## Contents

1. Proven Solution to Automate B2B Transactions  
2. EDI over the Internet  
Hermes Business Messaging Gateway is a proven open-source solution for enterprises to automate business transactions with business partners through secure and reliable exchange of electronic documents (e.g., purchase orders). Hermes is secure; it allows you to encrypt and digitally sign the documents for transmission. Hermes is reliable; the sender can automatically retransmit a message when it is dropped in the network while the receiver can guarantee every message is delivered once and only once, and in the right order.
Electronic Data Interchange (EDI) was developed as the de facto standard for organizations to exchange business data. EDI is running on private networks and based on a cryptic protocol, which makes implementation complicated, expensive, and flexible. These disadvantages have limited the EDI usage to very large organizations only. Hermes is designed to use the Internet, Public Key Infrastructure (PKI), and XML technologies to replace the EDI as a more affordable and extensible solution. Hermes supports mainstream business-to-business (B2B) transport protocols, such as ebXML Message Service 2.0 (ebMS 2.0) and Applicability Statement 2 (AS2). (The ebMS 3.0 / AS4 support is currently under development.).
Hermes unifies different transport protocols into a single B2B messaging framework. Based on this framework, you can easily develop an enterprise application to exchange business data with trading partners via different transport protocols. Designed to be extensible, Hermes provides an open Simple Plug-in Architecture (SPA) for developers to implement new messaging protocols as plug-ins. Most importantly, Hermes is open-source; you can freely extend Hermes and integrate it with other systems to meet your own business needs.

Quickstart

Install Hermes with Docker

1. Install the Docker Engine on Ubuntu 16.04+.

   ```
sudo apt-get update
dsud apt-get install apt-transport-https ca-certificates curl software-properties-common

curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo apt-key add -
sudo add-apt-repository "deb [arch=amd64] https://download.docker.com/linux/ubuntu ${lsb_release -cs} stable"
sudo apt-get update
dsud apt-get install docker-ce
   ```

2. Run the Docker container for Hermes database (MySQL).

   ```
docker run --name hermes_db -e MYSQL_ROOT_PASSWORD=corvus -d cecid/hermes_db:2.2
   ```

3. Run the Docker container for Hermes application server (Tomcat).

   ```
docker run --name hermes_app --link hermes_db:db -p 8080:8080 -d cecid/hermes_app:2.2
   ```

4. Log in to the Hermes administration console at http://localhost:8080/corvus/admin/home (username: corvus, password: corvus) to check if Hermes is up and running.
Note:
1. In Step 2 and 3, the corresponding Docker image will be downloaded from the Docker Hub for the initial run. As the size of cecid/hermes_db and cecid/hermes_app are about 400MB and 1.0GB, these steps may take at least several minutes to complete depending on the network speed.
2. You may need the administrator or root privilege to execute docker run.

Loopback Messaging with Sample Clients

Preparation

Linux (Ubuntu 16.04+):
1. Install Java SE 8 or above.
   
   ```
sudo add-apt-repository ppa:webupd8team/java
dudo apt update
dudo apt install oracle-java8-unlimited-jce-policy
dudo apt install oracle-java8-set-default
   ```
2. Please check Java 8 has been set up properly.
   ```
java -version
   ```
3. Download and extract the Hermes sample clients to a working directory `<WorkDir>`
   ```
cd <WorkDir>
unzip Hermes_client_sample.zip
sudo chmod -R 755 sample
   ```
4. Change the current directory to `<WorkDir>/sample`.

Windows:
1. Install Java 8 or above.
2. Please check Java 8 has been set up properly.
   ```
java -version
   ```
   If the above command fails to run, please try to set environment variable JAVA_HOME to the directory where Java is installed.
1. Download and extract the Hermes simple clients to a working directory `<WorkDir>/sample`.
2. Change the current directory to `<WorkDir>/sample`.

Create Loopback Partnership

Linux / Unix:
```
./ebms-partnership.sh
```

Windows:
Hermes Documentation, Release 2.2

 ebms-partnership.bat

You will see the following message.

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>EBMS Partnership Maintainance Tool</td>
<td></td>
</tr>
<tr>
<td>--------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>Initialize logger ..</td>
<td></td>
</tr>
<tr>
<td>Importing EBMS partnership parameters ...</td>
<td></td>
</tr>
<tr>
<td>Importing EBMS administrative sending parameters ...</td>
<td></td>
</tr>
<tr>
<td>Initialize EBMS HTTP data service client...</td>
<td></td>
</tr>
<tr>
<td>log4j:WARN No appenders could be found for logger  (org.apache.commons.httpclient. HttpClient).</td>
<td></td>
</tr>
<tr>
<td>log4j:WARN Please initialize the log4j system properly.</td>
<td></td>
</tr>
<tr>
<td>Sending EBMS HTTP partnership maintenance request ...</td>
<td></td>
</tr>
<tr>
<td>Sending Done:</td>
<td></td>
</tr>
</tbody>
</table>

The result status : Operation executed successfully.
Please view log for details ..

In the Hermes administration console at http://localhost:8080/corvus/admin/ebms/partnership, you will find a new Partnership ebms-loopback is created.

**Send Loopback Message**

**Linux / Unix:**

./ebms-send.sh

**Windows:**

ebms-send.bat

This program sends a request attached with the payload named testpayload under the directory <WorkDir>/sample/config/ebms-send to local Hermes server. You will see the following message.

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>EbMS sender web service client</td>
<td></td>
</tr>
<tr>
<td>--------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>Initialize Logger ...</td>
<td></td>
</tr>
<tr>
<td>Importing ebMS sending parameters ... ./config/ebms-send/ebms-request.xml</td>
<td></td>
</tr>
<tr>
<td>Importing ebMS partnership parameters ... ./config/ebms-partnership.xml</td>
<td></td>
</tr>
<tr>
<td>Initialize ebMS web service client...</td>
<td></td>
</tr>
<tr>
<td>Adding payload in the ebMS message...</td>
<td></td>
</tr>
<tr>
<td>Sending ebMS sending request ...</td>
<td></td>
</tr>
<tr>
<td>Sending Done:</td>
<td></td>
</tr>
</tbody>
</table>

New message id: 20170204-090520-45900@172.17.0.3

In the Hermes administration console at http://localhost:8080/corvus/admin/ebms/message_history, you will find a new message is created in outbox.

3.1. Quickstart
Query Message History

Linux / Unix:

```bash
./ebms-history.sh
```

Windows:

```bash
ebms-history.bat
```

This program lists all sent and received messages. You will see the following message.

```
----------------------------------------------------
EbMS Message History Queryer
----------------------------------------------------
Initialize Logger ...
Importing ebMS config parameters ... ./config/ebms-history/ebms-request.xml
Initialize ebMS messsage history queryer ...
Sending ebMS message history query request ...

Sending Done:
----------------------------------------------------
----------------------------------------------------
EbMS Message Query Result
----------------------------------------------------
0 | Message id : 20170204-090520-45900@172.17.0.3 | MessageBox: outbox
1 | Message id : 20170204-090520-45900@172.17.0.3 | MessageBox: inbox
```

Select message (0 - 1), -1 to exit: 0

Enter 0 to check the sent message and the following message will be displayed:

```
Sending EBMS-status sending request ...

Sending Done:
----------------------------------------------------
Query Message ID : 20170204-090520-45900@172.17.0.3
Query Message Status : DL
Query Message Status Desc : Message was sent.
ACK Message ID : null
ACK Message Status : null
ACK Message Status Desc : null
```

Please view log for details ..

Download Payload of Received Message

Linux / Unix:

```bash
./ebms-history.sh
```

Windows:
ebms-history.bat

You will see the following message.

```
EbMS Message History Queryer
Initialize Logger ...
Importing ebMS config parameters ... ./config/ebms-history/ebms-request.xml
Initialize ebMS message history queryer ...
Sending ebMS message history query request ...

Sending Done:
```

```
EbMS Message Query Result
```

```
0 | Message id : 20170204-090520-45900@172.17.0.3 | MessageBox: outbox
1 | Message id : 20170204-090520-45900@172.17.0.3 | MessageBox: inbox
```

Select message (0 - 1), -1 to exit: 1
Current Dir: /home/cecid/WorkDir/sample
Please provide the folder to store the payload(s):
Initialize ebMS receiving web service client...
Sending ebMS receiving request ... for 20170204-090520-45900@172.17.0.3

Please view log for details..

