

IBM Software Group

C3: Implementing SSL Security in WebSphere Partner Gateway

Presenter: Max Terpolilli – WPG L2 Support







Objectives

Provide an easy reference guide to configure for the different SSL security levels

Group together the configuration steps necessary for all WBIC/WPG products set

Make use of screen shots to facilitate the user implement the desired security level

Introduction to the product tools used to mManage Certificates



IBM

Agenda

i	Digital Signature – Basic Concepts Encryption – Basic Concepts Client/Server Authentication – Basic Concepts	3-4 5-6 7-8
;	Digital Signature – WBIC/WPG Adv/Ent Implementation: Outbound Digital Signature – WBIC/WPG Adv/Ent Implementation: Inbound Digital Signature – WBIC/WPG Express Implementation: Outbound Digital Signature – WBIC/WPG Express Implementation: Inbound	10 11 12 13
;	Encryption – WBIC/WPG Adv/Ent Implementation: Outbound Encryption – WBIC/WPG Adv/Ent Implementation: Inbound Encryption – WBIC/WPG Express Implementation: Outbound Encryption – WBIC/WPG Express Implementation: Inbound	14 15 16 17
;	Server Authentication – WBIC/WPG Adv/Ent Implementation: Outbound Server Authentication – WBIC/WPG Adv/Ent Implementation: Inbound Server Authentication – WBIC/WPG Express Implementation: Outbound Server Authentication – WBIC/WPG Express Implementation: Inbound	18 19 20 21
;	Client Authentication – WBIC/WPG Adv/Ent Implementation: Outbound Client Authentication – WBIC/WPG Adv/Ent Implementation: Inbound Client Authentication – WBIC/WPG Express Implementation: Outbound Client Authentication – WBIC/WPG Express Implementation: Inbound	22 23 24 25-26
i	Managing Certificates for WBIC/WPG Adv/En: Ikeyman utility Managing Certificates for WBIC/WPG Express: Built-in utility	28-32 33-34
	Q/A	35



Digital Signature – Basic Concepts 1/2

Uses "public-key cryptography" algorithm

Signing a document

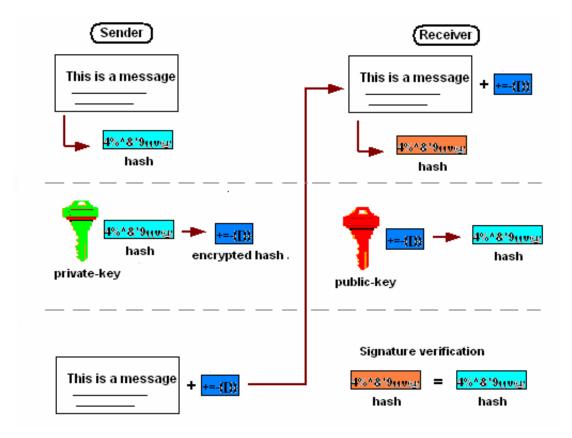
- The content of the message is "hashed"
- The "hashed" message is processed by the Private-key to produce a "Digital Signature"
- The Digital Signature is attached to the message and sent with it

Signature Verification

- > "Hashes" the message received
- Uses the public-key to decrypt the Digital Signature
- Compares whether the 2 hashes match



Digital Signature – Basic Concepts 2/2







Encryption – Basic Concepts 1/2

>There are two main types of encryption:

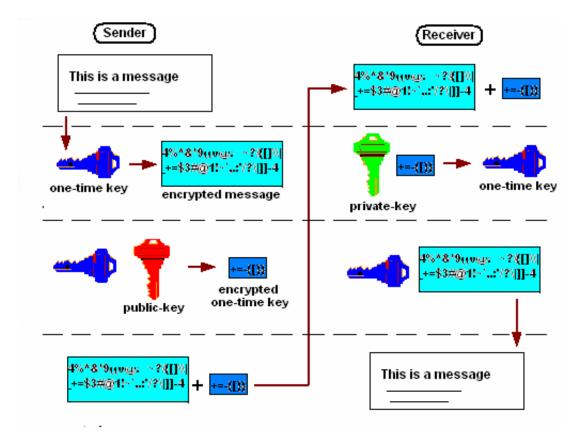
- Asymmetric encryption or public-key encryption: Public-key to encrypt and Private-key to decrypt
- Symmetric encryption or private-key encryption: Uses the same "secret" key to encrypt and decrypt

Combination of Asymmetric and Symmetric encryption systems:

- Symmetric secret-key to be used to encrypt the message
- Encrypt the secret-key using the asymmetric Public-key
- > Add the encrypted secret key to the encrypted message
- Recipient uses his private-key to decrypt the secret-key, and uses it to decrypt the message



