



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

Agenda

- **Digital Signature – Basic Concepts** 3-4
- **Encryption – Basic Concepts** 5-6
- **Client/Server Authentication – Basic Concepts** 7-8

- **Digital Signature – WBIC/WPG Adv/Ent Implementation: Outbound** 10
- **Digital Signature – WBIC/WPG Adv/Ent Implementation: Inbound** 11
- **Digital Signature – WBIC/WPG Express Implementation: Outbound** 12
- **Digital Signature – WBIC/WPG Express Implementation: Inbound** 13

- **Encryption – WBIC/WPG Adv/Ent Implementation: Outbound** 14
- **Encryption – WBIC/WPG Adv/Ent Implementation: Inbound** 15
- **Encryption – WBIC/WPG Express Implementation: Outbound** 16
- **Encryption – WBIC/WPG Express Implementation: Inbound** 17

- **Server Authentication – WBIC/WPG Adv/Ent Implementation: Outbound** 18
- **Server Authentication – WBIC/WPG Adv/Ent Implementation: Inbound** 19
- **Server Authentication – WBIC/WPG Express Implementation: Outbound** 20
- **Server Authentication – WBIC/WPG Express Implementation: Inbound** 21

- **Client Authentication – WBIC/WPG Adv/Ent Implementation: Outbound** 22
- **Client Authentication – WBIC/WPG Adv/Ent Implementation: Inbound** 23
- **Client Authentication – WBIC/WPG Express Implementation: Outbound** 24
- **Client Authentication – WBIC/WPG Express Implementation: Inbound** 25-26

- **Managing Certificates for WBIC/WPG Adv/En: Ikeyman utility** 28-32
- **Managing Certificates for WBIC/WPG Express: Built-in utility** 33-34

- **Q/A** 35

Digital Signature – Basic Concepts 1/2

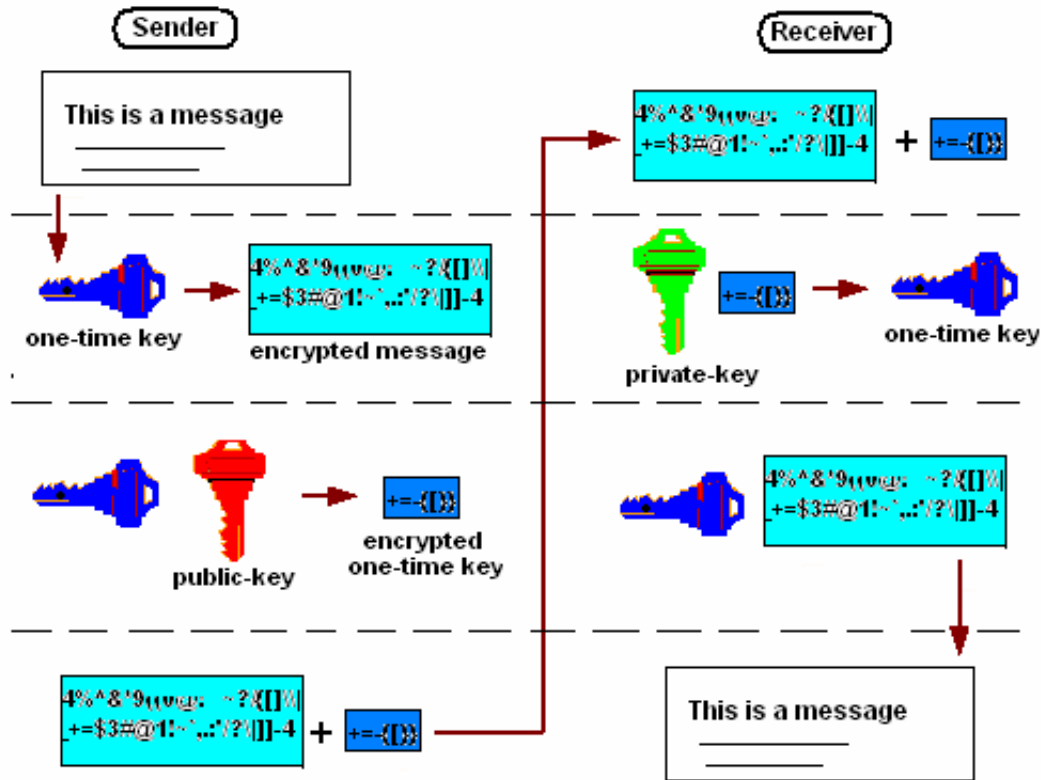
- Uses "public-key cryptography" algorithm
- Signing a document
 - The content of the message is "hashed"
 - The "hashed" message is processed by the Private-key to produce a "Digital Signature"
 - The Digital Signature is attached to the message and sent with it
- Signature Verification
 - "Hashes" the message received
 - Uses the public-key to decrypt the Digital Signature
 - Compares whether the 2 hashes match

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

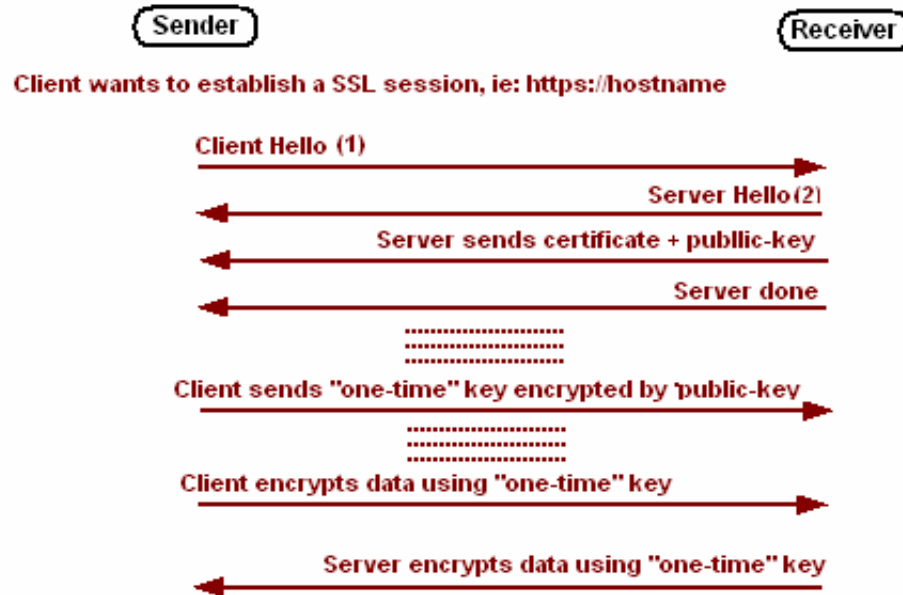
Encryption – Basic Concepts 2/2



Client/Server Authentication - Basic Concepts 1/2

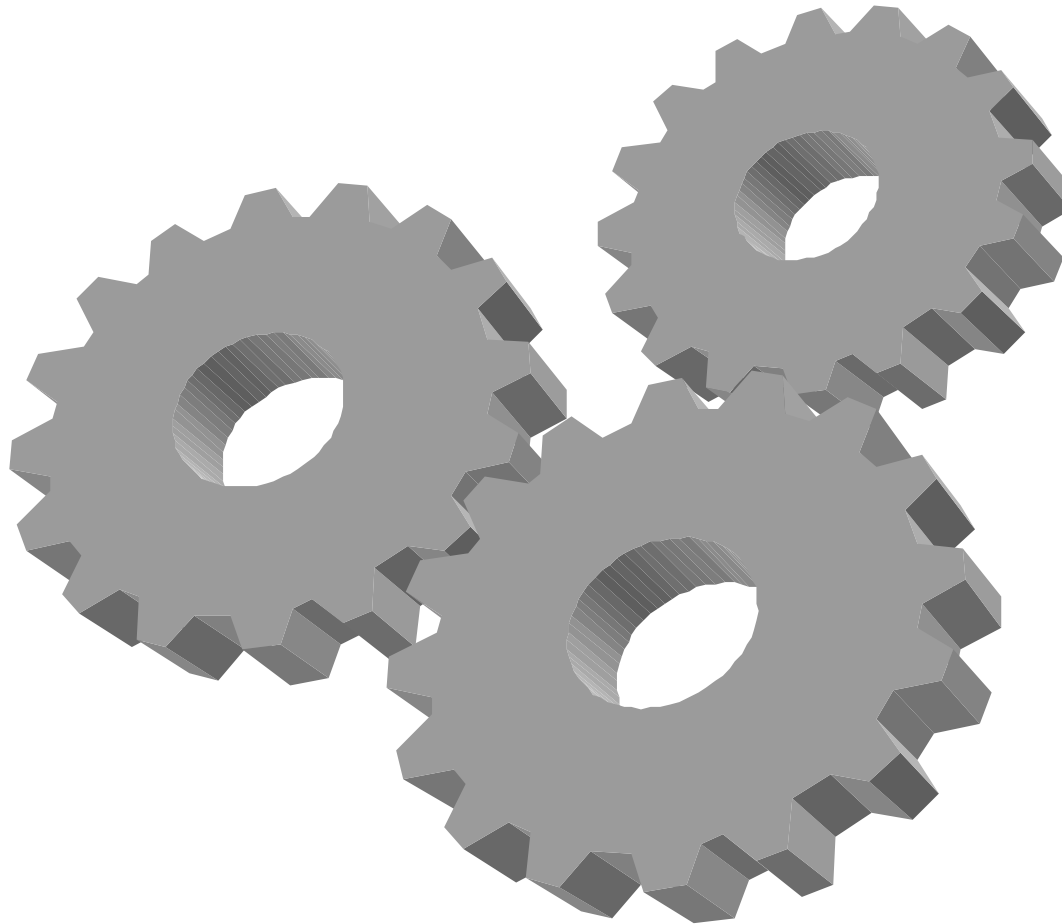
- Certifies the identity of the Server/Client in session
 - The Client starts a SSL session with the Server
 - The Server sends its certificate
 - The Client verifies the Server certificate
 - The Client sign and sends its certificate
 - The Server verifies the Client certificate
 - The Client sends 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