1. Enter 1 to select the received message and you will be asked to the folder to store the payloads.
2. Press enter to save the payload in the current folder. A file named `ebms.<timestamp>@127.0.1.1.Payload.0` will be downloaded, where `<timestamp>` indicates the time `ebms-send` was executed.
3. Open the payload file and you will see the following content:

```
This is an sample message.
```

```
:+
++
`++`
++
++
+=
++
```

3.1. Quickstart
Installing Hermes

Introduction

The Hermes installer is packaged in a self-extracted Java archive (JAR). Please download the source code from GitHub and build the Hermes Installer by Maven. Otherwise, you may download the JAR file from hermes2_installer.jar. Upon proper invocation, you will see an installation wizard, either in graphical or text format. Following the steps will install the following components:

- Hermes core
- Hermes plugins (AS2 / AS2 Plus / ebMS)
- Database tables of Hermes plugins in one of the following database:
  - Postgres 9.4 or later
  - Oracle 11gR2 or later
  - MySQL 5.5 or later with InnoDB storage engine supported
- Web service usage sample

**Prerequisite**

1. Java SE Development Kit 8 (For details, pls refer to Install Java SE 8)
2. Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files
   
   (a) Download the JCE Unlimited Strength Jurisdiction Policy Files for JDK 8 from http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html

   (b) Unzip the downloaded file

   ```
   unzip jce_policy-8.zip
   ```

   (c) Replace the two jar files local_policy.jar and US_export_policy.jar in the directory /usr/lib/jvm/java-8-oracle/jre/lib/security with the corresponding jar file unzipped in the previous step.

   ```
   cd UnlimitedJCEPolicyJDK8
   sudo cp local_policy.jar /usr/lib/jvm/java-8-oracle/jre/lib/security/local_policy.jar
   sudo cp US_export_policy.jar /usr/lib/jvm/java-8-oracle/jre/lib/security/US_export_policy.jar
   ```

2. Tomcat 8.5 or above with port 8080
   
   (a) Install Tomcat8.5+ (Ubuntu 16.04)

   ```
   sudo apt update
   sudo apt install -y tomcat8
   ```
(b) Change the ownership and mode of tomcat-users.xml

```
sudo chown <current user>:tomcat8 /etc/tomcat8/tomcat-users.xml
sudo chmod 640 /etc/tomcat8/tomcat-users.xml
```

(c) Restart Tomcat

**Note:** To access the admin page, please create a Tomcat user with an admin role by defining this user in tomcat-users.xml. Please refer to the Realm Configuration section in the Tomcat documentation for more details.

Sample of tomcat-user.xml:

```
<?xml version='1.0' encoding='utf-8'?>
<tomcat-users>
    <role rolename="tomcat"/>
    <role rolename="admin"/>
    <role rolename="api"/>
    <user username="corvus" password="corvus" roles="tomcat,admin,api"/>
</tomcat-users>
```

1. One of the following databases is installed:
   - PostgreSQL 9.2 or later. `<POSTGRES_HOME>` is referring to the home directory of PostgreSQL in the remaining parts of the document.
   - MySQL 5.5 or later. `<MYSQL_HOME>` is referring to the home directory of MySQL in the remaining parts of the document.
   - Oracle 11gR2 or later. `<ORACLE_HOME>` is referring to the home directory of Oracle in the remaining parts of the document.

**Installation**

**Step 1 – Environment setup**

The above prerequisite items are installed and running on the same machine.

**Step 2 – Database Configuration**

**Postgres**

1. Create a new DB user `corvus` with password `corvus`.
   (a) Open a terminal
   (b) Login an account with root or sudo privilege
   (c) Change folder to `<POSTGRES_HOME>/bin`
   (d) Type `sudo -u postgres createuser -A -d -P corvus`
   (e) Enter the sudo password to escalate privilege to root user, if the current account is not `root`
   (f) Enter the password `corvus` for the new user `corvus`
   (g) Enter the password again for confirmation

3.2. Installing Hermes
2. Create two databases named as2 and ebms with the corvus user.
   (a) Change folder to `<POSTGRES_HOME>/bin`
   (b) Type `sudo -u postgres createdb -U corvus -W as2`
   (c) Enter the sudo password to escalate privilege to root user, if the current account is not `root`
   (d) Enter the password `corvus`
   (e) Repeat steps 2b - 2d for the ebms database.

MySQL

1. Create two databases named as2 and ebms with username corvus and password corvus.
   (a) Open a terminal
   (b) Login an account
   (c) Change folder to `<MYSQL_HOME>/bin`
   (d) Type `mysql -u <MYSQL_ADMIN> -p` where `<MYSQL_ADMIN>` represents the name of an administrator/super-user in the MySQL database (default: `root`)
   (e) Enter the command below to create the as2 database. Note that specifying collate to `latin1_general_cs` is essential.
      ```
      create database as2 collate=latin1_general_cs;
      ```
   (f) Enter the command below to create and assign access privileges to user corvus.
      ```
      grant all on as2.* to 'corvus'@'localhost' identified by 'corvus';
      ```
   (g) Repeat steps 1e – 1f for the ebms database.

Oracle

Oracle database creation involves a number of steps and custom parameters for different requirements. Below is a guideline for creating an Oracle database for Hermes:

https://docs.oracle.com/cd/E11882_01/server.112/e10897/install.htm#ADMQS0232

Step 3 – Hermes Deployment

3.1 Execute the installer
   - For Unix/Linux, open terminal and type
     ```
     sudo java -jar hermes2_installer.jar
     ```
Press Enter until you get to Screen in 3.2 Configure Hermes.

- For Windows, open a command prompt as an Administrator and type `java -jar hermes2_installer.jar` or if `java` is not set in your environment path, specify the full path.

Click Next until you get to Screen in 3.2 Configure Hermes.
3.2 Configure Hermes

Description of the settings:
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Application Folder</td>
<td>Folder to place the web application (e.g. <code>webapps</code>) in Tomcat.</td>
</tr>
<tr>
<td>Hermes Home</td>
<td>Folder to place the Hermes core library and system files.</td>
</tr>
<tr>
<td>JDBC Driver</td>
<td>Specify which database vendor to connect to. One of the following 3 database vendors can be selected:</td>
</tr>
<tr>
<td></td>
<td>• Postgres</td>
</tr>
<tr>
<td></td>
<td>• Oracle</td>
</tr>
<tr>
<td></td>
<td>• MySQL</td>
</tr>
<tr>
<td>Hermes ebMS Plugin</td>
<td>Optional. Install the ebMS component.</td>
</tr>
<tr>
<td>Hermes AS2 Plugin</td>
<td>Optional. Install the AS2 component.</td>
</tr>
<tr>
<td>Web Service Usage Sample</td>
<td>Optional. Install the sample program of web service client.</td>
</tr>
</tbody>
</table>

Click Next and press Yes if the installer prompts you to create a new folder.

### 3.3 Configure Database Driver

Oracle and MySQL JDBC drivers are not bundled with this Installer. Please download it manually. Once this is done, specify the location of the driver:
Description of the settings:

**JDBC Driver Folder (.jar)**: Path to the downloaded JDBC driver file.

3.4 Configure Database for ebMS Plugin (Optional)
Description of the settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database URL</td>
<td>The URL address of the database server. Port number may be attached to the address with the format <code>&lt;HOST_ADDRESS&gt;:</code> <code>&lt;PORT&gt;</code> where <code>&lt;HOST_ADDRESS&gt;</code> is the hostname of the database server and <code>&lt;PORT&gt;</code> is the port number listened by the database server.</td>
</tr>
<tr>
<td>Database Name/SID</td>
<td>For Postgres and MySQL, please specify the name of the database. For Oracle, please specify the Oracle System ID (SID).</td>
</tr>
<tr>
<td>Username</td>
<td>Username to access the database.</td>
</tr>
<tr>
<td>Password</td>
<td>Password to access the database.</td>
</tr>
<tr>
<td>Re-create Tables</td>
<td>Optional. Re-create all the tables in the specified database.</td>
</tr>
</tbody>
</table>

**Important Notes:**
- If this is your first time installing Hermes, please check this option.
- If you choose to re-create the tables, all of the existing data in the specified database will be removed during installation. Please backup all the data in the selected database before re-creating the tables.

If you followed the steps in prerequisite Step 2 – Database Configuration above, you can just leave the settings as default value. Click Next when you have finished the configuration.

3.5 Configure Database for AS2 Plugin (Optional)
Description of the settings:
Hermes Documentation, Release 2.2

### Database URL
The URL address of the database server. Port number may be attached to the address with the format `<HOST_ADDRESS>:<PORT>` where `<HOST_ADDRESS>` is the address of the database server and `<PORT>` is the port number of the database server address.