Encryption – Basic Concepts 2/2







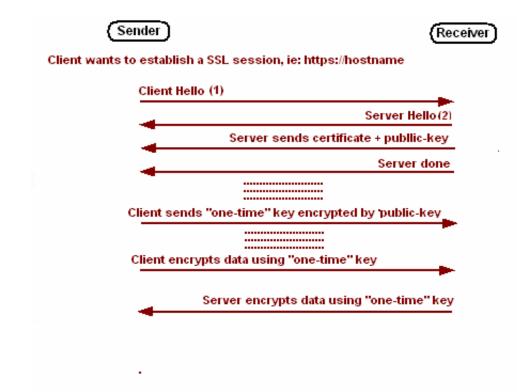
Client/Server Authentication - Basic Concepts 1/2

Certifies the identity of the Server/Client in session

- The Client starts a SSL session with the Server
- The Server sends its certificate
- > The Client verifies the Server certificate
 - >The Client sign and sends its certificate
 - The Server verifies the Client certificate
- The Client sends to the Server the "one-time key" to encrypt/decrypt data during the SSL session

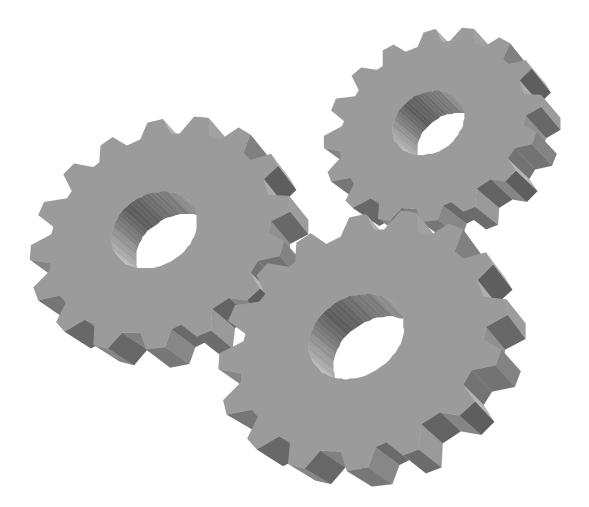


Client/Server Authentication - Basic Concepts 2/2



- 1 Highest SSL Version, Ciphers Supported, data compression methods, SessionID, ...
- 2 Selected SSL Version, Selected Ciphers, Selected data compr, Assigned SessionID, ...







Digital Signature: WPG Adv/Ent Implementation

≻Outbound:

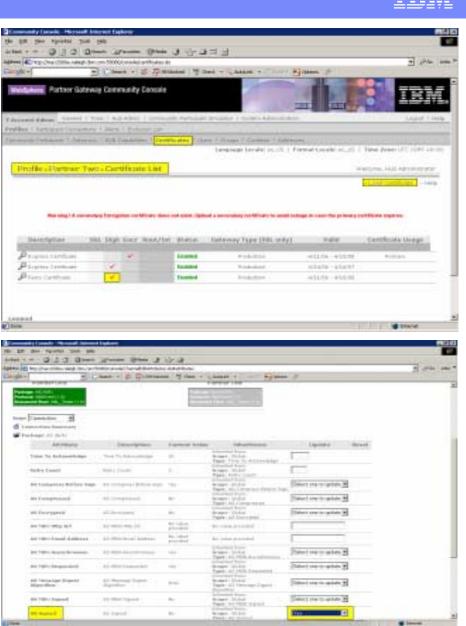
- Load company.p12 as Hub Operator's PKCS12 digital signature certificate
- Enable "AS Signed" in the Participant Connection
- Send certificate to the Participant

and the second se			TALANT L. B.		
			3123		-
City Inc. 2004 Had-			Cant + 9, Settint +	Name of	214
	-	a gamen	April 100 and a second as		60
num: Partner Gate	way Dommunity	Console	100		
				122.1	the state of the s
didnes Vanis i	THOR & Hug Martin	A Symposite Series	and involving a lower and	automa:	Lipid
And the second second	1. 2. 2000 2. 4100	and the second second			
the Person of Cases	TTT REP Considering	ing Treeffication	inter / Proge 7 Conten.)		Contract of the Second Second
			Feedboarts (solds) out	Lin Perseat Locater	v(.1)) Nee Nee (1) (01
office Plub Diser	dor - Cartilica	te Let			Averante All Administ
and the second se				Hand	Inthus (caterola) -
Protocol 1 A Associated	my Paper Ingeniet is a	at Blocks down and sum	t, sprind a recording contracts	to ever other in user 3	e anter plantitude septem.
mg 1 h are saving 112 or	Address in states and state		man types. Heined a secondary	service and strategy	in case the printer or this are real
7 h					A Design of the second second
Discription II	n over tear a	cost/pet Otation	Gateway Type (88L a	1997, Hand	Certificate thap
	1	ingend	Projection	4110-4	
Perry Carelinate	8	Tradition of	· Passinders	41140-0	14.94
d is to then Carthoon					
d hi haa Carthian	later				1 Turnet
a t ter (effen)	CONTRACTOR OF STREET	kdr. and Hart			
a t ter (effen)	CONTRACTOR OF STREET	kdr. and Hart			
a to the Carthoun a to the Carthoun a to the to the total a total a total and a total a total a total a tota	CONTRACTOR OF STREET				
an free (efficie) an frees to at	CONTRACTOR OF STREET				
a to the Carthoun a constrained and a constrained	CONTRACTOR OF STREET				
a to the Carthoun a to the Carthoun a to the to the total a total a total and a total a total a total a tota	CONTRACTOR OF STREET				
	CONTRACTOR OF STREET				
	CONTRACTOR OF STREET				
	CONTRACTOR OF STREET				- 100 March 100
	CONTRACTOR OF STREET			-	
					- 100 March 100
					apata
					Tapidat ma Tapidat ma Tapidat series Sector copies 1 Sector copies 1 Sector copies 1 Ferrom Management (*
				March 1997	Table and the second se
				Internet of a constraint of a	Tapakas ma Tapakas ma Tapakas para tapaka Tapakas para tapaka Tapakas para tapaka Tapakas para tapaka Tapakas para tapaka Tapakas para tapaka
					Tapakas mar Tapakas mar Tapakas mar Tapakas tapaka Tapakas tapaka Tapakas tapaka Tapakas tapaka Tapakas tapaka Tapakas tapaka Tapakas tapaka
					apalalar mar apalalar mar Sance on a para di Sance on a para di
					apalala mar apalala mar Patro e apala a Sant e a apala a Sant
A Pare (P PRoperty Sector Secto					apalalar mar apalalar mar Sance on a same al Sance on a same al