The top screenshot shows the 'Certificates List' page in the IBM Security Console. It displays a table of certificates with columns for Description, SSL, Digi, Cert, Root/PA, Status, Gateway Type (SSL only), Validity, and Certificate Usage. Two 'Proxy Certificate' entries are visible, both with a status of 'Enabled'.

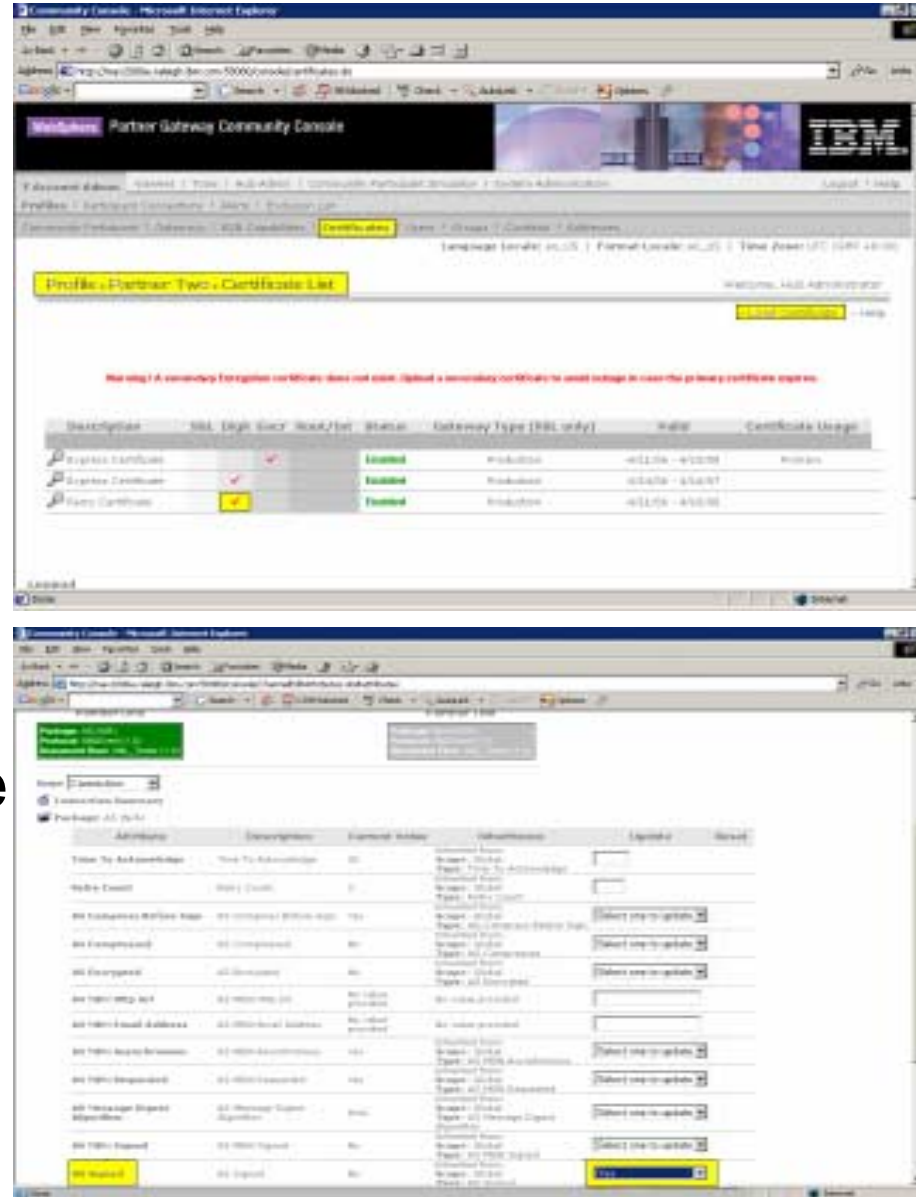
Description	SSL	Digi	Cert	Root/PA	Status	Gateway Type (SSL only)	Validity	Certificate Usage
Proxy Certificate	✓	✓	✓	✓	Enabled	Proxy	4/12/06 - 4/12/09	Proxy
Proxy Certificate	✓	✓	✓	✓	Enabled	Proxy	4/12/06 - 4/12/09	Proxy

The bottom screenshot shows the 'Participant Connection' configuration page. It features a table with columns for Description, Description, Connection Status, and Subscriptions. The 'AS Signed' checkbox is highlighted in yellow, indicating it is checked.

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



The top screenshot shows the 'Profile - Partner Two - Certificate List' page. A red error message states: 'No way! A secondary Enterprise certificate does not exist. Upload a secondary certificate to avoid outage to cover the primary certificate outage no.' Below this is a table of certificates:

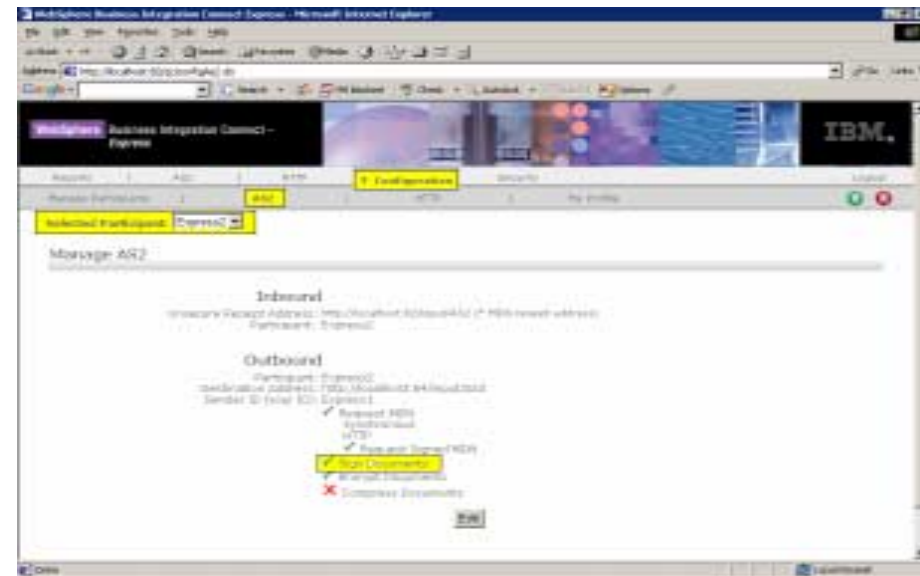
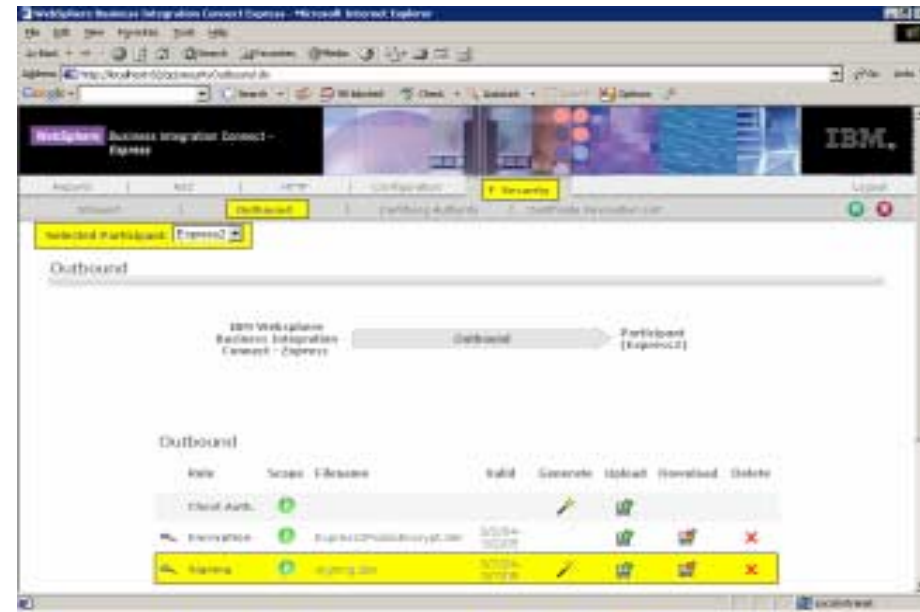
Description	SSL Sign Cert	Root/Int	Status	Gateway Type (SSL only)	Valid	Certificate Usage
Enterprise Certificate	<input type="checkbox"/>	<input type="checkbox"/>	Enabled	Production	4/11/06 - 4/12/08	Sign
Enterprise Certificate	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Enabled	Production	12/12/06 - 12/12/07	Sign
Trust Certificate	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Enabled	Production	4/11/06 - 4/12/08	Sign