### Database Name/SID
For Postgres and MySQL, please specify the name of the database. For Oracle, please specify the Oracle System ID (SID).

### Username
Username to access the database.

### Password
Password to access the database.

### AS2 Plugin
- **AS2**: Original AS2 plugin certified by Drummond Group Inc.
- **AS2 Plus**: Built based on AS2 plugin with new/enhanced features.

### Re-create Tables
Optional. Re-create all the tables in the specified database.

**Important Notes:**
- If this is your first time installing Hermes, please check this option.
- If you are switching from AS2 to AS2 Plus or vice versa, we highly recommend you check this option.
- If you choose to re-create the tables, all of the existing data in the specified database will be removed during installation. Please backup all the data in the selected database before choosing to re-create the tables.

If you followed the prerequisite Step 2 – Database Configuration above, you can just leave the settings as default value. Click Next when you have finished the configuration.

3.6 Click on Install and you’re done!

### Step 4 – Start Hermes2

1. **Checklist:**
   - Java JDK 8 or above with Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files.
   - Apache Tomcat 8.5 or above Servlet/JSP Container.
   - Database server is running with ebMS and/or AS2 database instances and the tables are created.
   - If you are running Unix/Linux, make sure that at least read permissions are set to the core directory and read/write for the AS2 repository directory in `<HERMES2_HOME>`.
   - Start Tomcat.

2. To verify that Hermes is running, access the following URL from a web browser:
   ```
   http://localhost:8080/corvus/home
   ```
   The welcome page should be displayed as below:
3. To access the admin page, go to the following URL. The login user and password are the same as the Tomcat user with admin privileges specified in Point 3 of Prerequisite.

   http://localhost:8080/corvus/admin/home

4. Once you have logged in, you should see the Hermes Administration Console page:
That's it! Hermes should now be up and running. You can test your setup by running our Web Service Usage Sample in next section.

**Partnership Maintenance and Web Service Usage Sample**

A tool kit called **Web Service Usage Sample** was installed under the `<HERMES2_HOME>/sample` folder. It contains tools to test the Hermes.

**Directory Organization**

<table>
<thead>
<tr>
<th>Directory/File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>config/*</td>
<td>Contains the configuration file for the sample programs. Each folders contain related files for specific sample programs.</td>
</tr>
<tr>
<td>config/ebms-partnership.xml</td>
<td>Contains partnership settings for ebMS and AS2 as the input of sample programs.</td>
</tr>
<tr>
<td>config/as2-partnership.xml</td>
<td></td>
</tr>
<tr>
<td>logs/*</td>
<td>A set of logs that contain the output from each sample program.</td>
</tr>
<tr>
<td>lib/*</td>
<td>The library files used by the sample programs.</td>
</tr>
<tr>
<td><em>.bat/</em>.sh</td>
<td>The scripts to run the sample programs.</td>
</tr>
</tbody>
</table>

**Preparation**
Windows environment

1. Set environment variable JAVA_HOME to the folder where Java is located.

   **Note:** To run the sample program, Administrator privilege or root access is required.

UNIX environment

1. Set environment variable JAVA_HOME to the folder where Java is located.

2. Change the owner and the group of `<HERMES2_HOME>` and `<TOMCAT_HOME>/webapps/corvus` with the following commands:

   ```
   sudo chown -R <tomcat user>:<OWNER_GROUP> <HERMES2_HOME>
   sudo chown -R <tomcat user>:<OWNER_GROUP> <TOMCAT_HOME>/webapps/corvus
   ```

3. Change the permissions of all files in `<HERMES2_HOME>` and `<TOMCAT_HOME>/webapps/corvus` to 775 with the following command:

   ```
   sudo chmod -R 775 <HERMES2_HOME>
   sudo chmod -R 775 <TOMCAT_HOME>/webapps/corvus
   ```

Partnership Maintenance

Users need to define a partnership, which contains the messaging details between sender and recipient. It is required to identify the sender and the recipient when transporting messages.

A web service sample program is provided to manage partnerships (add, update and delete). The partnership configuration for the AS2/ebMS loopback test is placed in `<HERMES2_HOME>/sample/config/<as2/ebms>-partnership.xml`.

<table>
<thead>
<tr>
<th>Program</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>as2-partnership</td>
<td>Maintains a specified AS2/ebMS partnership between sender and recipient.</td>
</tr>
<tr>
<td>ebms-partnership</td>
<td></td>
</tr>
</tbody>
</table>

Creating an AS2 Partnership

To perform the AS2 messaging loopback test using *Steps to run AS2 Sample*, you need to create the required partnership by executing the script `as2-partnership`.

Or:

Access `http://localhost:8080/corvus/admin/as2/partnership` to configure the partnership manually. Below is a simple loopback configuration sample:
3.2. Installing Hermes
<table>
<thead>
<tr>
<th>Partnership ID</th>
<th>as2-loopback</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS2 From</td>
<td>as2loopback</td>
</tr>
<tr>
<td>AS2 To</td>
<td>as2loopback</td>
</tr>
<tr>
<td>Disabled</td>
<td>No</td>
</tr>
<tr>
<td>Subject</td>
<td>none</td>
</tr>
<tr>
<td>Recipient Address</td>
<td><a href="http://127.0.0.1:8080/corvus/httpd/as2/inbound">http://127.0.0.1:8080/corvus/httpd/as2/inbound</a></td>
</tr>
<tr>
<td>Hostname Verified in SSL?</td>
<td>No</td>
</tr>
<tr>
<td>Request Receipt?</td>
<td>No</td>
</tr>
<tr>
<td>Signed Receipt?</td>
<td>No</td>
</tr>
<tr>
<td>Asynchronous Receipt?</td>
<td>No</td>
</tr>
<tr>
<td>Receipt Return URL</td>
<td><a href="http://127.0.0.1:8080/corvus/httpd/as2/inbound">http://127.0.0.1:8080/corvus/httpd/as2/inbound</a></td>
</tr>
<tr>
<td>Message Compression Required?</td>
<td>No</td>
</tr>
<tr>
<td>Message Signing Required?</td>
<td>No</td>
</tr>
<tr>
<td>Signing Algorithm</td>
<td>sha1</td>
</tr>
<tr>
<td>Message Encryption Required?</td>
<td>No</td>
</tr>
<tr>
<td>Encryption Algorithm</td>
<td>rc2</td>
</tr>
<tr>
<td>Certificate For Encryption</td>
<td>none</td>
</tr>
<tr>
<td>MIC Algorithm</td>
<td>sha1</td>
</tr>
<tr>
<td>Maximum Retries</td>
<td>1</td>
</tr>
<tr>
<td>Retry Interval (ms)</td>
<td>30000</td>
</tr>
<tr>
<td>Message Signature Enforced?</td>
<td>No</td>
</tr>
<tr>
<td>Message Encryption Enforced?</td>
<td>No</td>
</tr>
<tr>
<td>Certificate For Verification</td>
<td>none</td>
</tr>
</tbody>
</table>

**Creating an AS2 Plus Partnership**

Please follow the same procedure listed in *Creating an AS2 Partnership*.

**Creating an ebMS Partnership**

To perform the ebMS messaging loopback test using *Steps to run ebMS Sample*, you need to create the required partnership by executing the script `ebms-partnership`.

**Or:**

Access [http://localhost:8080/corvus/admin/ebms/partnership](http://localhost:8080/corvus/admin/ebms/partnership) to configure the partnership manually. Below is a simple loop-back configuration sample:
### 3.2. Installing Hermes

**Partnership ID**
- `ebms-loopback`

**CPA ID**
- `cpaid`

**Service**

**Action**
- `action`

**Disabled**
- No

**Transport Endpoint**

**Hostname Verified in SSL?**
- No

**Sync Reply Mode**
- `none`

**Acknowledgement Requested**
- `never`

**Acknowledgement Signed Requested**
- `never`

**Duplicate Elimination**
- `never`

**Message Order**
- `NotGuaranteed`

**Signing Required?**
- No

**Encryption Required? (Mail Only)**
- No

**Certificate For Encryption**
- None

**Maximum Retries**
- 1

**Retry Interval (ms)**
- 30000

**Certificate For Verification**
- None
Web Service Usage Sample Flow

In order to validate the installation of Hermes, the following web service usage sample programs are provided.