Digital Signature: WPG Adv/Ent Implementation

≻Inbound:

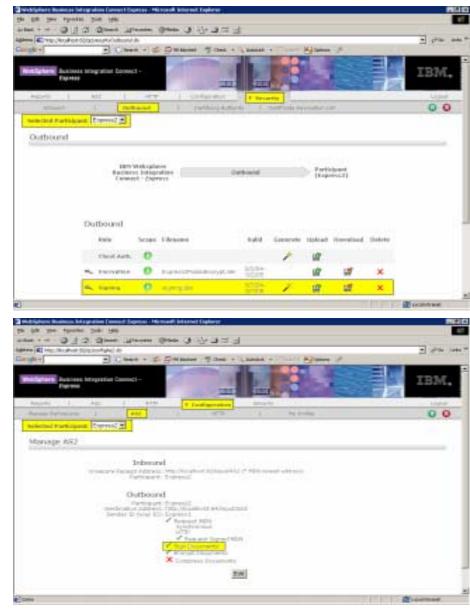
- Load Participant.cer in the Participant profile as digital signature certificate
- If signed by a CA, install the CA certificate in the Hub Operator profile, as root
- Enable "AS Signed" in the Participant Connection



Digital Signature: WPG/WBIC Express Implementation

≻Outbound:

- Upload or generate a .p12 keypair
- Download the certificate and send it to the Partner
- Enable Digital Signature for outbound documents



IBM

Digital Signature: WPG/WBIC Express Implementation

≻Inbound:

Add the Partner certificate in the "Certifying Authority" list

al 💽 hitsy (Recollect All/sy /m) ghi e		Balanded 19 Card +	Antal	2 20 1
Matern Bestess bing Express	elter Correct -	-		IBM.
Papana) p22	1 1077	Carlgerten	+ seconder	10040
inatany 1	Artonal	Lantifaria Autho	eta (1. Californ konsense Cor	0 0
C Barrat av	Character day		3.044 - 12.06 3.1/04 - 3.0 m	×
	Superverty (see)			×
 View Ceylificate 440/(Artists (artificital)) Debris Certificata/cas 	**			
. See a second s				WebSplace authority



Encryption: WPG Adv/Ent Implementation

≻Outbound:

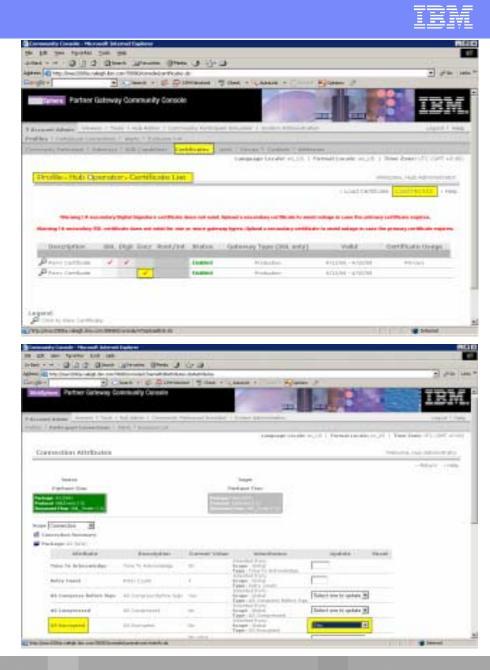
- Load Participant certificate in the Participant profile as encryption certificate
- If signed by a CA, install the CA certificate in the Hub Operator profile, as root
- Enable "AS Encrypted" in the Participant Connection

