom Development	Reviewer

1.1.2 History

Date	Version	Chapter	Name	Change/Enhancement	Agreed with
07/12/2012	0.1.0	All	Vivek Vishal	Document Created	Viswanath Natesan

1.1.3 Intended Audience

This document is intended for persons in the following roles:

- Primary audience:
 - System administrators
 - Technology and security consultants
- Secondary audience:

 Support consultants
 - Functional consultants
 - Partners and customers

1.1.4 Related Documentation

- Configuration Guide
- Corporate ERP Connectivity Guide
- SAP Solution Manager

1.2 Purpose and Scope

The purpose of this document is to describe the security configurations that are required for enabling a reliable and secure certificate-based asynchronous communication between *Westpac Bank's (the bank')* landscape and the customer's landscape. Integration between standard programs or components on the ERP side on the one hand, and, the bank's PI system, and further, to the bank's system on the other, is channeled through this secure communication path across the communicating landscape.

This security information document provides a central starting point for the technical implementation of the security standards and configurations as a part of SAP Corporate Connectivity for Banking Westpac solution (the solution).

© 2013 SAP AG	Title: SAP Corporate Connectivity for Banking	Page 4 of 23
Dietmar-Hopp-Allee 16	Version: 1.0	
D-69190 Walldorf	Date: January 25, 2013	



1.3 Glossary

Term	Definition
Web service	Web services are self-contained application functions that can be processed through open standards.
Endpoint	An Endpoint, identified by its address, is a location, from where, a service that is associated with the binding of a specific interface, can be accessed.
Certificate	An electronic "identity card" that establishes a user's credentials when doing business or other transactions on the Web. It is issued by a Certification Authority (CA) and contains name, serial number, expiration date, a copy of the certificate holder's public key (used for encrypting and decrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real.
CA	An external instance that issues public-key certificates. The Certification Authority (CA) guarantees the identity of the person who is granted the certificate.
PSE	Secure location where a user or component's public-key information is stored. The <i>Personal Security Environment</i> (PSE) for a user or component is typically located in a protected directory in the file system or on a smart card. It contains both the public information (public-key certificate and private address book) as well as the private information (private key) for its owner. Therefore, only the owner of the information should be able to access his or her PSE.
ICF	Software layer in Application Server that provides an ABAP interface for HTTP, HTTPS & SMTP requests. The AS ABAP environment uses the Internet Communication Framework to communicate with Web applications in the server role and in the client role. ICF receives Web-based ABAP calls through Internet Communication Manager (ICM).
X.509	In cryptography, X.509 is an ITU-T standard for a public key infrastructure (PKI) for single sign-on (SSO) and <i>Privilege Management Infrastructure</i> (PMI). X.509 specifies, amongst other things, standard formats for public key certificates, certificate revocation lists, attribute certificates, and a certification path validation algorithm.
SOAP	SOAP, originally defined as <i>Simple Object Access Protocol</i> , is a protocol specification for exchanging structured information in the implementation of Web Services. It relies on <i>Extensible Markup Language</i> (XML) for its message format, and usually relies on other application layer protocols such as HTTP or RPC.

2 User Administration and Authorization

2.1 Authorization Object for the Payment Cockpit

The payment cockpit that is inbuilt into the *solution* is secured with an authorization strategy that contains standard authorization objects. This will also be used as a screening mechanism to ensure a secure authenticated payment run and monitoring in the system.

The following authorization objects are created for Monitor: /CBCOM/PRT

- Activity 16 for execution the report
- Activity A9 for resending the messages

A user must have the above mentioned authorizations to execute the payment cockpit.

© 2013 SAP AG	Title: SAP Corporate Connectivity for Banking	Page 5 of 23
Dietmar-Hopp-Allee 16	Version: 1.0	
D-69190 Walldorf	Date: January 25, 2013	



3 Certificate Implementation

3.1 Overview

This section describes the configurations and the step by step approach to enable the customer's SAP ERP system, and Westpac Bank's BANKPI System along with the intermediate load balancer at the bank's end to provide a secure message communication between the customer's and the bank's landscape by using the *Client Certificate Authentication* mechanism.

3.2 Security Mechanisms

A security-level defines the way a message that is embedded in a communication channel is handled between the interacting systems. The general HTTP security levels are as follows.

- HTTP without SSL
- HTTP with SSL (=HTTPS) without client authentication.
- HTTP with SSL (=HTTPS) with client authentication.