<table>
<thead>
<tr>
<th>Program</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>as2-send / ebms-send</td>
<td>Send an AS2/ebMS message to the installed Hermes.</td>
</tr>
<tr>
<td>as2-history / ebms-history</td>
<td>Show the message history of Hermes. This program will list the inbox and outbox messages in the data storage of Hermes. The user can view the details of the inbox and outbox. For inbox messages, the user can also download the payload in the repository of Hermes, if available.</td>
</tr>
</tbody>
</table>

We suggest running the sample programs in the following steps:

1. Send a message to the local Hermes by running `as2-send/ebms-send`.

2. Check the status of the sent message by running `as2-history/ebms-history` and select the message from the outbox.

3. Check the received message by running `as2-history/ebms-history` and select the message from the inbox to download the payload.

Steps to run AS2 Sample

Before executing the following AS2 web service usage sample, the partnership from Creating an AS2 Partnership must be created.

1. Send a message to the local Hermes using the script `as2-send`.

   This program creates and sends a request attached with the payload named `testpayload` under the directory `<HERMES2_HOME>/sample/config/as2-send` to Hermes.

   Upon successful execution, you should be able to see the similar output shown as follow:

   ![AS2 Message Sender](image)

2. Check the sent message using the script `as2-history`.

   This program retrieves the list of sent/received message from Hermes.
Enter 0 to check the sent message. A display similar to the following will appear:

```
A file named as2.<timestamp>@127.0.1.1.Payload.0 will be downloaded, where <timestamp> is the time as2-send was executed. Open that file and you will see the follow content:
```

3. Check the received message and download the payload.

From the select message screen of as2-history, enter 1 to select the inbox message and it will display Please provide the folder to store the payload(s):. Press enter to save the payload in the current folder. A file named as2.<timestamp>@127.0.1.1.Payload.0 will be downloaded, where <timestamp> is the time as2-send was executed. Open that file and you will see the follow content:
Steps to run ebMS Sample

Before executing the following ebMS web service usage sample, the partnership from *Creating an ebMS Partnership* must be created.

1. Send a message to the local Hermes server using the script `ebms-send`.

   This program creates and sends a request attached with the payload named `testpayload` under the directory `<HERMES2_HOME>/sample/config/ebms-send` to Hermes.

   Upon successful execution, an output similar to the following will be displayed:
2. Check the sent message using the script `ebms-history`.

This program retrieves the list of sent/received message from Hermes.

```
---
EbMS Message History Queryer
---
Initializing Logger ... 
Importing ebMS config parameters ... ./config/ebms-history/ebms-request.xml
Initializing ebMS message history queryer ...
Sending ebMS message history query request ...

Sending Done:
---
EbMS Message Query Result
---
<table>
<thead>
<tr>
<th>Message id</th>
<th>20170207-160023-86402@127.0.1.1</th>
<th>MessageBox: outbox</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message id</td>
<td>20170207-160023-86402@127.0.1.1</td>
<td>MessageBox: inbox</td>
</tr>
</tbody>
</table>
Select message (0 - 1), -1 to exit:
---

Sending  EBMS-status sending request ...

Sending Done:
---
Query Message ID : 20170207-160023-86402@127.0.1.1
Query Message Status : DL
Query Message Status Desc : Message was sent.
ACK Message ID : null
ACK Message Status : null
ACK Message Status Desc : null

Please view log for details. ..
---
```

Enter 0 to check the sent message and a screen similar to the following will be displayed:

3. Check the received message and download the payload.

From the select message screen of `ebms-history`, enter 1 to select the inbox message and it will display

```
Please provide the folder to store the payload(s):. Press enter to save the payload in
the current folder. A file named ebms.<timestamp>@127.0.1.1.Payload.0 will be downloaded,
where <timestamp> is the time `ebms-send` was executed. Open that file and you will see the following
content:
---
```
This is an sample message.

**Configuration for Sending Secure Message**

To send signed message through HTTPS, we have to configure a trust-store, keystore and certificate separately in Hermes and Tomcat. For details, please refer to the section *Send Messages Through HTTPS*.

**FAQ**

**Hermes Deployment**

Q1. The `corvus.log` shows:

```
hk.hku.cecid.piazza.commons.spa.PluginException: Error in processing activation by handler: hk.hku.cecid.ebms.spa.EbmsProcessor which is caused by java.io.IOException: exception decrypting data - java.lang.SecurityException: Unsupported keysize or algorithm parameters
```

A1. Please ensure the Java 8 SE files have been replaced by the JCE files as mentioned in *Prerequisite*.

Q2. Some log files show the following error:

```
hk.hku.cecid.piazza.commons.dao.DAOException: Unable to begin transaction.
```

A2. Ensure PostgreSQL/MySQL/Oracle was installed properly and check the following files:
For AS2:

\texttt{<HERMES2\_HOME>/plugins/corvus-as2/conf/hk/hku/cecid/edi/as2/conf/as2.module.core.xml}. There is a tag in this file named \texttt{parameter} with the attribute \texttt{name=url}. Check the \texttt{value} attribute to see if it references the correct server address. The format of the \texttt{value} attribute is the same as the JDBC connection string.

For ebMS:

\texttt{<HERMES2\_HOME>/plugins/corvus-ebms/conf/hk/hku/cecid/ebms/spa/conf/ebms.module.xml}. There is a tag in this file named \texttt{parameter} with the attribute \texttt{name=url}. Check the \texttt{value} attribute to see if it references the correct server address. The format of the \texttt{value} attribute is the same as the JDBC connection string.

\section*{Web Service Usage Sample}

Q1. The following exception is thrown:

\begin{verbatim}
Exception in thread "main" java.lang.UnsupportedClassVersionError: xxx
  at (Unsupported major.minor version 49.0)
\end{verbatim}

A1. It is very likely you are using an incompatible Java version. The web service usage sample requires Java 8 SE or above to run properly. In the terminal, please type \texttt{java -version} to check the Java version.

Q2. The following error occurs:

\begin{verbatim}
Sending ebMS/AS2 sending request ...
java.net.ConnectException: Connection refused: connect
\end{verbatim}

A2. Check that the Application Container (Tomcat) has been started.

\section*{The First Step}

\subsection*{Introduction}

One of the most common difficulties in using Hermes for new developers/users is managing a partnership and programming the web service requester before they are able to deliver messages to their partner. This article is purposed to assist the user to create and maintain partnerships in Hermes. For more information on the installation and administration console of Hermes, please refer to \textit{Installing Hermes}.

\subsection*{What is a partnership?}

A partnership in Hermes is defined as a channel to your business partner. A partnership is a \textbf{Simplex} (one-way) communication channel to your business partner. In a typical two-way business document exchange, the Hermes in each party should have \textbf{TWO} matching partnership for sending and receiving\(^1\). After the partnerships have been defined, the application can reference the partnerships to send or receive business messages.

\begin{figure}[h]
\centering
\includegraphics[width=0.5\textwidth]{example.pdf}
\caption{Diagram of partnership configuration in Hermes.}
\end{figure}

\begin{footnote}{\textsuperscript{1}}\textbf{Duplex} communication channel in Hermes can also be setup by configuring only \textbf{ONE} matching partnership in sending and receiving parties.\end{footnote}
Existing partnership types

Currently, Hermes has two types of partnerships, which are ebMS and AS2. They represent the communication agreement with your partner to use ebMS protocol and AS2 protocol respectively.

**ebMS 2.0 partnership**

**What is an ebMS 2.0 partnership?**

For an ebms 2.0 partnership, CPA (Collaboration Protocol Agreement) ID, Service and Action are used to uniquely identify each partnership. The values of these parameters will appear in the headers of outgoing ebMS messages. The purpose of these parameters for a sending partnership and a receiving partnership are different:

- In a sending partnership, these values are taken as the values in the ebMS headers of outgoing messages.
- In a receiving partnership, these values are taken as filtering criteria. If Hermes receives an ebMS message whose CPA ID, Service and Action values do not have a matching partnership, a negative acknowledgement will be sent back to the sender and no application can retrieve the message on the receiving side.

Since the receiving partnership’s CPA ID, Service and Action filter the incoming messages, the values in the receiving partnership of the receiving Hermes should always be the same as the values in the sending partnership of the sending Hermes.