14 per Syntem		-	-				
	Town The	and grant of	11025.08				- P4
ak-			and Total	A + LADOR +			1.00
				With stress	100	100	
and it is not the second second	Anternay Commu	and Charlook		199	178	17 200	IEW
					111	ALL COMPANY	
himmiddeni			estimation of the	many (bodge, ab	5/1/1 Http://		lapor t la
ettee 1 februari Co-		Toring of Lat.	1	Contract Contractor	* ***		
		and the second second				NAMES OF A DR	e fere (75,1177,41.0
Profile LHub Op	inators Cort	State Live				100	and and the second second
					1	Lini Lewista	1,000 001222
The stage is not	and a light line of		or sent spice	al a resultance of the second s		total the printers and	That cannot
Second days	in the second					Value In	officie lines
Section of the sectio	the star fits		a second second	derren Tane (153)			and a state of the later.
Place Sectors	4 4		-	Production		10-A4A/01	Preserv
Press Landada	the sub-reg	2 Au	dand.	Resident	-61.0	96 - 197.8794	
7***		areas a				- 19	a hered
Chief and the state of the state	a land lagers					- 12	a yeard
	a lattiyodarik) i se jasi _d isələr	en a co	Area (1
	a lattiyodarik) i se jasi _d isələr	en a co	Area (ees 14 -		1
	a lattiyodarik) i se jasi _d isələr	en a co	Area (certification -			1 per 1
	a lattiyodarik) i se jasi _d isələr	en a co	Area (certification -		111 111	1 per 1
	a latti yoo a ta	en a co	Area (certification -			1 (m) (m)
	a latti yoo a ta	en a co	Area (certification -		n ander en an 1 fe	1 per 1
	a latti yoo a ta	en a co				e tanaka eo ar 1 fe	1 per 1
Concerning and and an an and an an an a	a latti yoo a ta	en a co				1000 m = 10	1 per 1
	a latti yoo a ta	en a co				1 an aire	1 per 1
Concernance of the second seco	a latti yoo a ta	en a co				e tanaka es ara 1 fe	1 per 1
	a latti yoo a ta	en a co				- 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1	1 per 1
	and a second at the second at	en a co	tan Ger I (, M Parter I Parter I	an formation and	an e		
	Annual Contraction of	Pre d 3- d		an formation and	1999 Ford		
Contract of the second	Energy Field		tan Ger I (, M Tarter Parter I	an formation and	Harris I I Harris		
	Annual Contraction of	Pre d 3- d	tan Ger I (, M Tarter Parter I	an formation and	Harris I I Harris		
Contract of the second	Energy Field		tan Ger I (, M Tarter Parter I	an formation and	Harris I I Harris		
Conservations and the second s	Annual and an		tan Ger I (, M Tarter Parter I	an formation and	Hereiter	inner Transier Dielet ner op ski	
Control of the second s	Annual and an		tan Ger I (, M Tarter Parter I	an formation and	HERE IN THE PARTY OF THE PARTY	innin innin Director option Director option	
Conservations and the second s	Annual and an		tan Ger I (, M Tarter Parter I	an formation and	Hereiter	innin innin Director option Director option	

Encryption: WPG Adv/Ent Implementation

≻Inbound:

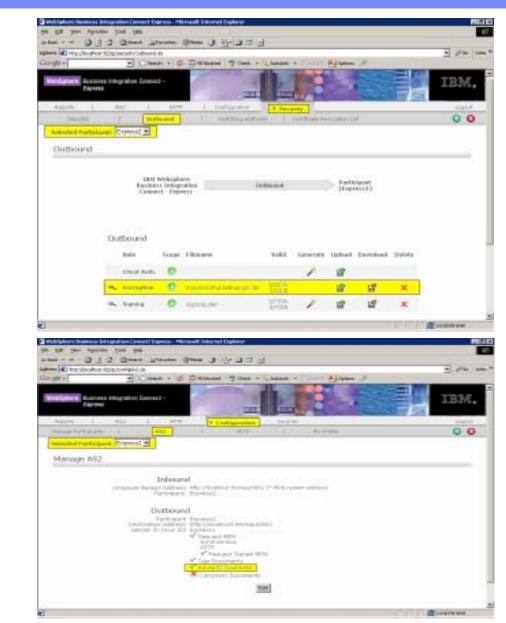
- Load company.p12 as Hub Operator's PKCS12 Encryption certificate
- Enable "AS Encryption" in the Participant Connection
- Send certificate to the Participant



Encryption: WPG/WBIC Express Implementation

≻Outbound:

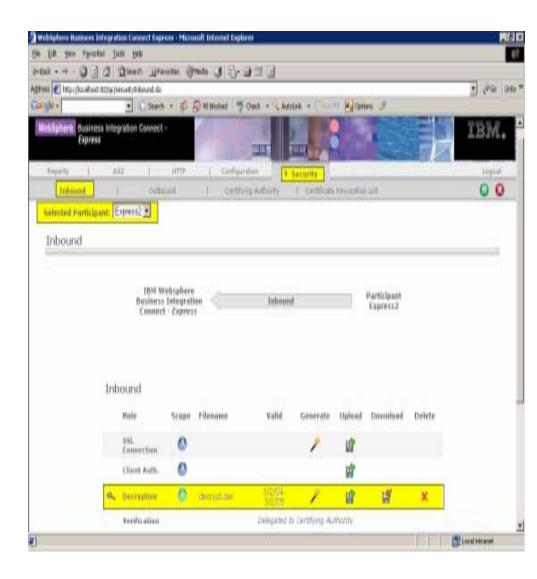
- Upload Participant certificate in Security>Outbound
- Enable Encryption for the Participant outbound documents