The security level used in this integration between the customer and the bank is *HTTP with SSL client authentication*. This security level is meant to ensure that only those messages/communication that are initiated over an HTTPS connection and are authenticated by client certificates, are accepted at the integration server / load balancer security framework as applicable.

Messages are rejected and dropped if the security level of the HTTP connection is lower or not as expected at the verification point for the incoming channel.

For more Information, see SAP Note **891877**.

3.3 Step-by-Step Instructions

3.3.1 Transaction STRUST

Managing certificates within the SAP environment (ABAP stack) is done through the standard transaction *STRUST*. The transaction contains a list of available PSE containers (on the left-side of the screen) and the trusted certificates that are available for them (on the right-side) Transaction *STRUST* also provides the option of creating custom PSEs for maintaining certificates relevant to a particular scenario.

For more Information on creating and managing PSEs, see the SAP Help Portal at: <u>http://help.sap.com/saphelp_nw04/helpdata/en/59/6b653a0c52425fe10000000a114084/content.h</u> <u>tm</u>

© 2013 SAP AG	Title: SAP Corporate Connectivity for Banking	Page 6 of 23
Dietmar-Hopp-Allee 16	Version: 1.0	
D-69190 Walldorf	Date: January 25, 2013	



The following figure shows a sample *STRUST* screen:

System PSE	SSL client SSL Client (Sta	indar
SNC SAPCryptolib	Own Certificate	
SSL server Standard	Owner	CN=
SSL client SSL Client (Anon)		
Ideiveb YCB 11		
SSL client Test Client Ident	i Certificate List	
 X WS Security Standard 		Owner
WS Security Other System		EMAIL=
 X SMIME Standard 	()	CN=stq.
• © File		
SSF E-Learning		
		Certificate Information
PSE Containers	Veri. PSE	Password relevant to a PSE
	Certificate	
	Owner	
	Issuer	
	Serial Number (Hex.)	
	Serial Number (Dec.)	
	Valid From	to
	Algorithm	Key Length
	Check Sum (MD5)	

Figure 1

© 2013 SAP AG	Title: SAP Corporate Connectivity for Banking	Page 7 of 23
Dietmar-Hopp-Allee 16	Version: 1.0	
D-69190 Walldorf	Date: January 25, 2013	



3.3.2 Certificates Used – Scenario Information

Figure 2 shows the technical implementation of the security configurations across the customer's and bank's landscapes





Communication Identifiers

E1C – Client Certificate of ERP E1C' - E1C Signed by CA of Load Balancer

PC – Client Certificate of Bank PI PC' - PC signed by CA of Corporate ERP

Figure 2

© 2013 SAP AG	Title: SAP Corporate Connectivity for Banking	Page 8 of 23
Dietmar-Hopp-Allee 16	Version: 1.0	
D-69190 Walldorf	Date: January 25, 2013	



Details of installed Certificates:

The following table provides details of various certificates that are used as a part of security configurations for the integration scenarios between customer's SAP ERP and BANKPI.

Scenario Information	Certificate Type	Signing Authority	Installation Location
Corporate ERP to BANKPI via load balancer See section 3.3.3 for implementation details	Client certificate	Trusted signing authority of load balancer in the Westpac landscape	Corporate ERP
BANKPI to Customer's SAP ERP See Section 3.3.4 for Implementation Details	Client certificate	Trusted signing authority of corporate ERP system	BANKPI

3.3.3 Security Configurations in the Customer's ERP

This section deals with the security configurations to be implemented in the customer's SAP ERP system for communication between ERP and BANKPI via load balancer.

Note: We have used the SSL client standard PSE for all communications and scenarios that leverages the solution and establishes connectivity with the mentioned security configurations. The steps given in sections 3.3.3 and 3.3.4 describe the same.

Step 1: Expand the folder of PSE - SSL Client SSL Client Standard in the ERP system as shown in

figure 3. Double-click on the corresponding entry. The PSE will have the root certificate of the concerned ERP system as shown in the following figure:

© 2013 SAP AGTitle: SAP Corporate Connectivity for BankingPage 9 of 23Dietmar-Hopp-Allee 16Version: 1.0D-69190 WalldorfDate: January 25, 2013