**How to create your first ebMS 2.0 partnership**

1. Open a Web browser.
2. Go to Hermes Administration Console at `http://<LOCALHOST>:\<PORT>/corvus/admin/home`.
3. Enter the administrator username and password for Hermes.
4. Click Ebms Plugin in the module tab located on the left hand side.
5. Click the Partnership tab on the central horizontal tabbed bar to display the partnership creation page.
6. To create the simplest ebMS 2.0 partnership, you are only required to fill in the following seven fields in the form:

   - Partnership ID
   - CPA ID
   - Service
   - Action
   - Transport URL
   - Retries
   - Retry Interval

1. Fill in Partnership ID, CPA ID, Service and Action as shown below: Partnership ID is the unique identifier of the partnership in the sending Hermes while the three remaining fields (CPA ID, Service and Action) form a composite identifier between sending and receiving systems.

---

2 Detailed description of the parameters in ebMS 2.0 partnership can be found in the next section Setting Up ebMS 2.0 Partnerships.
2. Fill in the **Transport Endpoint** (the receiver’s URL) as shown below:

   The Transport Endpoint URL should be formatted as `http://<RECEIVER_HOST>:<PORT>/corvus/httpd/ebms/inbound`

   where `corvus/httpd/ebms/inbound` is the context path for accepting and receiving incoming ebXML messages if the receiving system is also using Hermes.

   Since the receiving host below is the same as the sending host (i.e. the ebMS message loops back to the sender), only **ONE** partnership is required for sending and receiving.

   **Transport Endpoint**  
   `http://localhost:8080/corvus/httpd/ebms/inbound`

3. Fill in the number of retries allowed if the message fails to be delivered and the retry interval as shown below:

<table>
<thead>
<tr>
<th>Retries</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retry Interval (ms)</td>
<td>30000</td>
</tr>
</tbody>
</table>

4. Now you have completed all required fields and you should have the same input as the figure shown here.

5. Click the *add* button at the bottom of the page.

6. A dialog box will prompt you to confirm adding the partnership. Click *Ok*.

7. The message **Partnership Added Successfully** will be shown on the status bar (the bottom of the page).

8. Congratulations! You have successfully created your first ebMS 2.0 partnership.
How to update an ebMS 2.0 partnership

1. Do steps 1-5 in *How to create your first ebMS 2.0 partnership* or all steps if you have not registered a partnership in Hermes.

2. You should able to see a drop-down list under the header *Registered Partnership*.

3. Click the *Change* button.

4. Now you should able to see a module called *Selected Partnership* that contains the information of selected partnership from the previous step like here.

<table>
<thead>
<tr>
<th>General</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partnership ID</td>
</tr>
<tr>
<td>CPA ID</td>
</tr>
<tr>
<td>Service</td>
</tr>
<tr>
<td>Action</td>
</tr>
<tr>
<td>Disabled</td>
</tr>
<tr>
<td>Transport Endpoint</td>
</tr>
<tr>
<td>Hostname Verified in SSL</td>
</tr>
<tr>
<td>Sync Reply Mode</td>
</tr>
<tr>
<td>Acknowledgement Requested</td>
</tr>
<tr>
<td>Acknowledgement Signed Requested</td>
</tr>
<tr>
<td>Duplicate Elimination</td>
</tr>
<tr>
<td>Message Order</td>
</tr>
<tr>
<td>Signing Required?</td>
</tr>
<tr>
<td>Encryption Required? (Mail Only)</td>
</tr>
<tr>
<td>Certificate For Encryption</td>
</tr>
<tr>
<td>Maximum Retries</td>
</tr>
<tr>
<td>Retry Interval (ms)</td>
</tr>
<tr>
<td>Certificate For Verification</td>
</tr>
</tbody>
</table>

5. Change the desired parameters/fields and click *Update* when you are done.

6. A dialog box will prompt you to confirm the updates. Click *Ok*.

7. The message *Partnership Updated Successfully* will be shown on the status bar (the bottom of the page).

How to delete an ebMS 2.0 partnership

1. Do the steps 1-4 in *How to update an ebMS 2.0 partnership*.

2. Click the *Delete* button.

3. The message *Partnership deleted successfully* will be shown on the status bar (the bottom of the page).

AS2 partnership
What is an AS2 partnership?

For an AS2 partnership, the AS2 From and AS2 To fields in a partnership are used to uniquely identify it. The values of these parameters will appear in AS2 message headers. The purpose of these parameters for a sending partnership and a receiving partnership are different:

- In a sending partnership, these values are taken as the values in the headers of outgoing messages.
- In a receiving partnership, these values are taken as filtering criteria. If Hermes receives an AS2 message whose AS2 From and AS2 To values do not have a matching partnership, the incoming message is rejected/ignored and no application can retrieve the message on the receiving side.

**Note:** The values of AS2 From and AS2 To in the incoming AS2 message are interchanged before finding the matching partnership (i.e. the filtering criteria [AS2 From, AS2 To] = [Incoming AS2 To, Incoming AS2 From] in the AS2 message).

Although the values of AS2 From and AS2 To have no constraints, it is highly recommended that they be company specific, such as Data Universal Numbering System (DUNS) numbers, or simply identification strings agreed upon between trading partners.

Let us look at a typical example below, in which two Hermes communicate using AS2 protocol:

![Diagram of two Hermes communicating using AS2 protocol]

How to create your first AS2 partnership

1. Open a Web browser.
3. Enter the administrator user name and password for Hermes.
4. Click the AS2 Plugin in the module tab located on the left hand side.
5. Click the Partnership tab on the central horizontal tabbed bar to display the partnership creation page.
6. To create the simplest AS2 partnership, you are only required to fill in the following seven fields in the form:
   (a) Partnership ID
   (b) AS2 From
   (c) AS2 To
   (d) Subject
   (e) Transport URL
   (f) Retries
   (g) Retry Interval

   3 Detailed description of the parameters in AS2 partnership can be found in the next section Setting Up AS2 Partnerships
1. Fill in **Partnership ID**, **AS2 From** and **AS2 To** as shown below: Partnership ID is the unique identifier of the partnership in the sender Hermes while the two remaining fields (AS2 From, AS2 To) form a composite identifier between sending and receiving systems.

<table>
<thead>
<tr>
<th>Partnership ID</th>
<th>MyFirstPartnership</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS2 From</td>
<td>FromMyMachine</td>
</tr>
<tr>
<td>AS2 To</td>
<td>ToMyMachine</td>
</tr>
</tbody>
</table>

2. Fill in the **Subject** and **Transport Endpoint** (the receiver’s URL) as shown below:

   The Transport Endpoint URL should be formatted as `http://<RECEIVER_HOST>:<PORT>/corvus/httpd/as2/inbound`

   where `corvus/httpd/as2/inbound` is the context path for accepting and receiving incoming AS2 messages if the receiving system is also using Hermes.

   Since the receiving host below is the same as the sending host (i.e. the AS2 message loops back to the sender), only **ONE** partnership is required for sending and receiving.

<table>
<thead>
<tr>
<th>Subject</th>
<th>MyFirstSubject</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transport Endpoint</td>
<td><a href="http://localhost:8080/corvus/httpd/as2/inbound">http://localhost:8080/corvus/httpd/as2/inbound</a></td>
</tr>
</tbody>
</table>

3. Fill in the number of retries allowed if the message fails to be delivered and the retry interval as shown below:

<table>
<thead>
<tr>
<th>Retries</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retry Interval (ms)</td>
<td>30000</td>
</tr>
</tbody>
</table>

4. Now you have completed to all required fields and you should have the same input as the figure shown here.
5. Click the *add* button at the bottom of the page.

6. A dialog box will prompt you to confirm adding the partnership. Click *Ok*.

7. The message *Partnership Added Successfully* will be shown on the status bar (the bottom of the page).

8. Congratulations! You have successfully created your first AS2 partnership.

**How to update an AS2 partnership**

1. Do the steps 1-5 in *How to create your first AS2 partnership* or all steps if you have not registered a partnership in Hermes.

2. You should able to see a drop-down list under the header *Registered Partnership*.

3. Click the *Change* button.

4. Now you should able to see a module called *Selected Partnership* that contains the information of selected partnership from previous step like here.
5. Change the desired parameters/fields and click **Update** when you are done.

6. A dialog box will prompt you to confirm the update. Click **Ok**.

7. The message *Partnership Updated Successfully* will be shown on the status bar (the bottom of the page).

**How to delete AS2 partnership**

1. Do the steps 1-4 in *How to update an AS2 partnership*.

2. Click the **Delete** button.

3. The message *Partnership deleted successfully* will be shown on the status bar (the bottom of the page).

**Conclusion**

The main benefit of partnerships is that it provides abstraction on technical parameters. The abstraction is beneficial because:

1. The application does not need to change if your business partner changes the parameters, since all technical parameters are contained within the partnership.
2. The application only needs to submit payloads. It does not contain any code that is specific to the communication protocol between messaging gateways.