Encryption: WPG/WBIC Express Implementation

≻Inbound:

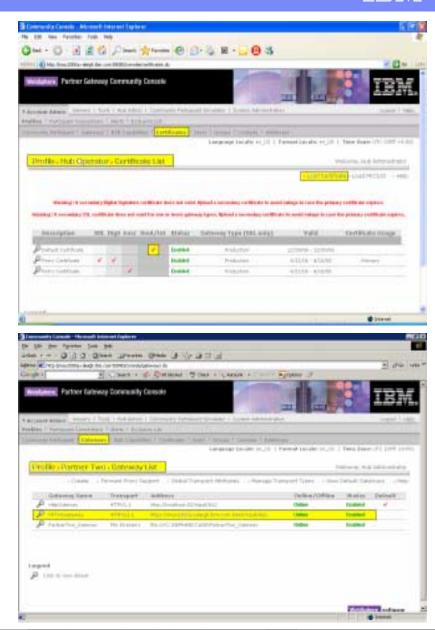
- Upload or Generate a .p12 certificate keypair
- Download the certificate and send it to the Partner



Server Authentication: WPG Adv/Ent Implementation

≻Outbound:

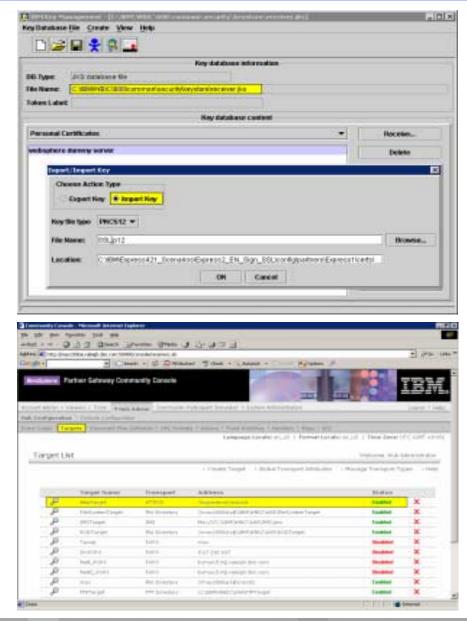
- Load Participant certificate as Hub Operator's root certificate
- Define a HTTPS Gateway in the Participant's profile
- Select that HTTPS Gateway for the Participant Connection between ComMgr and Participant



Server Authentication: WPG Adv/Ent Implementation

≻Inbound:

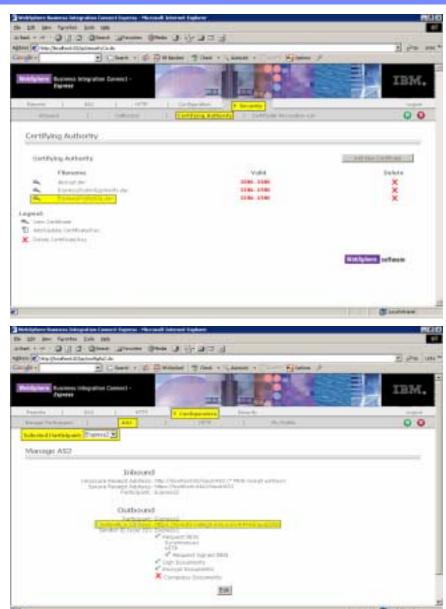
- Import company.p12 to the receiver.jks keystore
- Define an HTTPS Target
- Make sure the secure port (default 57443) has been defined at installation time and is active)



Server Authentication: WPG/WBIC Express Implementation

≻Outbound:

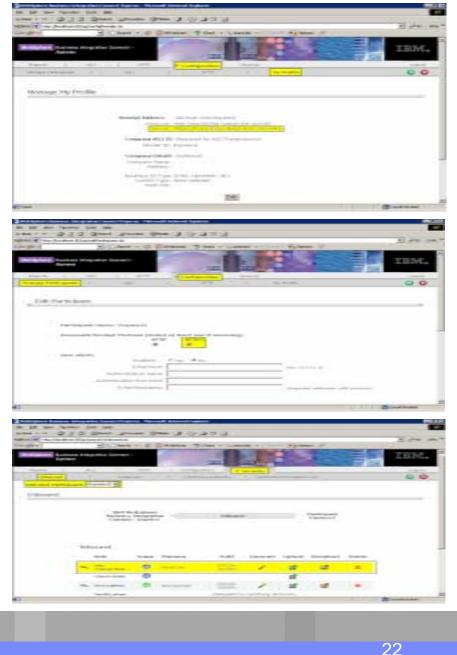
- > Add Participant Certificate in Security>CertifyingAuthority
- In Configuration>AS2 update the Participant outbound destination address, i.e.: https://ipaddr:5443/input/AS2