The bottom screenshot shows the 'Participant Profile' page. The 'AS Signed' checkbox is highlighted in yellow, indicating it is checked. The page lists various connection parameters such as 'Title To Acknowledge', 'Media Event', and 'AS Transport'.

Digital Signature: WPG/WBIC Express Implementation

➤ Outbound:

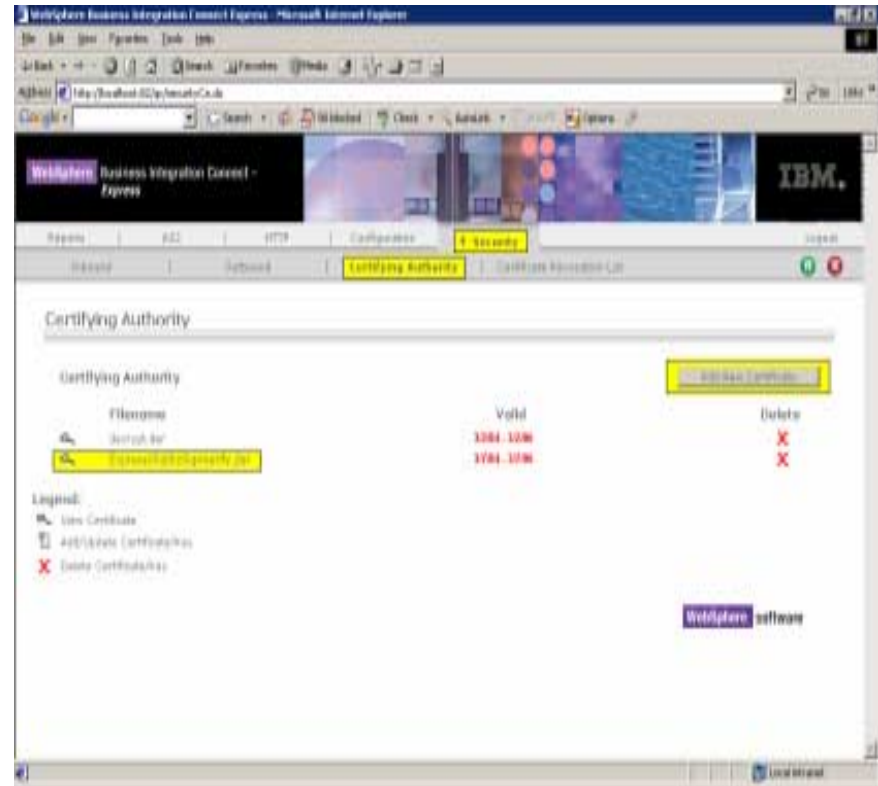
- Upload or generate a .p12 keypair
- Download the certificate and send it to the Partner
- Enable Digital Signature for outbound documents



Digital Signature: WPG/WBIC Express Implementation

➤ Inbound:

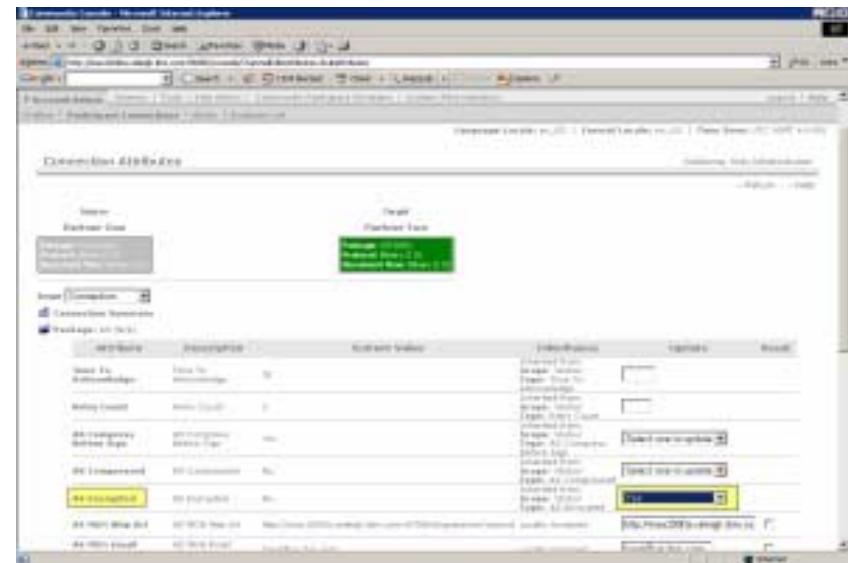
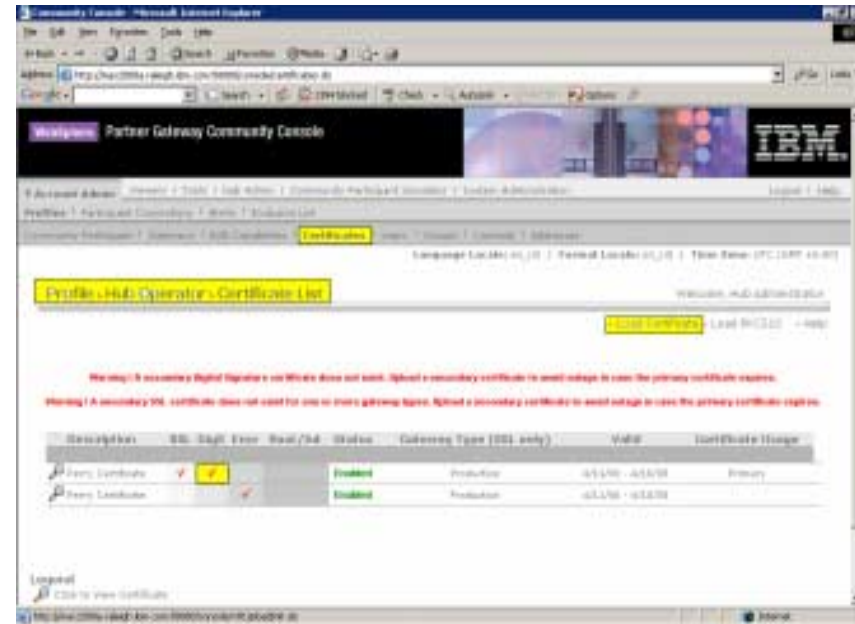
- Add the Partner certificate in the “Certifying Authority” list



Encryption: WPG Adv/Ent Implementation

➤ Outbound:

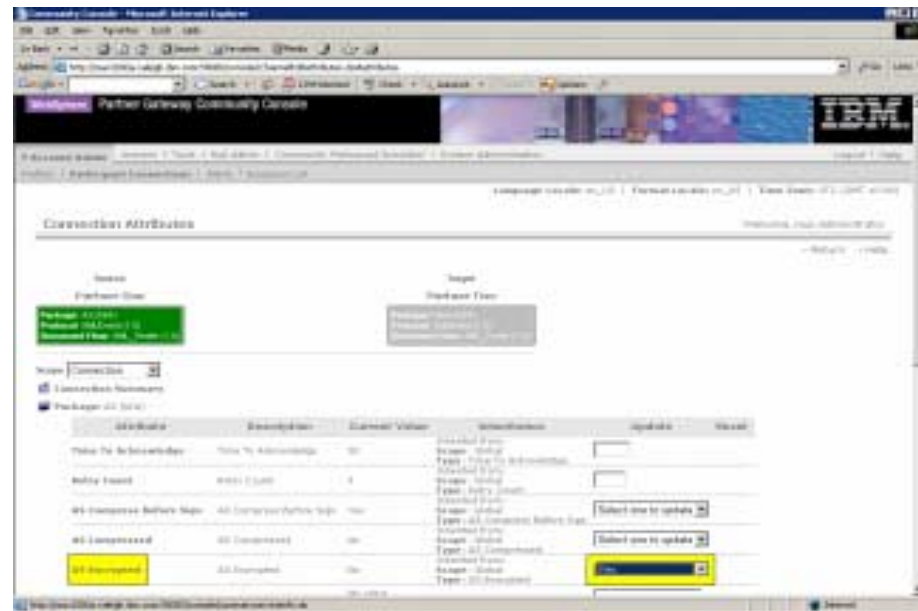
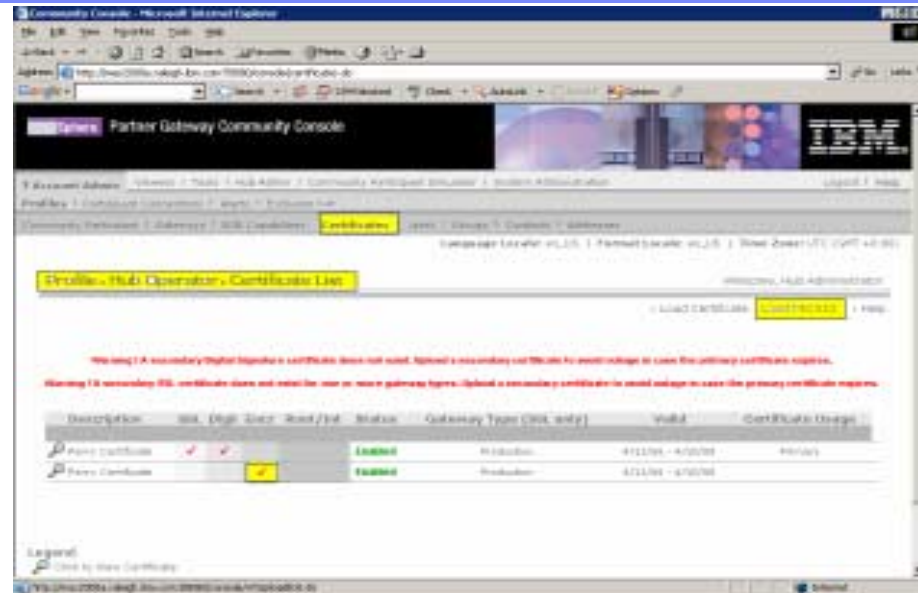
- Load Participant certificate in the Participant profile as encryption certificate
- If signed by a CA, install the CA certificate in the Hub Operator profile, as root
- Enable “AS Encrypted” in the Participant Connection



Encryption: WPG Adv/Ent Implementation

➤ Inbound:

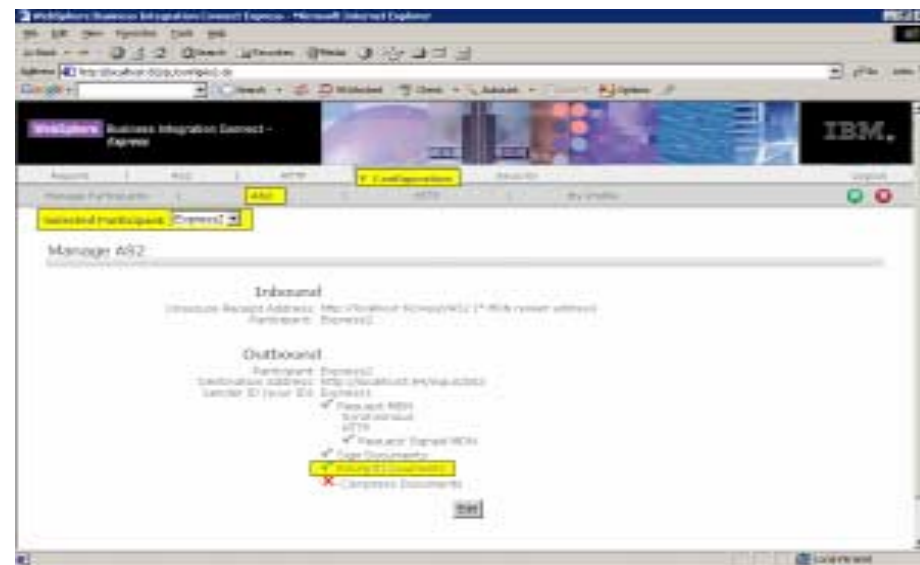
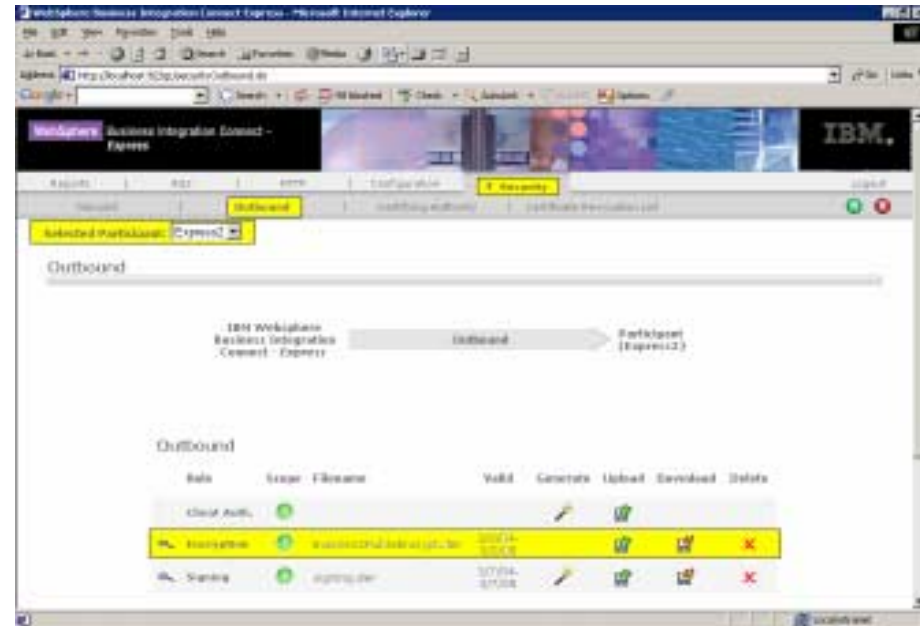
- Load company.p12 as Hub Operator's PKCS12 Encryption certificate
- Enable "AS Encryption" in the Participant Connection
- Send certificate to the Participant



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

The screenshot shows the IBM WebSphere Business Integration Connect Express Security configuration page in a Microsoft Internet Explorer browser. The page title is "WebSphere Business Integration Connect Express - Microsoft Internet Explorer". The address bar shows "http://localhost:8339/secure/inbound.do". The page has a navigation menu with tabs for Reports, All, HTTP, Configuration, Security, and Logout. The Security tab is active, and the "Selected Participant" is set to "Express2". The main content area is titled "Inbound" and shows a diagram of an inbound connection from "Participant Express2" to "IBM WebSphere Business Integration Connect Express". Below the diagram is a table of inbound connections:

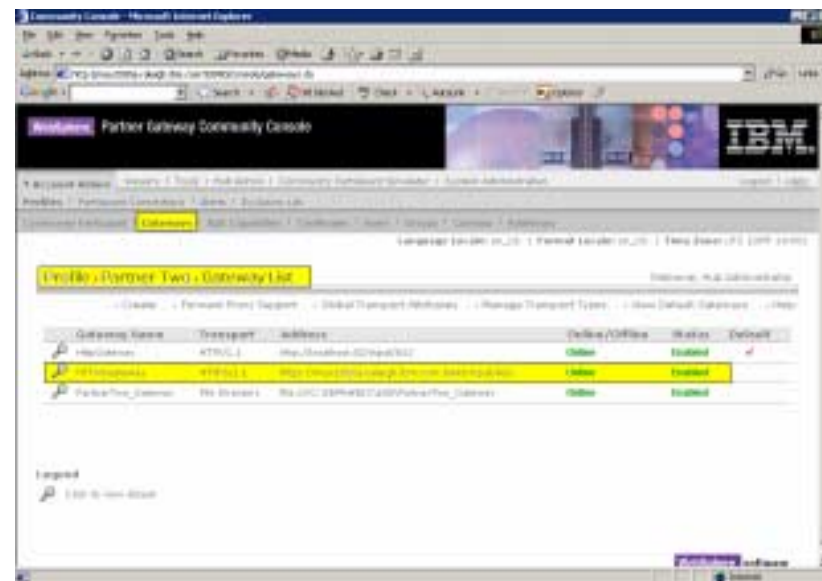
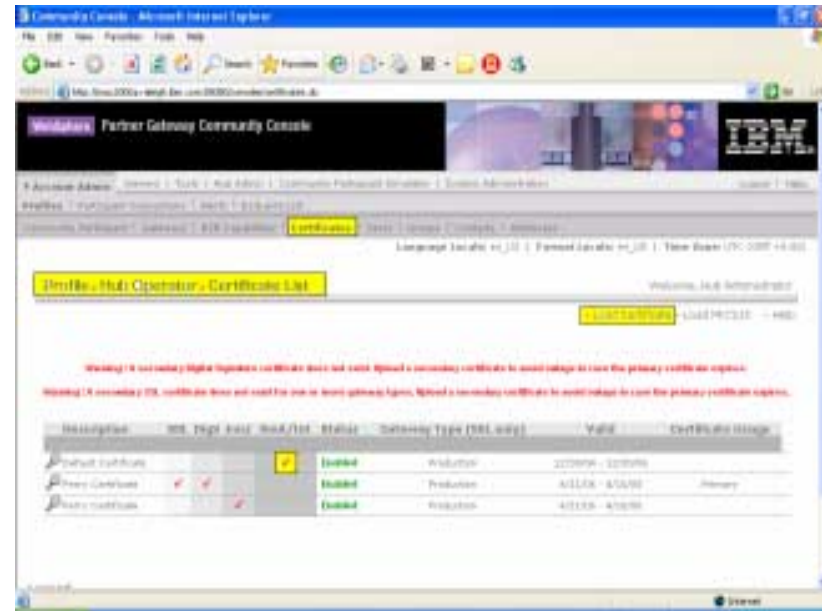
Role	Scope	Filename	Valid	Generate	Upload	Download	Delete
SSL Connection	A						
Client Auth.	A						
Decryption	A	decrypt.do	3/25/04-3/27/04				

Below the table, the "Verification" section is set to "Delegated to Certifying Authority".

Server Authentication: WPG Adv/Ent Implementation

➤ Outbound:

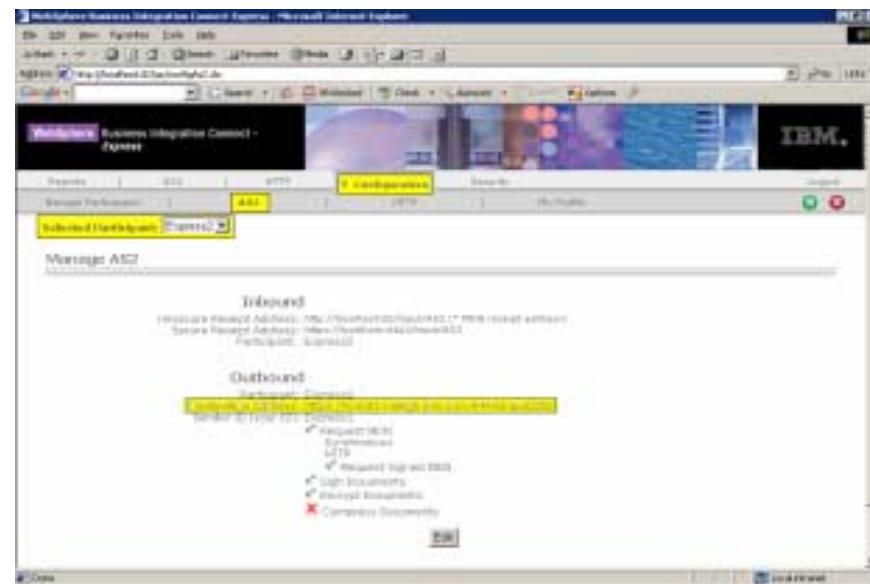
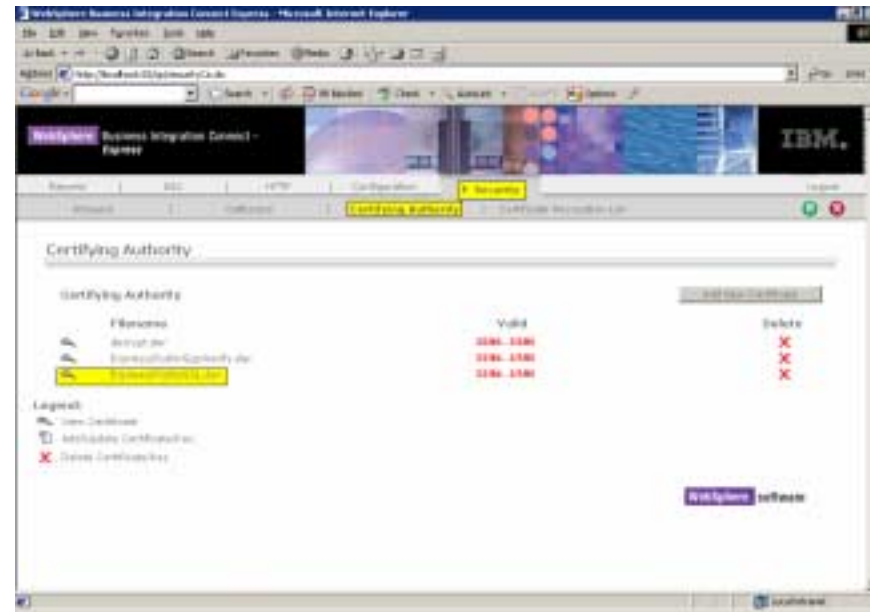
- Load Participant certificate as Hub Operator's root certificate
- Define a HTTPS Gateway in the Participant's profile
- Select that HTTPS Gateway for the Participant Connection between ComMgr and Participant



Server Authentication: WPG/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

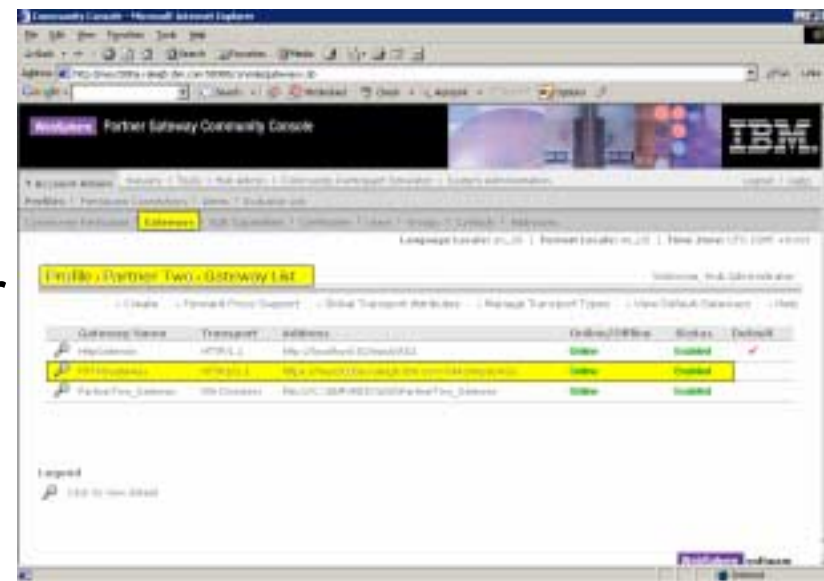
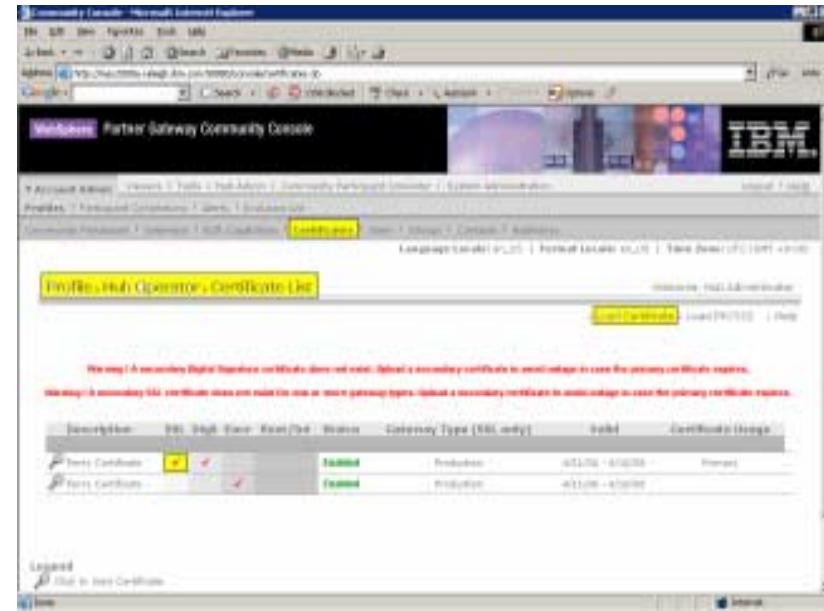
- Inbound:
 - Enable HTTPS domain for Express
 - Check HTTPS box for the Participant
 - Upload or generate the keypair.
 - Download the certificate and send it to the Participant