Trust Manager		
 System PSE SNC SAPCryptolib SSL server Standard SSL client SSL Client (Anonymo Idciycb_YCB_11 SSL client SSL Client (Standar Idciycb_YCB_11 SSL client Test Client Identit Idciycb_YCB_11 SSL client Test Client Identit Idciycb_YCB_11 SSL client Test Client Identit Idciycb_YCB_11 SSL client Test Client Identit Idciycb_YCB_11 SSL client Test Client Identit SSL client Test Client Identit SSE curity Standard SSE Security Other System Encry SMIME Standard SF File SSF E-Learning 	SSL client SSL Client (Stan Own Certificate Owner Certificate List	dar <u>CN=' I, OU=! J, O=</u> <u>CN=' OU=!</u>
	🔄 Veri. PSE 🔒	Password
	Certificate	
	Owner	EMAIL=r @sap-ag.de, CN= , OU= O
	Issuer	EMAIL=r @sap-ag.de, CN= , OU= O
	Serial Number (Hex.)	01000000
	Serial Number (Dec.)	16777216
	Valid From	04.05.1998 11:56:34 to 18.07.2015 12:00:00
	Algorithm	RSA Key Length 1024
	Check Sum (MD5)	
	Checksum (SHA1)	
		Add to Certificate List

Figure 3

Step 2: Choose Create Certificate Request to copy the certificate request as shown.

© 2013 SAP AG	Title: SAP Corporate Connectivity for Banking	Page 10 of 23
Dietmar-Hopp-Allee 16	Version: 1.0	
D-69190 Walldorf	Date: January 25, 2013	



Trust Manager					
 System PSE 	SSL client SSL Client (Standar			
SNC SAPCryptolib	Own Certificate				
 SSL server Standard SSL client SSL Client (Anony 	Owner	<u>CN='</u>		, OU=	<u>0=</u>
▼ SSL client SSL Client (Stand					
Idciycb_YCB_11 Idciycb_YCB_11	Create Certificate R	lequest			
 WS Security Standard 		Owner			
 WS Security Other System WS Security WS Security Ke 		EMAIL=	@sap-aq.de,		<u>t</u> . 33
 X SMIME Standard 					
• 🔗 File					
 X SSF E-Learning 					-
	Veri. PSE	Password			

Figure 4

Step 3: Copy the certificate request and store it in the buffer. This certificate request now needs to be signed in PKCS #7 format (ideally) by the bank's LB trusted Authority.

🗧 Certificate Reques	t		×
i de la compacta de l			
BEGIN CERTI MIIB0jCCATsCAQAw Q29tbXVuaXR5MRMw MDg2MjE5MDcGA1UE ZXMgUFNFIFNjZW5F maYJ7w7EARMyQu3F 5ZQBSLWZVw8EkBv6 OgXJfQCUIBazV0C4 BQADgYEA49HsAvu3 IpkStf81qDj00fY1 m7cwT007J/1TMNAF END CERTIF1	FICATE REQUEST gZExCzAJBgNVBAYTAkRFMRww(EQYDVQQLEwpTQVAgV2ViIEFTN AxMwWUNCIFNTTCBjbG11bnQgV acm1vMIGfMA0GCSqGSIb3DQEBJ bdqzHqLdHJQMcj0/bI29Y7gca0 G8DSTT5C+7DNvgAFQ+keSrCR bvTFzWGaD54CntaPMwSBYQIDJ mhFuoWeXwnsf8xGsAxc922Is1 vifTTT8wr7e1Ku5hqnk1uQB6B BL6//1kPHmEXk/3Fm7MyfGWmce CATE REQUEST	GgYDVQQKExNTQVAgVHJ1c3Qg MRQwEgYDVQQLEwtJMDAyMDI3 /GVzdG1uZyBDZXJ0aWZpY2F0 AQUAA4GNADCBiQKBgQD+weWf DuqxrmpNSJwYUJ+vWpyxniPt /qhbnFhT60bEirD3uC7C7oM6 AQABoAAwDQYJKoZIhvcNAQEF rfeoL1bJWcW8YvzAgShzcOMS H8dVn8IEGrMANJPgIroMc1cQ eMHHYthSmWs=	

Figure 5

Step 4: Once the signed certificate response has been received from the bank, it should be imported in the same SSL client SSL standard PSE. Choose *Import Certificate Response* as shown in Figure 6.