3. The application does not need to handle the raw and cryptic ebMS / AS2 messages. Therefore, developers only need to focus on business logic and integration with the backend systems.

See also

- Setting Up ebMS 2.0 Partnerships
- Setting Up AS2 Partnerships
- OASIS ebMS 2.0 Specification
- AS2 Specification

Setting Up ebMS 2.0 Partnerships

**Partnership ID**

| Description | The unique identifier of an ebMS 2.0 partnership in local Hermes. The value of this field has no restriction but it is **RECOMMENDED** to be unique between sender and recipient. This field is **mandatory** and its maximum length is 255. |

**CPA ID**

| Description | The Collaboration Protocol Agreement (CPA) ID is a string that identifies the parameters governing the exchange of messages between the parties. The recipient of a message must be able to resolve the CPA ID to an individual set of parameters, taking into account the sender of the message. Simply put, it is an arbitrary and **mandatory** string that can be used to identify both sender and recipient. See [OASIS ebXML Messaging Service Spec v2.0] for details. |

**Service**

| Description | In Hermes, this **mandatory** parameter is used for mapping a partnership between sender and recipient. |

**Action**

| Description | This identifies a process within a Service that processes the ebMS message. Action must be unique within the Service in which it is defined. The value of the Action element is specified by the designer of the Service. This field is **mandatory** and its maximum length is 255 characters. |
### Disabled

**Description**

This boolean option indicates whether the partnership is disabled or not. Disabled partnership do not deliver/receive any outgoing/incoming messages.

**Options**

- `true` = disabled
- `false` = enabled

### Transport Endpoint

**Description**

The endpoint URL of the receiving messaging gateway. If the receiving messaging gateway is Hermes and HTTP/HTTPS is the transport protocol, the endpoint URL is formatted as `http://<RECIPIENT_HOST>:<PORT>/corvus/httpd/ebms/inbound`. The recipient should set this field to `http://<SENDER_HOST>:<PORT>/corvus/httpd/ebms/inbound` in order to send acknowledgements to sender upon request. Otherwise, if the recipient host is an SMTP gateway, the endpoint URL is formatted as `mailto:<EMAIL_ADDRESS>`. This field is mandatory and the format must be an HTTP/HTTPS URL or EMAIL ADDRESS.

### Hostname Verified in SSL?

**Description**

This boolean flag indicates whether HTTP SSL/TLS protocol is used to verify the recipient hostname. This is relevant only if HTTPS transport protocol is used in `Transport Endpoint`.

**Options**

- `true` = hostname verified using SSL
- `false` = no verification using SSL

### Sync Reply Mode

**Description**

Indicates whether the receiver should reply to incoming ebMS messages using the same HTTP/HTTPS connection that the sender is using for delivery. This parameter is only applicable to send partnerships using HTTP/HTTPS transport protocol.

**Options**

- `mshSignalsOnly` = synchronous reply
- `none` = asynchronous reply

**Synchronous reply**

ebMS message acknowledgement is included in the HTTP/SOAP response.
Asynchronous reply

ebMS message acknowledgement will be delivered through another HTTP/SOAP connection from the recipient to the sender.

### Acknowledgement Requested

<table>
<thead>
<tr>
<th>Description</th>
<th>Indicates whether the sender has requested the recipient to reply with an ebMS acknowledgement. An acknowledgement is a type of ebMS message which has an <code>&lt;acknowledgement&gt;</code> element. For interoperability of this feature, both sender and recipient must enable it. Otherwise, the recipient will return a negative acknowledgement. How the acknowledgement is sent depends on the value of <em>Sync Reply Mode</em>. If it is enabled, the acknowledgement will be sent immediately using the same HTTP connection as the received message. Otherwise, if the recipient is using Hermes, the acknowledgement will be placed in an outgoing queue until it is delivered to the sender. It is <strong>RECOMMENDED</strong> to set this parameter to <code>always</code> for reliable messaging.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Options</td>
<td>[ <code>always</code> = acknowledgement requested ], [ <code>none</code> = acknowledgement is not requested ]</td>
</tr>
</tbody>
</table>
Acknowledgement Signed Requested

<table>
<thead>
<tr>
<th>Description</th>
<th>Indicates whether the recipient must sign the ebMS acknowledgement digitally using their private key before delivering it to the sender. For interoperability of this feature, both sender and recipient must enable it. Otherwise, the recipient will return a negative acknowledgement. The format of the private key should be in PKCS12 and the created signatures should conform to W3C XML Signatures Specification [XMLDsig]. The send partnership must set Acknowledgement Requested to always for this feature to run properly. The recipient is required to provide a Certificate for Verification so the signature in the acknowledgement can be verified.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dependencies</td>
<td>[Acknowledgement Requested = always], [Certificate For Verification REQUIRED]</td>
</tr>
<tr>
<td>Options</td>
<td>[true = acknowledgement must be digitally signed], [false = acknowledgement must not be digitally signed]</td>
</tr>
</tbody>
</table>

Duplicate Elimination

<table>
<thead>
<tr>
<th>Description</th>
<th>Indicates whether the recipient will ignore duplicate messages. For interoperability of this feature, both sender and recipient must enable it. Otherwise, the recipient will return a negative acknowledgement.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Options</td>
<td>[always = ignores duplicate messages], [never = receives duplicate messages]</td>
</tr>
</tbody>
</table>

Message Order

<table>
<thead>
<tr>
<th>Description</th>
<th>Indicates whether the recipient must receive ebMS messages in the same sequence that they were sent. For interoperability of this feature, both sender and recipient must enable it. Otherwise, the recipient will return a negative acknowledgement.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dependencies</td>
<td>[Sync Reply Mode = none], [Acknowledgement Requested = always], [Duplicate Elimination = always]</td>
</tr>
<tr>
<td>Options</td>
<td>[Guaranteed = recipient receives ebMS messages in sending order], [NotGuaranteed = recipient receives ebMS message with best effort behavior]</td>
</tr>
</tbody>
</table>
### Signing Required?

<table>
<thead>
<tr>
<th>Description</th>
<th>Indicates whether the sender must sign ebMS messages digitally using their private key. For interoperability of this feature, both sender and recipient must enable this. Otherwise, the recipient will return a negative acknowledgement. The format of the private key should be in PKCS12 and the created signature should conform to W3C XML Signatures Specification [XMLDsig]. For details of signing message, please refer to <a href="#">Sign and Verify Message</a>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Options</td>
<td><code>[true = outgoing ebMS messages must be digitally signed]</code>, <code>[false = outgoing ebMS messages are not required to be digitally signed]</code></td>
</tr>
</tbody>
</table>

### Encryption Required? (Mail Only)

<table>
<thead>
<tr>
<th>Description</th>
<th>Indicates whether the sender must encrypt ebMS messages using the recipient’s public certificate defined in Certificate For Encryption. This is only applicable when using SMTP protocol for Transport Endpoint. The encryption method is based on S/MIME standard.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Options</td>
<td><code>[true = outgoing ebMS messages must be encrypted]</code>, <code>[false = outgoing ebMS messages are not required to be encrypted]</code></td>
</tr>
</tbody>
</table>

### Certificate For Encryption

<table>
<thead>
<tr>
<th>Description</th>
<th>The certificate file for encrypting outgoing ebMS messages using SMTP protocol by using the public key generated by the recipient. The recipient should use the keystore in the ebMS plugin to export the public certificate for the sender. ebMS default keystore location: <code>&lt;HERMES2_HOME&gt;/plugins/corvus-ebms/security</code> The certificate must be in X.509 format. See <a href="#">Encryption Required? (Mail Only)</a> for details.</th>
</tr>
</thead>
</table>
Maximum Retries

<table>
<thead>
<tr>
<th>Description</th>
<th>The maximum number of retries allowed for the sender to attempt delivering an ebMS message. Hermes tries to deliver the ebMS message under the features of reliable messaging until exceeding the maximum number of retries. There will be a time interval between each attempt, which is defined in Retry Interval (ms). It is recommended that the value of this field be between 1-10.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dependencies</td>
<td>[Acknowledgement Requested = always]</td>
</tr>
</tbody>
</table>

Retry Interval (ms)

<table>
<thead>
<tr>
<th>Description</th>
<th>The time interval (milliseconds) between each consecutive attempt to deliver an ebMS message. It is recommended that the value of this field be between 30000-300000.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dependencies</td>
<td>[Acknowledgement Requested = always]</td>
</tr>
</tbody>
</table>