Server Authentication: WPG/WBIC Express Implementation

≻Inbound:

- Enable HTTPS domain for Express
- Check HTTPS box for the Participant
- Upload or generate the keypair.
- Download the certificate and send it to the Participant



- Client Authentication: WPG Adv/Ent Implementation >Outbound:
 - Load company.p12 as Hub Operator PKCS12 'SSL Client' certificate
 - Define a HTTPS Gateway in the Participant's profile
 - Select that HTTPS Gateway for the Participant Connection
 - Send the Certificate to the Participant

annen villa en de Letter
annen villa en de Letter
and a local sector of the
and a second second
a set for paragenetical range.
Continues (Songe)
ana Perat
eW.
2 100 1
STATE OF STREET
IBM
Internet internet has
1112-23613
PLUE 1. New York 175, 1991 ADDR
Sectores, Sold Sciences and
 March March 1991 (1997) and Southerness, took Spin and adar March Salard, Spin and Street
Sectores, Sold Sciences and
transminist Schember Vereiter Schember Reise Schember
Summer, to A. Marson Anton I. Vere Table A. Sanamarer

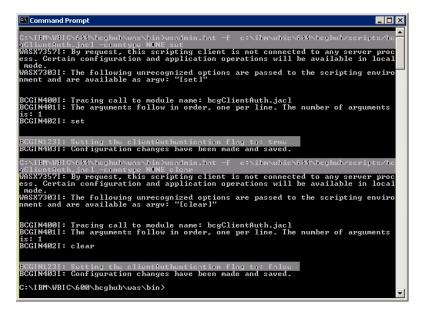
Client Authentication: WPG Adv/Ent Implementation >Inbound:

- Load Participant certificate (CA or self-signed) in receiverTrust.jks
- Run bcgClientAuth script to enable Client SSL

Turn Client Authentication ON: bcghub/was/bin/wsadmin.sh –f bcghub/scripts/bcgClientAuth.jacl conntype NONE set

Turn Client Authentication OFF: bcghub/was/bin/wsadmin.sh –f bcghub/scripts/bcgClientAuth.jacl conntype NONE clear

		Key database information		
A hyper Justi antes		and the second		
A CONTRACTOR OF A CONTRACTOR OFICACTOR OFICIONO OFICIA CONTRACTOR OFICACTOR OF	CERCE STREET BUILD	Ways and the second		
kee Labet				
		Ray database content		
gare Certificates			*	AM.
ALCA's Dentils of a line	matte			
hala type	Binary (ICH mata			
ertificate file exercit	and der			fromse.
AC 490(4)	Transferrance.	all-state.		1
		UK Cancel		
	prinary certification as	1		





Client Authentication: WBIC/WPG Express Implementation

≻Outbound:

- Upload or Generate a .p12 certificate keypair
- Download the certificate and send it to the Partner

Terbilghere Bankers		farmer 1	inseed interest factors					-		
Q - 1- 101-1	1 1 Quest	p.huiyahuai	1999ada () ()- ()-) of Capacitor an O () () () () () () () () () () () () ()	alanan s	0-#1	California (,		1.24	444
WebSphern Inc. Trav	nuus krisgrudden Con ###	wet-	-			5		THE R	IBM.	
Frink 1	107		Contraction of the second seco	t treat					Lipsi	1
Intered Parts	lovel. partner/line -	i i i i i i i i i i i i i i i i i i i	II. Collespital	NAME OF BRIDE	elfonti li el	100900-10	F1		0 0	-
Outbound										
	10 Duci Cue	4 Webspi Hoss Jubsc Absc2 - 63g	uru protuk protu	Outsiand		Partici Luorth	paer erOne)			
	Outbound Pate		Hanna	Vulla	Gainerato	Uptions	Involut	Datate		
	the Almost Alm	- 0	HOP	期時	1	ġ,	đ	x		
	A. Enrypha	. 0	where in discretions	4144.444		đ	đ	х		
	1 110111	0	Intractarticity. Init	4/14/01- 4/14/01	1	ut.	11	x		
		-							d breret.	7

Client Authentication: WBIC/WPG Express Implementation 1/2

≻Inbound:

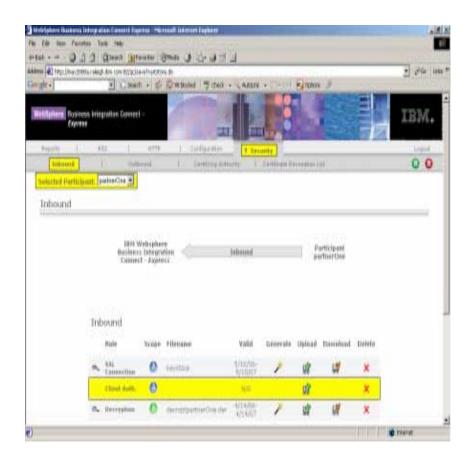
- Create a truststore to import the Participant certificate.
- Copy the certificate in Express folder: \jre\bin
- Use "keytool" to add the certificate into a truststore