© 2013 SAP AG	Title: SAP Corporate Connectivity for Banking	Page 11 of 23
Dietmar-Hopp-Allee 16	Version: 1.0	
D-69190 Walldorf	Date: January 25, 2013	



Trust Manager		
 Frust Manager System PSE SNC SAPCryptolib SSL server Standard SSL client SSL Client (Anonymo Idciycb_YCB_11 SSL client SSL Client (Standar Idciycb_YCB_11 SSL client Test Client Identit Idciycb_YCB_11 SSL client Test Client Identit Idciycb_YCB_11 	SSL client SSL Client (Standar Own Certificate Owner OU= OU= O= Import Certificate Response Certificate List Owner EMAIL= @sap-aq.de, CN= OU=	
 WS Security Other System Encry WS Security WS Security Keys SMIME Standard File SSF E-Learning 	Veri. PSE Password Certificate Owner EMAIL= Issuer EMAIL= Osap-ag.de, CN= OU= OU= O	

Figure 6

Step 5: Copy the response and choose *Import Certificate Response* as shown in Figure 6. The certificate response should be input and saved for it to be registered in the PSE as shown below.

Certificate Response	
10 16 16 16 18 12 12 12 12 12 12 12 12 12 12 12 12 12	
BEGIN CERTIFICATE	
IIIFYQYJKoZIhvcNAQcCoIIFUjCCBU4CAQExADALBgkg	hkiG9w0BBwGgggU2MIIC
zCCAjSgAwIBAgIPAOnvmNWqhaV5EAIBADf0MA0GCSqG	SIb3DQEBBQUAMFAxCzAJ
gNVBAYTAkRFMRwwGgYDVQQKExNTQVAgVHJ1c3QgQ29t	bXVuaXR5MQ8wDQYDVQQL
wZTZXJ2ZXIxEjAQBgNVBAMICVN1cnZ1ciBDQTAeFw0x	MjExMDYwMjUOMTFaFw0x
<pre>izAxMDUwNjU0MTFaMIG1MQswCQYDVQQGEwJERTEcMBoG</pre>	AlUECHMTUOFQIFRydXNO
IENvbW11bm10eTEPMA0GA1UECxMGU2VydmVyMRMwEQYD	VQQLEwpIQVAgV2V1IEFT
KRQwEgYDVQQLEwtJMDAyMDI3MDg2MjE5MDcGA1UEAxMw	WUNCIFNTTCBjbGllbnQg
/GVzdGluZyBDZXJ0aWZpY2F0ZXMgUFNFIFNjZW5hcmlv/	MIGIMAOGCSqGSIb3DQEB
AQUAA4GNADCB1QKBgQD+weWfmaYJ7w7EARMyQu3bdqzH	qLdHJQMcj0/bI29Y7gca
DugxrmpNSJwYUJ+vWpyxniPt5ZQBSLWZVw8EkBv6G8DS	TI5C+7DNvgAFQ+keSrCR
<pre>?qhbnFhT60bEirD3uC7C7oM60gXJfQCUIBazV0C4bvTF</pre>	zWGaD54CntaPMwSBYQID
AQABo1QwUjAMBgNVHRMBA18EAjAAMBMGA1UdJQQMMAoG	CC#GAQUFBWMBMA4GA1Ud
DwEB/wQEAwIESDAdBgNVHQ4EFgQUvuKeJFvtgzoNiHko	VARJBinYpOUwDQYJKoZI
nvcNAQEFBQADgYEAUoI7L79uuCZaJQvLfpq3gWdXEoCK	1/E1MrEkI75c52KfBvzP
sKFg6XRYoU1cbeFkcwzDU9jpEHAYELjeb0QusGJf2WmA	rqzeaylMQvpX/c6+we9h
RpWj+KCwdGWCRwzLpmrTK5JgaMGSMvjlmeYKjhdtTScY	IgWA8L5EGVxp5MgwggJj
411BzKADAgECAgQBAAAAMA0GCSqGS1b3DQEBBQUAMFAx	CZAJBGNVBAYTAKRFMRww
3gYDVQQKExNTQVAgVHJ1c3QgQ29tbXVuaXR5MQ8wDQYD	VQQLEwZIZXJ2ZXIxEjAQ
SgNVBAMTCVN1cnZ1c1BDQTAeFw0wMDA3MTgxMDAwMDBa	FWOXNTA3MIGXMDAwMDBa
AFAXCZAJBGNVBAYIAKRFMRWWGGYDVQQKEXNIQVAGVHJ1	c3QgQ29tbXVuaXR5MQ8w
JQYDVQQLEW2I2XJ22XIXEJAQBGNVBAMICVN1ch21c1BD	QICBNZANBGRGhRIG9W0B
KQEFAAOBJQAWGIKCGIEA/VE4AMIHJ88UJFINDAUDXIIX	X3X11C2SMKesmiWolech
pp2on60veg3h0LMSSKpxawL01L01He00vgndgewwck9/	AYVKWALOALYISVQ+4ZDY
SANOHMIS/JM2WZMU9JN816NIJUBSINKNYCIIA4XDX2K8	SejzporiesvsevsmaLuc
AWERAGINALGWUWIDVRUIRYA/DAUWAWED/ZAIDGAVARIE	njacnnpodnawolovczvy
THE JESSELARGE FOLLENDERUDGEVENODELEDARCHEIW	UNITADI INVERNICI DUAD
1991 2nos 20To 1 h Eon 3 of a Vacuture Aht CO1 + Var PDEV7	ai fel VThVatSI dVhII3DT
SDOSnFCD=RoSafN102YTfdnNonHFdhfDDuHn9hu3=DRu	Schuller
END CERTIFICATE	
* Li 31, Co 26	Ln 1 - Ln 31 of 31 lines
	¥