Client Authentication: WPG Adv/Ent Implementation

➤ Outbound:

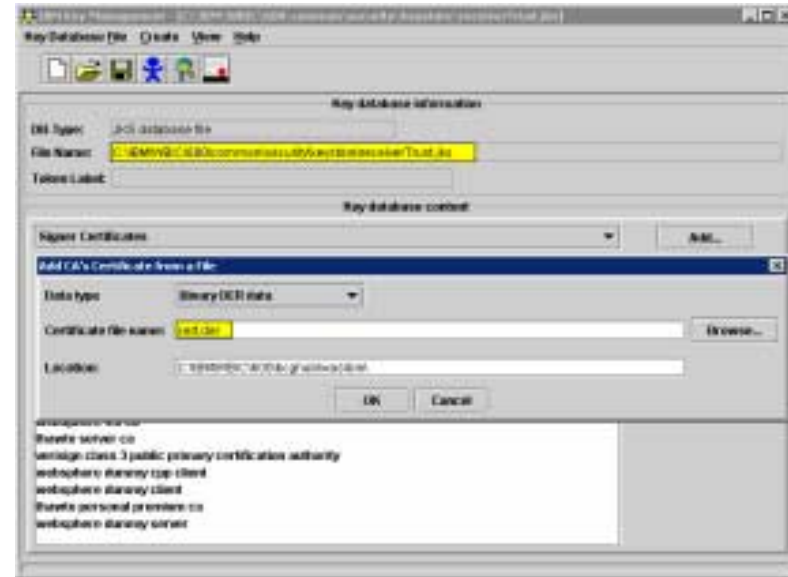
- Load company.p12 as Hub Operator PKCS12 'SSL Client' certificate
- Define a HTTPS Gateway in the Participant's profile
- Select that HTTPS Gateway for the Participant Connection
- Send the Certificate to the Participant



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



```

C:\IBM\WBI\600\bcghub\was\bin>wsadmin.bat -f c:\IBM\wbi\600\bcghub\scripts/bcgClientAuth.jacl -conntype NONE set
WASX7357I: By request, this scripting client is not connected to any server process. Certain configuration and application operations will be available in local mode.
WASX7303I: The following unrecognized options are passed to the scripting environment and are available as argv: "[set]"

BCGIN400I: Tracing call to module name: bcgClientAuth.jacl
BCGIN401I: The arguments follow in order, one per line. The number of arguments is: 1
BCGIN402I: set

BCGIN123I: Setting the clientAuthentication flag to: true
BCGIN403I: Configuration changes have been made and saved.

C:\IBM\WBI\600\bcghub\was\bin>wsadmin.bat -f c:\IBM\wbi\600\bcghub\scripts/bcgClientAuth.jacl -conntype NONE clear
WASX7357I: By request, this scripting client is not connected to any server process. Certain configuration and application operations will be available in local mode.
WASX7303I: The following unrecognized options are passed to the scripting environment and are available as argv: "[clear]"

BCGIN400I: Tracing call to module name: bcgClientAuth.jacl
BCGIN401I: The arguments follow in order, one per line. The number of arguments is: 1
BCGIN402I: clear

BCGIN123I: Setting the clientAuthentication flag to: false
BCGIN403I: Configuration changes have been made and saved.

C:\IBM\WBI\600\bcghub\was\bin>
  
```


Client Authentication: WBIC/WPG Express Implementation

➤ Outbound:

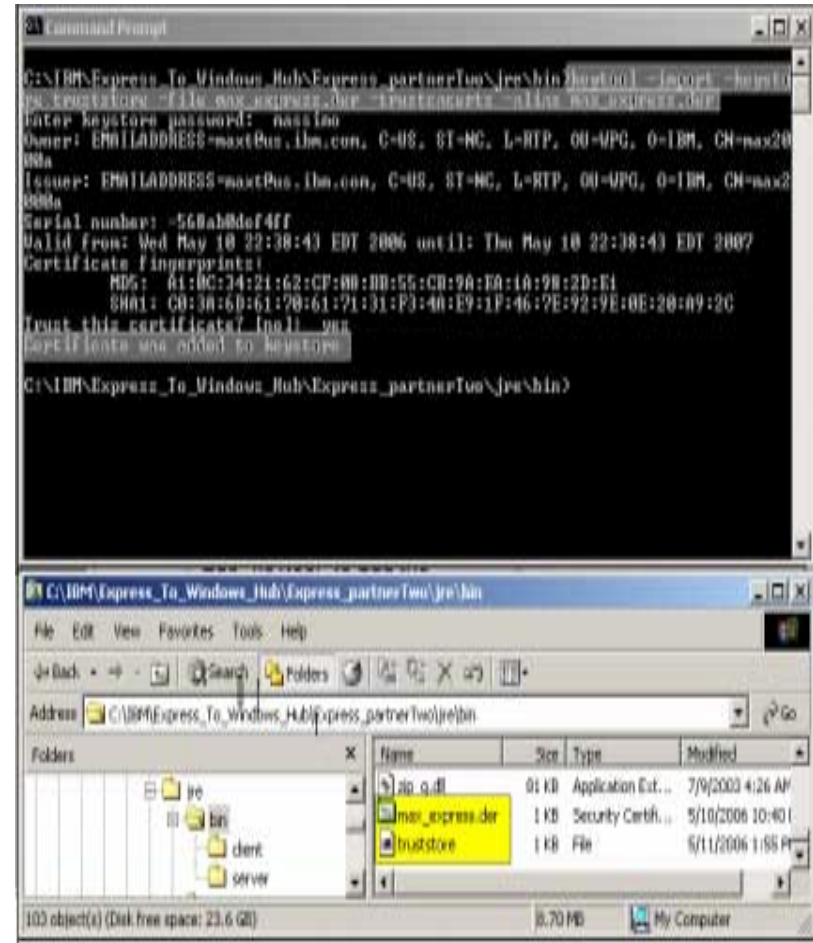
- Upload or Generate a .p12 certificate keypair
- Download the certificate and send it to the Partner

Name	Usage Flexion	Valid	Generate	Upload	Download	Delete
ClientAuth	client	11/05-01/06				
Exception	WBIOutPublicCertificate	11/05-01/06				
Signin	WBIOutPartnerOne	11/05-01/07				

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



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".

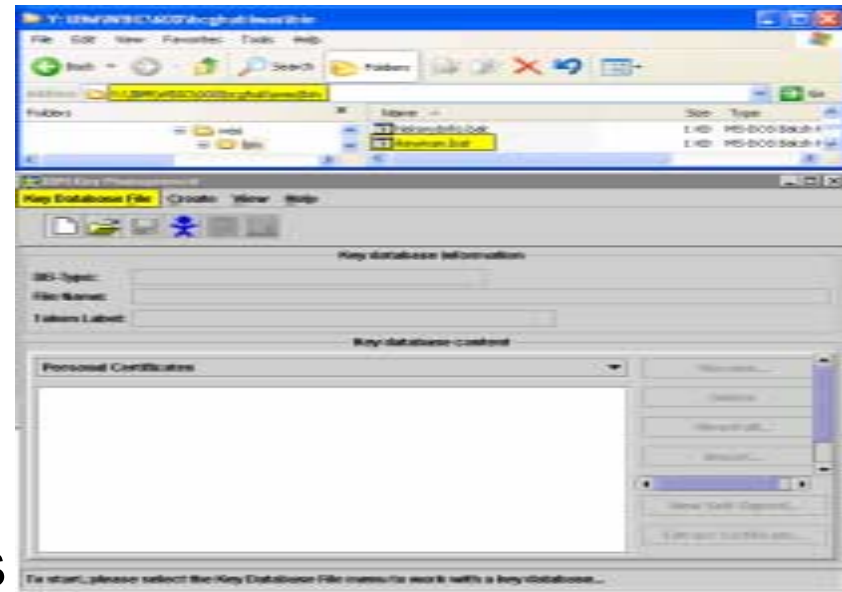
The screenshot shows the IBM WebSphere Business Integration Connect Express Security console. The 'Security' tab is selected, and the 'Inbound' section is active. A diagram illustrates the flow from 'Participant partnerOne' to 'Inbound' and then to 'IBM WebSphere Business Integration Connect - Express'. Below the diagram is a table listing the inbound configurations:

Role	Scope	Filename	Valid	Generate	Upload	Download	Delete
SSL Connection	Application	truststore	1/1/2008-8/1/2007				
Client Auth	Application	N/A	N/A				
Decryptor	Application	decryptorOne.jar	4/14/08-4/14/07				



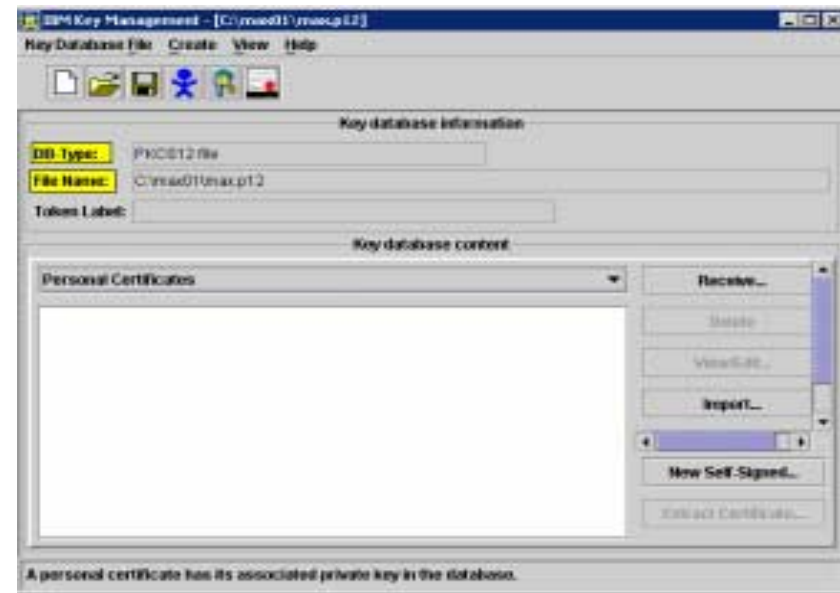
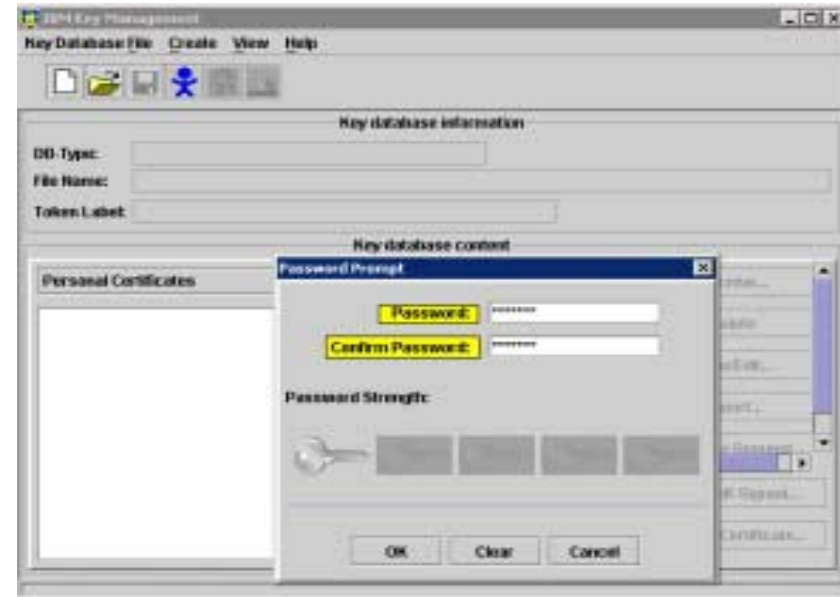
Managing Certificates WBIC/WPG Adv/Ent Ikeyman utility 1/5

- 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



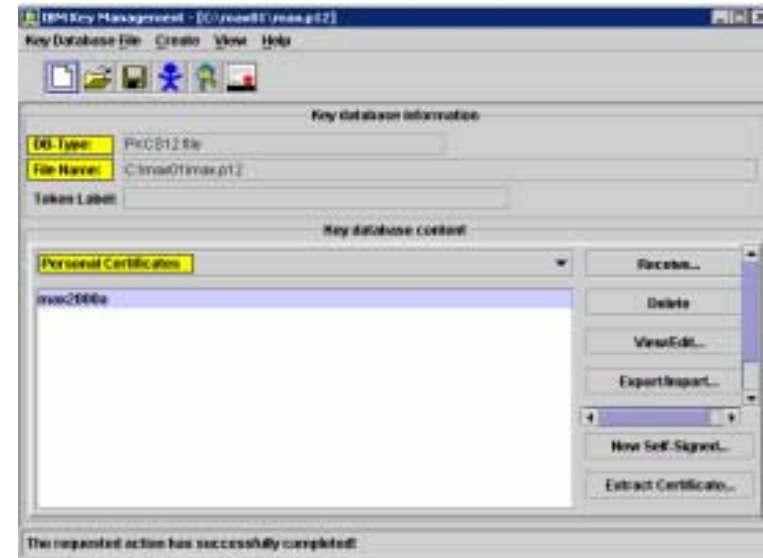
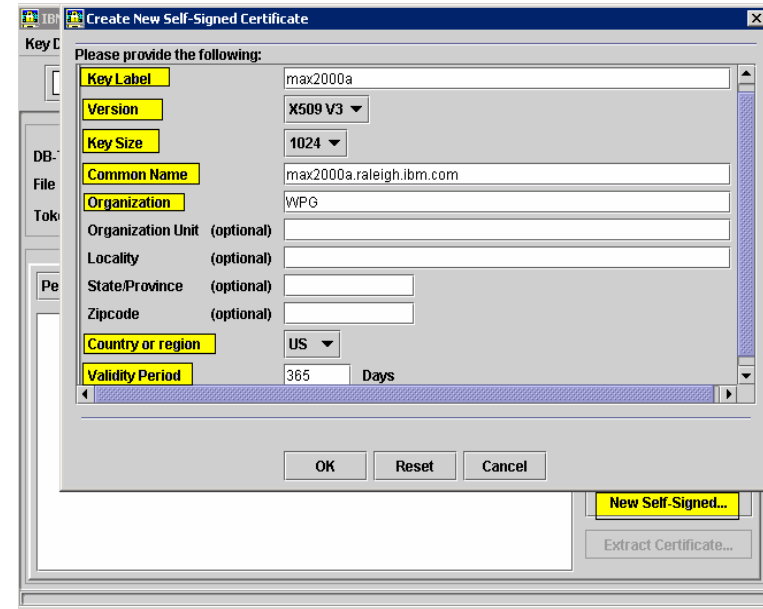
Managing Certificates WBIC/WPG Adv/Ent Ikeyman utility 2/5

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



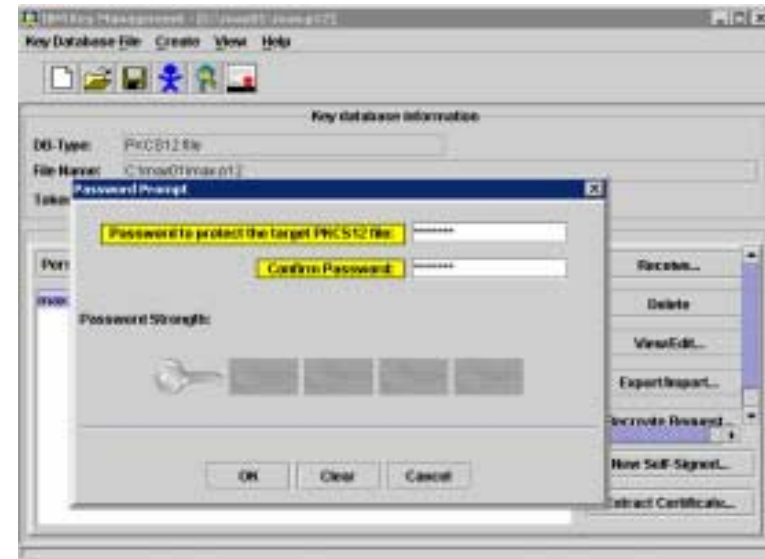
Managing Certificates WBIC/WPG Adv/Ent Ikeyman utility 3/5

- 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.