Command Permpt		-	
CENTRENERGY To Mindows Hul	Express_partnerTuo\jr	whin hout out -	Laport - hoursto
Fater Reystore password: nas Owner: EMBILADDNESS-maxtBus. MMa	16100		
Issuer: EMAILADDRESS-maxtPus. BBBa	ibm.con, C=US, ST=NC,	L-RTP, OU-WPG,	0-1BH, CH-max2
Terial number: -560ab0dof4ff Valid from: Ved May 10 22:38: Certificate fingerprint: HD5: A1:00:34:21:62	2:CF:00:DD:55:CD:90:F0: 0:61:71:31:F3:40:E9:1F:	1A:98:2D:E1	
Certificate was added to keys			
TC/10M/Express_To_Windows_Indvfc			.0
He Edit View Pavorites Tools He	9	1.	
He Edit View Pavorites Tools He	9 den Ø № 9:×49 I	J•	
He Eak Vew Pavorkes Tools He J+Back • → - 🔄 🛱Search 💁 Po	9 den Ø № 9:×49 I]. 3ce 1400	
File Edit Vew Favorites Tools He d+Back • + • • 😭 🛱 Search 💁 Pc Address 🖼 C/UBMExpress To, Windows H	n stors J Al Ri X an I Alfopress, partner Twolpelton X Norme Data q.dl	3ce Type 01 KD Application Ext	Mudified
Hie Edit Vew Favorites Tools He d+Back + +	Norman Aliferte Contraction (Contraction) Aliferte Contraction (Sco Type 91 KB Application Ext 1 KB Security Certif	Modified 1 7/9/2003 4:26 AV 1 5/10/2006 10:401
Hie Edit Vew Favorites Tools He d+Back • + - • • • • • • • • • • • • • • • • •	n stors J Al Ri X an I Alfopress, partner Twolpelton X Norme Data q.dl	3ce Type 01 KD Application Ext	t 7/9/2003 4:26 AV

Client Authentication: WBIC/WPG Express Implementation 2/2

≻Inbound:

- Upload the truststore in Express Security "Inbound" section for Client Authentication:
 - ➢ Note: The truststore won't be listed under 'Filename' column. The only thing changed is the 'Valid' column which now shows "N/A".









Managing Certificates WBIC/WPG Adv/Ent Ikeyman utility 1/5

Ikeyman utility can be used to manage certificates:

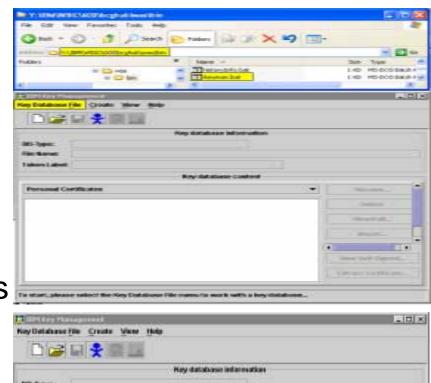
Create Self-Signed Certificates

Import/Export Certificates

>Add/Delete Certificates

≻Etc…

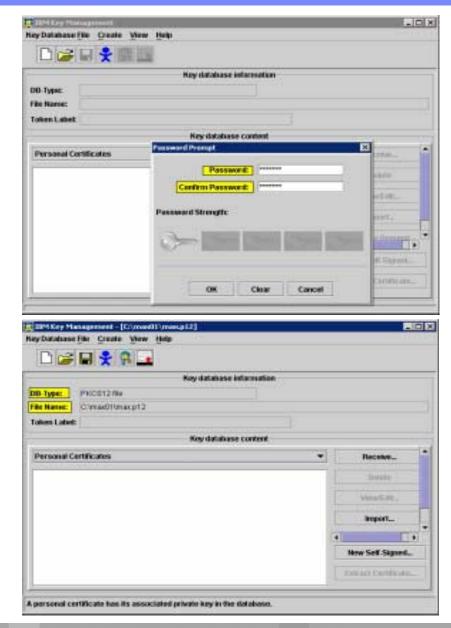
I.E.: Create Self-signed certificates
 Step 1: Create a new keystore



	3 m + 1			
	·			
		Hay database in	facerson.	
Name:				
kenLabet				
		Key database	content	
	1977	my us acese	canen	
ersanal Certifica	625			PPCINE_
				Debte-
New .				8
A CONTRACTOR OF	PRCS12 +			
Tray of a second of	Parcate +			
File Name:	macp12			Downe
Location	Ctimar011			
the second s	I I WARD IN AN	CK	Cancel	

Managing Certificates WBIC/WPG Adv/Ent Ikeyman utility 2/5

- Create Self-signed Certificates continue:
 - Step2: After providing the keystore filename and location, type-in your password
 - Step3: The new keystore is now created



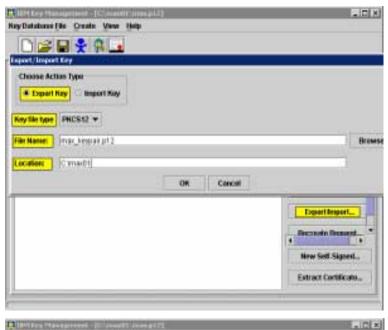
Managing Certificates WBIC/WPG Adv/Ent Ikeyman utility 3/5