Figure 7

Step 6: Save the response. You can see that the Issuer name has changed to the credentials from the signing authority presented by the bank as shown in Figure 8.

© 2013 SAP AG	Title: SAP Corporate Connectivity for Banking	Page 12 of 23
Dietmar-Hopp-Allee 16	Version: 1.0	
D-69190 Walldorf	Date: January 25, 2013	



Trust Manager		
		-
System PSE SNC SARCorptolib	SSL client SSL Client (Stan	dar
 SSL server Standard SSL client SSL Client (Anon) SSL client SSL Client (Stand 	Own Certificate Owner	<u>CN=YCB</u>
 Idciycb_YCB_11 SSL client Test Client Identi WS Security Standard 	Certificate List	
WS Security Other System WS Security WS Security K		Owner EMAIL= @sap-aq.de, CN= , OU=
 File SSF E-Learning 		
	Veri. PSE	Password
	Certificate	
	Owner	CN=YCB :
	Issuer	CN=stg-dc, DC=stg-intsol, DC=westpac, DC=com, DC=au
	Serial Number (Hex.)	1723C483000000004C

Serial Number (Dec.)	1092742253:
Valid From	31.10.2012 03:04:06 to 25.07.2013 02:48:12
Algorithm	RSA Key Length 1024
Check Sum (MD5)	A2:AB:85:4D:39:9F:5F:14:5C:71:60:5C:57:A1:03:F7
Checksum (SHA1)	8F89810BA7871BDE53F7A9372BE1D6773FABBB49
	Add to Certificate List

Figure 8

Step 7: Choose Add to Certificate List to add this certificate to the current PSE list as shown in Figure 9.

© 2013 SAP AG	Title: SAP Corporate Connectivity for Banking	Page 13 of 23
Dietmar-Hopp-Allee 16	Version: 1.0	
D-69190 Walldorf	Date: January 25, 2013	



Trust Manager		
 System PSE SNC SAPCryptolib SSL server Standard SSL client SSL Client (Anonymo Idciycb_YCB_11 SSL client SSL Client (Standar Idciycb_YCB_11 SSL client Test Client Identit Idciycb_YCB_11 SSL client Test Client Identit Idciycb_YCB_11 SSL client Test Client Identit Idciycb_YCB_11 SSL client Test Client Identit Idciycb_YCB_11 SSL client Test Client Identit Idciycb_YCB_11 SSL client Test Client Identit SSL client Test Client Identit SSL client YCB_11 	SSL client SSL Client (Stand Own Certificate Owner De De Certificate List	dar $\begin{array}{c c} \hline \\ \hline $
• X SSF E-Learning	Veri. PSE	Password
	Certificate	
	Owner	CN=Y(
	Issuer	CN=stg-dc, DC=stg-intsol, DC=westpac, DC=com, DC=au
	Serial Number (Hex.)	1723C483000000004C
	Serial Number (Dec.)	109274225310235057193036



Figure 9

Step 8: After completing the steps described above, execute a *DISTRIBUTE ALL* and restart ICM for the changes to come into effect.