Certificate For Verification

<table>
<thead>
<tr>
<th>Description</th>
<th>The certificate (.cer) file for verifying incoming digitally signed ebMS message by using the public key generated by sender. The sender should use the keystore in the ebMS plugin to export the public certificate for the recipient. ebMS default keystore location: &lt;HERMES2_HOME&gt;/plugins/corvus-ebms/security The keystore must be in PKCS12 format. See Signing Required? for details.</th>
</tr>
</thead>
</table>

Setting Up AS2 Partnerships

Partnership ID

| Description | The unique identifier of an AS2 partnership in Hermes. The value of this field has no restrictions but it is RECOMMENDED to be unique between sender and recipient. This field is mandatory and its maximum length is 255 characters. |
AS2 From

| Description | Identifier of the sending party in a data exchange. The values may be company specific, such as Data Universal Numbering System (DUNS) numbers, or they may simply be identification strings agreed upon between trading partners. [AS2 RFC4130 6.2] This parameter is used as the AS2-From property in AS2 message headers in this partnership. This field is mandatory and it is RECOMMENDED that the length of this value be less than 255 characters. See note below. |

Note: AS2 From and AS2 To form a pair that identify the send and receive partnerships (i.e. they form a composite key that identifies the parties involved in the data exchange). The values of [AS2 From, AS2 To] are reversed in the receive partnership with respect to the send partnership. For example:

Send: [CompanyA, CompanyB] -> Receive: [CompanyB, CompanyA].

AS2 To

| Description | Identifier of the receiving party in a data exchange. The values may be company specific, such as Data Universal Numbering System (DUNS) numbers, or they may simply be identification strings agreed upon between trading partners. [AS2 RFC4130 6.2] This parameter is used as the AS2-To property in AS2 message headers in this partnership. This field is mandatory and it is RECOMMENDED that the length of this value be less than 255 characters. See note below. |

Disabled

| Description | This boolean option indicates whether the partnership is disabled or not. Disabled partnerships do not deliver/receive any outgoing/incoming messages. |
| Options     | [true = disabled], [false = enabled] |

Subject

| Description | The subject of the partnership. This parameter is used as the Subject property in AS2 message headers in this partnership. This field is only applicable to send partnerships. |
### Recipient Address

| Description | The endpoint URL of the receiving messaging gateway. If the receiving messaging gateway is Hermes, the endpoint URL is http://<RECIPIENT_HOST>:<PORT>/corvus/httpd/as2/inbound. This field is mandatory and it must be an HTTP/HTTPS URL. |

### Hostname Verified in SSL?

| Description | This boolean flag indicates whether HTTP SSL/TLS protocol is used to verify the recipient hostname. This is relevant only if HTTPS transport protocol is used in Recipient Address. This field is only applicable to send partnerships. |
| Options | [true = hostname verified using SSL], [false = no verification using SSL] |

### Request Receipt

| Description | Indicates whether the sender has requested the recipient to reply with an AS2 receipt (acknowledgement). How the receipt is sent depends on the value of Asynchronous Receipt. If it is disabled, the receipt will be sent immediately using the same HTTP connection as the received message. Otherwise, if the recipient is using Hermes, the receipt will be placed in an outgoing queue until it is delivered to the sender. It is RECOMMENDED to set this parameter to true for reliable messaging. This field is only applicable to send partnerships. |
| Options | [true = receipt requested], [false = receipt is not requested] |
Signed Receipt

| Description | Indicates whether the sender has requested the recipient to digitally sign the AS2 receipt with their private key before delivering it. The format of the private key should be in PKCS12 and the created signatures should conform to IETF S/MIME. The send partnership must enable Request Receipt for this feature to function properly. The recipient is required to provide a Certificate for Verification so the source of the receipt can be verified. This field is only applicable to send partnerships. |
| Dependencies | [ Request Receipt = true ], [ Certificate for Verification REQUIRED ] |
| Options | [ true = receipt must be digitally signed ], [ false = receipt must not be digitally signed ] |

Asynchronous Receipt

| Description | Indicates whether the recipient should reply to incoming AS2 messages using the same HTTP/HTTPS connection that the sender is using for delivery. This field is only applicable to send partnerships. |
| Dependencies | [ Request Receipt = true ] |
| Options | [ true = asynchronous reply ], [ false = synchronous reply ] |

Synchronous reply

AS2 message receipts are encapsulated in the HTTP response.

Asynchronous reply

AS2 message receipts will be delivered through another HTTP connection from recipient to sender.
Receipt Return URL

| Description | This is the endpoint URL of Hermes or another compatible messaging gateway for receiving receipts. It is always the inbound endpoint URL of the send partnership. For example:
- **Sender (A)** IP address: 1.1.1.1:8080
- **Recipient (B)** IP address: 1.1.1.2:8080
- AS2 inbound endpoint: /corvus/httpd/as2/inbound
  Then the Receipt Return URL for an AS2 message from sender (A) is the inbound endpoint of sender (A), which is http://1.1.1.1:8080/corvus/httpd/as2/inbound/
  This field is only applicable to send partnerships. |
| Dependencies | [Request Receipt = true], [Asynchronous Receipt = true] |

Message Compression Required

| Description | Indicates whether the sender must compress outgoing AS2 messages in this partnership. This field is only applicable for send partnerships. |
| Options | [true = outgoing AS2 messages must be compressed], [false = outgoing AS2 messages must not be compressed] |

Message Signing Required

| Description | Indicates whether the sender must digitally sign AS2 messages using their private key. This field is only applicable for send partnerships. |
| Options | [true = outgoing AS2 messages must be digitally signed], [false = outgoing AS2 messages must not be digitally signed] |

Signing Algorithm

| Description | The algorithm used to digitally sign outgoing AS2 messages in this partnership. |
| Options | [SHA1], [MD5] |
### Message Encryption Required

<table>
<thead>
<tr>
<th>Description</th>
<th>Indicates whether the sender must encrypt AS2 messages using the recipient’s public certificate defined in Certificate for Encryption. The encryption method is based on the S/MIME standard. This field is only applicable for send partnerships.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dependencies</td>
<td>Certificate for Encryption REQUIRED</td>
</tr>
<tr>
<td>Options</td>
<td>[true = outgoing AS2 messages must be encrypted], [false = outgoing AS2 messages must not be encrypted]</td>
</tr>
</tbody>
</table>

### Encryption Algorithm

<table>
<thead>
<tr>
<th>Description</th>
<th>The algorithm used to encrypt outgoing AS2 messages in this partnership.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Options</td>
<td>[3DES], [RC2]</td>
</tr>
</tbody>
</table>

### Certificate for Encryption

<table>
<thead>
<tr>
<th>Description</th>
<th>The certificate (.cer) file for encrypting outgoing AS2 messages using the public key exported by the recipient. The recipient should use the keystore in the AS2 plugin to export the public certificate for the sender. AS2 default keystore location: $HERMES2_HOME/plugins/corvus-as2/security. The keystore must be in PKCS12 format. See Message Encryption Required for details.</th>
</tr>
</thead>
</table>

### MIC Algorithm

<table>
<thead>
<tr>
<th>Description</th>
<th>The algorithm used to create message digests/hashes for outgoing AS2 messages in this partnership.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Options</td>
<td>[SHA1], [MD5]</td>
</tr>
</tbody>
</table>

### Maximum Retries

<table>
<thead>
<tr>
<th>Description</th>
<th>The maximum number of retries allowed for the sender to attempt delivering an AS2 message. Hermes tries to deliver the AS2 message under the specification of reliable messaging until exceeding the maximum number of retries. There will be a time interval between each attempt, which is defined in Retry Interval (ms). It is RECOMMENDED that the value of this field be between 1–10.</th>
</tr>
</thead>
</table>
## Retry Interval (ms)

| Description | The time interval (milliseconds) between each consecutive attempt to deliver an AS2 message. It is RECOMMENDED that the value of this field be between 30000-300000. |

## Message Signature Enforced

| Description | Indicates whether incoming AS2 messages must be digitally signed. If enabled, AS2 messages in this partnership must be digitally signed by the sender before the message is received by the recipient. This field is only applicable to receive partnerships. |
| Options | [ true = incoming AS2 messages must be digitally signed ], [ false = incoming AS2 messages may not be digitally signed ] |

## Message Encryption Enforced

| Description | Indicates whether incoming AS2 messages must be encrypted. If enforced, AS2 message in this partnership must be encrypted by the sender before the message is received by the recipient. This field is only applicable to receive partnerships. |
| Options | [ true = incoming AS2 messages must be encrypted ], [ false = incoming AS2 messages may not be encrypted ] |

## Certificate for Verification

| Description | The certificate (.cer) file for verifying incoming digitally signed AS2 messages using the public key generated by the sender. The sender should use the keystore in the AS2 plugin to export the public certificate for the recipient. AS2 default keystore location: `<HERMES2_HOME>/plugins/corvus-as2/security` The keystore must be in PKCS12 format. See Message Signing Required for details. |
Configuring Hermes

Introduction

This document acts as a configuration reference for Hermes. The configurations of Hermes are specified by various XML-based configuration files. By modifying these files, administrators or developers can configure all the settings such as the location of the database and log file.