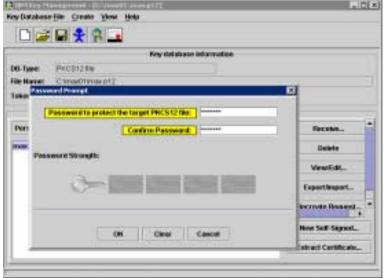
- Create Self-signed Certificates continue:
 - Step4: Create a Self-signed certificate providing the required values
 - Step5: The new Certificate is created and resides in our keystore.

lease provide the followi	ing:	
Key Label	max2000a	
Version	X509 V3 🔻	
Key Size	1024 🔻	
Common Name	max2000a.raleigh.ibm.com	
Organization _	WPG	
Organization Unit (opti	ional)	
Locality (opti	ional)	
State/Province (opti	ional)	
Zipcode (opti	ional)	
Country or region	US 🔻	
Validity Period	365 Days	
	OK Reset Cancel	
		New Self-Si
		Extract Certi
y Management - DC//ree		
lese file Greate View	w Hole	
use file Greate View	∎ ■	
ana ija Cranto Ver	w Hole	
Pricenzaw	er Hole E Key datatase biorratee	
Pacifit Grand You Pacifit Ste Chanditmarphi	er Hole E Key datatase biorratee	
ese jike Granto Yeo	er Hole Koy statutusor information F	
Paccal Sta Paccal Sta Chronol Throad ph 1 Seen	er Hole E Key datatase biorratee	
Paccal Sta Paccal Sta Chronol Throad ph 1 Seen	er Hole Koy statutusor information F	Facal
PROBILISM PROBILISM Chromotowarphi ad Certification	er Hole Koy statutusor information F	
PECETIZENE	er Hole Koy statutusor information F	Delet
PECETIZENE	er Hole Koy statutusor information F	Debt
All Certifications	er Hole Koy statutusor information F	Date:
All Certifications	er Hole Koy statutusor information F	Delet Vented
The second se	er Hole Koy statutusor information F	Facular Date: VessEd Experting How Set S
ese file greate you Peoping the Peoping the Commontwarphi and Centification	er Hole Koy statutusor information F	Dates Venalid Exporting

Managing Certificates WBIC/WPG Adv/Ent Ikeyman utility 4/5

- Create Self-signed Certificates continue:
 - Step6: The keypair can now be exported to a file and used with our application
 - Step7: Provide the password to protect the access to the private key

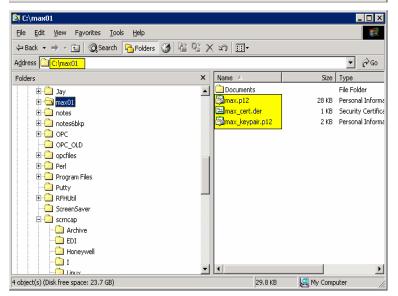




Managing Certificates WBIC/WPG Adv/Ent Ikeyman utility 5/5

- Create Self-signed Certificates continue:
 - Step8: Extract the Certificate to be sent to the Participant
 - Step9: Find Keystore, P12 and Certificate in the specified location

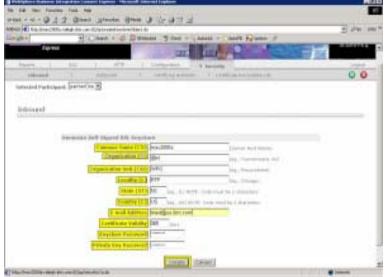
)ata type	Binary DER data	•			
<mark>ertificate file na</mark>	me: max_cert.der				
ocation:	C:\max01				
		ОК	Cancel		
		Key database con	tent		
			Kon		
Personal Cert	ficates		KEIK	•	Receive
	ficates			•	Receive Delete
	<mark>ficates</mark>			•	
	ficates			•	Delete
	ificates			•	Delete View/Edit
Personal Certi max2000a	ficates			•	Delete View/Edit Export/Import



Managing Certificates WBIC/WPG Express Built-in utility 1/2

- The Express version allows the user to upload/download or create certificates
- To create a self-signed certificate:
 - Step1: Click on the "magic wand" to generate the keypair
 - Step2: Provide the requested information

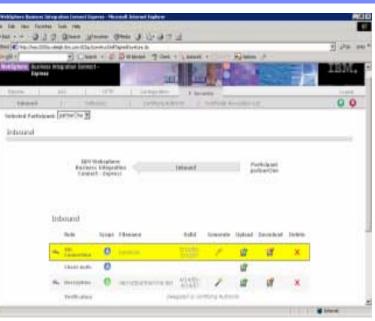




Managing Certificates WBIC/WPG Express Built-in utility 2/2

- Create a self-signed certificate continue:
 - Step3: The certificate information are reported for the desired level of security
 - Step4 Download the Certificate to be sent the Participant











Questions and Answers