© 2013 SAP AG	Title: SAP Corporate Connectivity for Banking	Page 14 of 23
Dietmar-Hopp-Allee 16	Version: 1.0	
D-69190 Walldorf	Date: January 25, 2013	



¢	<u>PSE E</u> dit <u>G</u> oto <u>C</u> ertifica	te En <u>v</u> ironment S <u>v</u> stem <u>H</u> elp
(Import Export Save as	▋ � � � □ ₩ ₩ 約 約 월 ፵ ፬ ⑨ ■
	Create Verification PSE	_
Г	Check <u>A</u> ll F5 Distribute A <u>l</u> l F6	SSL client SSL Client (Standar
	 Exit Shift+F3 SSL client SSL Client (Anony SSL client SSL Client (Stand SSL client SSL Client (Stand Idciycb_YCB_11 SSL client Test Client Identi WS Security Standard WS Security Other System 	Own Certificate Owner OU= O= Owner Owner Certificate List Owner Owner Owner FMAIL Owner
	 WS Security WS Security Ke SMIME Standard File SSF E-Learning 	CN=stq-dc, DC=stq-intsol, DC=westpac, DC=com, DC=au

Figure 10



3.3.4 Steps after Certificate-Installation in SAP ERP

The steps given in section 3.3.3 describe how the trusted authority of the load balancer at the bank's side signs the client certificate for the ERP. The key store view of this PSE – SSL client standard **DFAULT** can now be used to implement the security configuration for communication via SOAMANAGER from ERP to BANKPI as shown in the Figure 12.

© 2013 SAP AG	Title: SAP Corporate Connectivity for Banking	Page 15 of 23
Dietmar-Hopp-Allee 16	Version: 1.0	
D-69190 Walldorf	Date: January 25, 2013	



nfiguration of Logical Port 'LP_M	ODWSDL'
it Save Cancel	
Consumer Security Me	essaging Transport Settings Operation specific Administrative Information
Configuration of Consumer Set	tings additional to WSDL Document Information LP=LP_MODWSDL
User ID/Password	
User Name: WS_ Password: •••••	
X.509 SSL Client PSE	
SSL Client PSE of transaction STR	RUST: DFAULT Keystore view of the relevant PSE
Properties from WSDL Docum	nent
Transport Security	
Secure Communications:	SSL
Signature Expected:	false
Encryption Expected:	false
Sign Message:	false
Add Encryption:	false
PSE of Key:	WSSCRT
Authentication	
Authentication Method:	sapsp:HTTPX509
Authentication Method:	sapsp:HTTPBasic

Figure 11

For more details on this configuration and its usability, see the solution configuration guide.

3.4 Generic Steps – Creating a PSE (If required)

- The steps documented in this section should **ONLY** be implemented if the security configuration, as has been explained above, is to be carried out by creating Individual PSE's for every scenario relevant to a customer.
- ☑ The steps mentioned in sections 3.3.3 3.3.4 and in section 3.5 should be implemented in the given order after completing the steps in Section 3.4.

Step 1: Create a PSE by accessing the STRUST transaction.

© 2013 SAP AG	Title: SAP Corporate Connectivity for Banking	Page 16 of 23
Dietmar-Hopp-Allee 16	Version: 1.0	
D-69190 Walldorf	Date: January 25, 2013	



E FOE	<u>E</u> dit	Goto	<u>C</u> ertificate	En <u>v</u> ironment	System	<u>H</u> elp
0			• 4 🛛	0		8 20 10 10 20 🕱 🗾 20 📭
Trust	Man	ager				

Figure 12

Step 2: From *Environment* menu, select SSL Client Identities.

<u>PSE E</u> dit <u>G</u> oto <u>C</u> ertificate	En <u>v</u> ironment System <u>H</u> elp	
♥ ↓ ↓ Trust Manager	SSL Server Identities SSL <u>Client</u> Identities <u>WS</u> Security Identities S/MIME Identities SSF <u>P</u> aramters F9	
System PSE SNC SAPCryptolib	<u>L</u> ogon Ticket <u>I</u> CM Monitor	
 SSL server Standard Idciycb_YCB_11 SSL client SSL Client (Anonymo 	Display SS <u>F</u> Version Dele <u>t</u> e Temporary Files	
 Idciycb_YCB_11 SSL client SSL Client (Standar Idciycb_YCB_11 SSL client Test Client Identit 	Certificate List	



Figure 13

Step 3: Choose *New Entries* to create a new PSE.