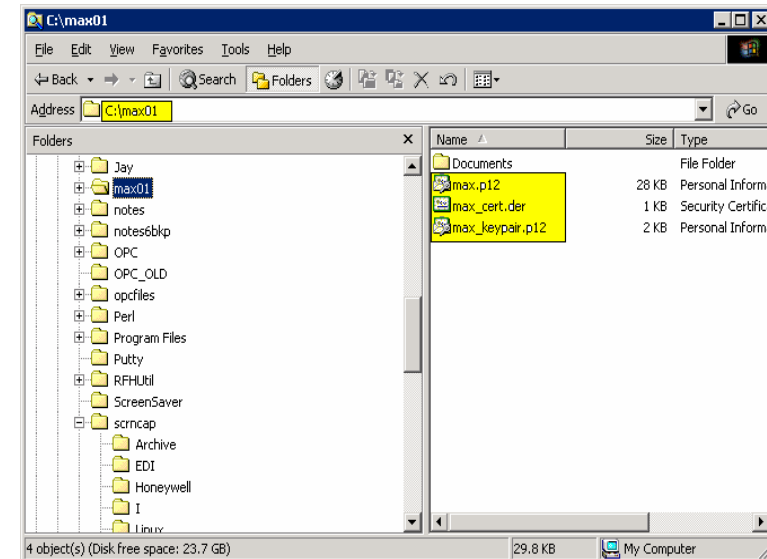
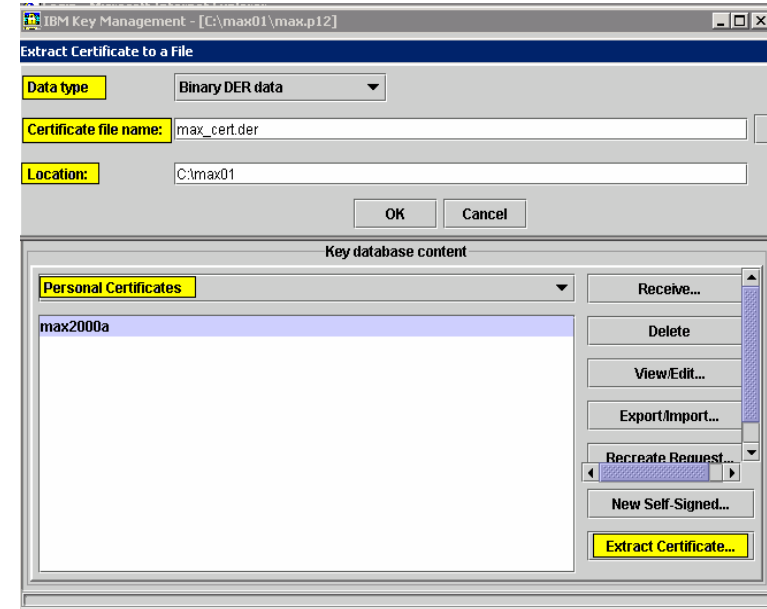
Managing Certificates WBIC/WPG Adv/Ent Ikeyman utility 4/5

- 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



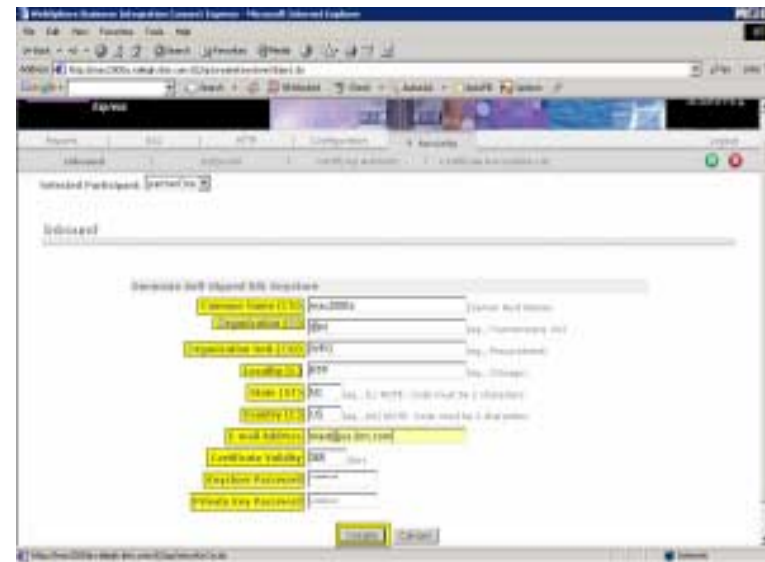
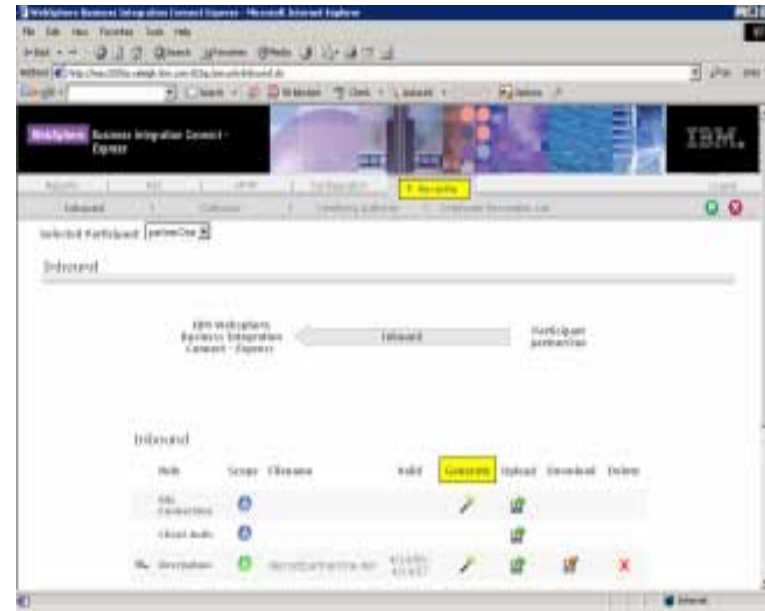
Managing Certificates WBIC/WPG Adv/Ent Ikeyman utility 5/5

- 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



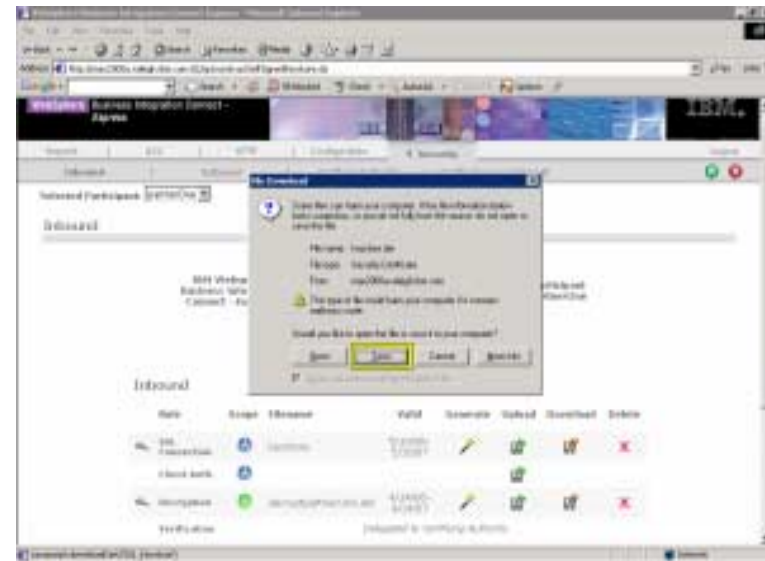
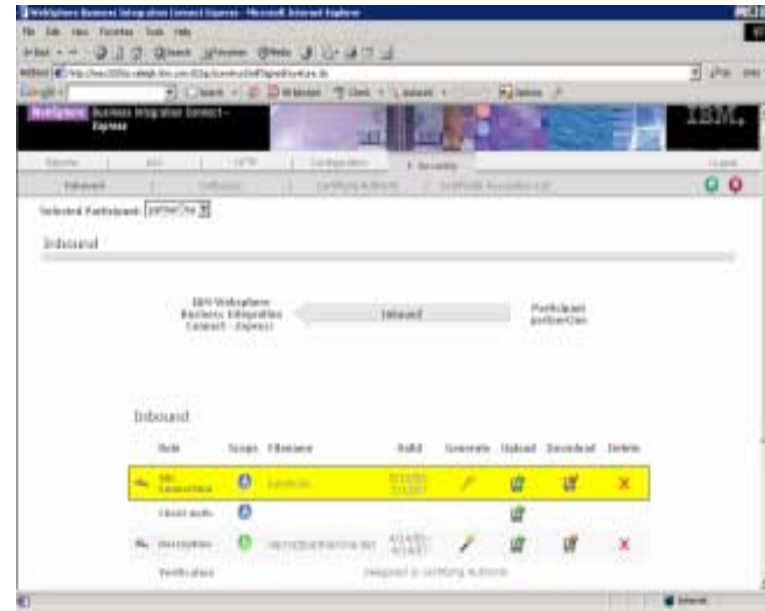
Managing Certificates WBIC/WPG Express Built-in utility 1/2

- 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