© 2013 SAP AG	Title: SAP Corporate Connectivity for Banking	Page 17 of 23
Dietmar-Hopp-Allee 16	Version: 1.0	
D-69190 Walldorf	Date: January 25, 2013	



Tanie viev	w <u>E</u> dit	<u>G</u> oto	<u>S</u> e	election	Uti	lities	Sy	stem	Help				
ð		•	٥	8 (3 🙆			HK	🖏	Ð	Ð	8 D	Ĺ
Change	View "	SSL C	lier	nt Id	enti	ties	of	Syste	em":	0	ver	vie	w
🦻 New Er	ntries	B 🔊]								
	New Entr	ries (F5))—										
and the second	a man ene		9										
SSL Client I	u												
SSL Client I Identity	Descript	tion											
SSL Client I Identity ANONYM	Descript	tion nt (Anon	iymo	us)							-		
SSL Client I Identity ANONYM DFAULT	Descript SSL Clier	tion nt (Anon nt (Stand	iymo dard j	ius))							-		

Figure 14

Step 4: Maintain a new PSE entry, for example TESTV as shown. Save and return to the initial screen.



Client Ic	dentities of System	
entity	Description	
STV	Testing Certificates PSE Scenario	

Figure 15

Step 5: You can see that the newly-created PSE has a red cross in the left column bar. Right-click this and choose *Select* to maintain the parameters of this PSE.

© 2013 SAP AG	Title: SAP Corporate Connectivity for Banking	Page 18 of 23
Dietmar-Hopp-Allee 16	Version: 1.0	
D-69190 Walldorf	Date: January 25, 2013	





Step 6: Choose *OK* to maintain the entry. The folder for the PSE will be created.

🕨 🛄 System PSE	SSL client TEST Scenario
SNC SAPCryptolib	Own Certificate
SSL server Standard	Ownor
 Idciycb_YCB_11 	
▼ SSL client SSL Client (Anonymo)	



• 😐	ldciycb_YCB_11	
🔹 🔂 SS	L <mark>client SSL Client</mark>	(Standar Certificate List
• 🖸	ldciycb_YCB_11	
• 💥 SS	L client Testing Ce	artificate
🕨 🗀 ss	L client Test Client	t Identit
• 🗙 w	S Security Standar	d l
• 🗙 W	🔄 Create PSE	×
• 🗙 w	9	F
• 💥 SN	Name	L client Testing Certificates PSE Scenario
• 🖓 File	Org. (Opt)	10020270862
• 🗙 SS	Comp./Org.	SAP Web AS
	Country	
	CA	O=SAP Trust Community, C=DE
	Algorithm	RSA
	Key Length	1024 💌

Figure 17

Step 7: Double-click on the folder of the created PSE to get the certificate information.

© 2013 SAP AG	Title: SAP Corporate Connectivity for Banking	Page 19 of 23
Dietmar-Hopp-Allee 16	Version: 1.0	
D-69190 Walldorf	Date: January 25, 2013	



Trust Manager		
 System PSE SNC SAPCryptolib SSL server Standard Idciycb_YCB_11 SSL client SSL Client (Anonymo Idciycb_YCB_11 SSL client SSL Client (Standar Idciycb_YCB_11 SSL client Testing certificate Idciycb_YCB_11 SSL client Test Client Identit SSL client Test Client Identit SSL client Test Client Identit SSE curity Standard SSE security Other System Encry SMIME Standard SSF E-Learning 	SSL client Testing Certificate Own Certificate Owner Certificate List Certificate List	ate CN=YCB. OU=10020 (Self-Signed) Owner Owner Password
	Certificate	
	Owner	EMAIL= @sap-ag.de, CN=: OU=: O
	Issuer	EMAIL= @sap-ag.de, CN=! OU=! O
	Serial Number (Hex.)	01000000
	Serial Number (Dec.)	
		PSA Key Length 1024
	Check Sum (MDS)	B5:5E:64:10:AE:09:6B:71:AC:77:A4:EE:61:09:21:71
	Checksum (SHA1)	2240E95CFE137B21394E61EDCB8F184757CADAA3
		Add to Certificate List

Figure 18

This PSE is now ready to be used for security scenarios.

3.5 Installing a Root Certificate – Generic Procedure

The steps documented in this section should **ONLY** be implemented if the security configuration, as explained above, is to be carried out by creating Individual PSEs for every scenario that is relevant to a customer.

The steps mentioned in sections 3.3.3 - 3.3.4 and section 3.5 should be implemented in the mentioned order after completing the steps in section 3.4.

Step 1: Open transaction *STRUST* for the PSE where the root certificate must to be installed.

© 2013 SAP AG	Title: SAP Corporate Connectivity for Banking	Page 20 of 23
Dietmar-Hopp-Allee 16	Version: 1.0	
D-69190 Walldorf	Date: January 25, 2013	



Trust Manager		
 System PSE SNC SAPCryptolib SSL server Standard Idciycb_YCB_11 SSL client SSL Client (Anonymo Idciycb_YCB_11 SSL client SSL Client (Standar Idciycb_YCB_11 SSL client SSL Client (Standar Idciycb_YCB_11 SSL client Testing Certificate Idciycb_YCB_11 SSL client Testing Certificate Idciycb_YCB_11 SSL client Test client Identit SSL client Test client Identit SSE client Test client Identit SSE client VS Security WS Security Keys SMIME Standard STIME Standard Stile 	SSL client Testing Certificate Owner Certificate List	te CN=YCB (Self-Signed)
• 🗙 SSF E-Learning	🔄 Veri. PSE 🗎	Password
	Certificate	
	Owner	EMAIL= OU= O
	Issuer	EMAIL= OU= O
	Serial Number (Hex.)	0100000
	Serial Number (Dec.)	16777216
	Valid From	04.05.1998 11:56:34 to 18.07.2015 12:00:00
	Algorithm	RSA Key Length 1024
	Check Sum (MD5)	B5:5E:64:10:AE:09:6B:71:AC:77:A4:EF:61:99:21:71
	Checksum (SHA1)	2240E95CFE137B21394E61EDCB8F184757CADAA3
	Import certificate	Add to Certificate List

Figure 19

Step 2: Choose Import Certificate Request and specify the path of the downloaded root certificate.

🔄 Import Certificate		×
File Database	Addr. Book Directory service SAP System	
File path	rs\I070230\Downloads\getCert.cer	þ
File format		
 Binary 		
OBase64		
		✓ ×

Figure 20

© 2013 SAP AGTitle: SAP Corporate Connectivity for BankingPage 21 of 23Dietmar-Hopp-Allee 16Version: 1.0Page 21 of 23D-69190 WalldorfDate: January 25, 2013Date: January 25, 2013



Step 3: Choose *OK;* you can now see the root certificate in the PSE as shown below. **STRUST before Import**

SSL client Testing Certifica	te			
Own Certificate				
Owner	CN=YCB]
	(Self-Signed)			
Certificate List				
	Owner			
				*
Veri. PSE	Password]		
Certificate				
Owner	EMAIL=	@sap-ag.de, CN=	OU	O
Issuer	EMAIL=	@sap-ag.de, CN=	OU	O
Serial Number (Hex.)	01000000			
Serial Number (Dec.)	16777216			
Valid From	04.05.1998	11:56:34 to 18.	07.2015 12:00:00	
Algorithm	RSA	Key Length	1024	
Check Sum (MD5)	B5:5E:64:10:A	E:09:6B:71:AC:77:A4:E	F:61:99:21:71	
Checksum (SHA1)	2240E95CFE1	37B21394E61EDCB8F18	4757CADAA3	
	🔂 Add t	o Certificate List		



STRUST after Import

Title: SAP Corporate Connectivity for Banking Version: 1.0 © 2013 SAP AG Page 22 of 23 Dietmar-Hopp-Allee 16 D-69190 Walldorf Date: January 25, 2013



SSL client Testing Certifica	te	
Own Certificate		
Owner	CN=YCB	
	(Self-Signed)	
Certificate List		
	Owner	
	EMAIL= <u>@sap-aq.de, CN=</u> OU=	
	Root Certificate Populated	
Certificate	Password	
Owner	EMAIL= r@sap-ag.de, CN= . OU= . O	
Issuer	EMAIL= r@sap-ag.de, CN= .OU= .O	
Serial Number (Hex.)	01000000	
Serial Number (Dec.)	16777216	
Valid From	04.05.1998 11:56:34 to 18.07.2015 12:00:00	
Algorithm	RSA Key Length 1024	
Check Sum (MD5)	B5:5E:64:10:AE:09:6B:71:AC:77:A4:EF:61:99:21:71	
Checksum (SHA1)	2240E95CFE137B21394E61EDCB8F184757CADAA3	
	Add to Certificate List	

Figure 22



4 Security Issues

For any issues regarding certificates and security-related configurations, raise a ticket under component BC-SEC-WSS

© 2013 SAP AG	Title: SAP Corporate Connectivity for Banking	Page 23 of 23
Dietmar-Hopp-Allee 16	Version: 1.0	
D-69190 Walldorf	Date: January 25, 2013	