The intended audience of this document includes system administrators, application developers and plugin developers of the Hermes system. It assumes the audience has following background knowledge:

- Java (Standard Edition)
- XML
- AS2
- ebXML Messaging Services
- Public Key Infrastructure
- Application server compliant to Servlet 2.x specification
- Databases

Overview on loading property files

Hermes has employed a module-group-component architecture where you can define your own module for each application. You can assign a property file for each component and the Hermes Core System will load these files.

There are two loading mechanisms, one for the core system and one for the plugins. The two are almost identical except for their initial definitions.

Let's take a look at how the core system modules are loaded.

For the core system, Hermes will look for the existence of a file named `sys.properties` from the classpath which contains the location of the module-group definition file. E.g.,

```
sys.module.group=doc-processor.module-group.xml
```

From there, the system will look for the specified XML file and load up the modules specified within. The modules could be System Modules, which contain infrastructure components such as logging and database access, or they could be Active Modules, which perform business functions such as sending messages.
For the plugins, instead of looking for a file named `sys.properties`, Hermes will look for a file named `plugin.xml` instead.

From within, a parameter with the value `module-group-descriptor` will define the location of the module-group definition.

```
<?xml version="1.0" encoding="UTF-8"?>
<plugin>
  <id>hk.hku.cecid.edi.as2</id>
  <name>Corvus AS2 Plugin</name>
  <version>1.0.1</version>
  <provider-name>hk.hku.cecid</provider-name>
  <class>hk.hku.cecid.edi.as2.AS2Processor</class>
  <parameters>
    <parameter name="module-group-descriptor" value="hk/hku/cecid/edi/as2/conf/as2.module-group.xml"/>
  </parameters>
</plugin>
```

**Hermes core system properties**

You can modify the following information either through the web admin interface or by manipulating the XML configuration files directly.

The configuration files are stored in `<WEBAPPS_LOCATION>/corvus/WEB-INF/classes/hk/hku/cecid/piazza/corvus/core/conf` (where `<WEBAPPS_LOCATION>` is the web application repository of the application server).
<table>
<thead>
<tr>
<th>Properties</th>
<th>Configuration file</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Hermes location</td>
<td>corvus.properties.xml</td>
</tr>
<tr>
<td>2. Plugin location for Hermes</td>
<td></td>
</tr>
<tr>
<td>3. SSL trust store information</td>
<td></td>
</tr>
<tr>
<td>4. HTTP/HTTPS proxy server</td>
<td></td>
</tr>
<tr>
<td>5. Encoding settings for core system</td>
<td></td>
</tr>
<tr>
<td>6. Connection timeout settings</td>
<td></td>
</tr>
<tr>
<td>7. Log file location and level of logging</td>
<td>corvus.log.properties.xml</td>
</tr>
</tbody>
</table>

### Hermes location

You can change the location of Hermes by modifying this element:

```
<corvus>
  <home>/corvus</home>
  ...
</corvus>
```

<table>
<thead>
<tr>
<th>XPath</th>
<th>Expected information</th>
</tr>
</thead>
<tbody>
<tr>
<td>/corvus/home</td>
<td>The location in which Hermes is installed. Note that the specified path is an absolute path.</td>
</tr>
</tbody>
</table>

### Plugin location for Hermes

You can change the plugin location of Hermes by modifying this element:

```
<corvus>
  ...
  <plugin>
    ...
    <registry>/home/hermes2/plugins</registry>
    <descriptor>plugin.xml</descriptor>
    ...
  </plugin>
  ...
</corvus>
```

<table>
<thead>
<tr>
<th>XPath</th>
<th>Expected information</th>
</tr>
</thead>
<tbody>
<tr>
<td>/corvus/plugin/registry</td>
<td>The location in which Hermes plugins are installed. By default, it should be the plugins directory under the home directory where Hermes is installed. Note that the specified path is an absolute path.</td>
</tr>
<tr>
<td>/corvus/plugin/descriptor</td>
<td>The name of the XML file which Hermes will use when loading the module-group-component.</td>
</tr>
</tbody>
</table>

### SSL trust store information

```
<corvus>
  ...
  <environment>
    <properties>
```
XPath | Expected information
--- | ---
/\corvus/environment/properties/javax.net.ssl.trustStore | The location of the Java keystore which is used for establishing SSL connections. The keystore should contain the certificates of trusted certificate authorities. To maintain the keystore, the reader should use the \texttt{keytool} provided by JDK. For more information, the reader may reference \url{http://docs.oracle.com/javase/8/docs/technotes/tools/windows/keytool.html}.
/\corvus/environment/properties/javax.net.ssl.trustStorePassword | The password used to access the keystore specified above.

**HTTP/HTTPS proxy server**

XPath | Expected information
--- | ---
/\corvus/environment/properties/http.proxyHost | The hostname or IP address of the proxy host that Hermes will establish HTTP connections with for outgoing messages.
/\corvus/environment/properties/http.proxyPort | The TCP port of the proxy server specified above.
/\corvus/environment/properties/https.proxyHost | The hostname or IP address of the proxy host that Hermes will establish HTTPS connections with for outgoing messages.
/\corvus/environment/properties/https.proxyPort | The TCP port of the proxy server specified above.

**Encoding settings for core system**

XPath | Expected information
--- | ---
/\corvus/encoding/servlet-request | UTF-8
/\corvus/encoding/servlet-response | text/html;UTF-8
XPath | Expected information
--- | ---
/corvus/encoding/servlet-request | The encoding of incoming HTTP or HTTPS requests. UTF-8 is the recommended value because it can handle most written languages.
/corvus/encoding/servlet-response | The encoding of outgoing HTTP or HTTP responses.

**Connection timeout settings**

```
<corvus>
  ...
  <properties>
  ...
  <sun.net.client.defaultConnectTimeout>30000</sun.net.client.defaultConnectTimeout>
  <sun.net.client.defaultReadTimeout>300000</sun.net.client.defaultReadTimeout>
  ...
  </properties>
  ...
</corvus>
```

XPath | Expected information
--- | ---
/corvus/properties/sun.net.client.defaultConnectTimeout | It specifies the timeout (in milliseconds) for establishing HTTP or HTTPS connections for outgoing messages. 30 seconds is the recommended value.
/corvus/properties/sun.net.client.defaultReadTimeout | It specifies the timeout (in milliseconds) for reading from input streams when a HTTP or HTTPS connection is established. 300 seconds is the recommended value.

**Log file location and level of logging**

To change the settings of the log written by the core system, you will need to modify the XML file named `corvus.log.properties.xml`. Configuring the logging module is the same as configuring Apache Log4j. Note that for configuring the logs of other plugins, you need to edit another configuration file as described in AS2 plugin properties and ebMS plugin properties.

```
  <appender name="stdout" class="org.apache.log4j.ConsoleAppender">
    <layout class="org.apache.log4j.PatternLayout">
      <param name="ConversionPattern" value="%d{yyyy-MM-dd HH:mm:ss} [%-12.12t] <%-5p&gt; <%m>%n"/>
    </layout>
  </appender>

  <appender name="corvus" class="org.apache.log4j.RollingFileAppender">
    <param name="File" value="/home/hermes2/logs/corvus.log"/>
    <param name="Encoding" value="UTF-8"/>
    <param name="MaxFileSize" value="100KB"/>
    <param name="MaxBackupIndex" value="1"/>
    <layout class="org.apache.log4j.PatternLayout">
      <param name="ConversionPattern" value="%d{yyyy-MM-dd HH:mm:ss} [%-12.12t] <%-5p&gt; <%m&gt;%n"/>
    </layout>
  </appender>
</log4j:configuration>
```

3.6. Configuring Hermes
```xml
<category name="hk.hku.cecid.piazza">
    <priority value="debug"/>
    <appender-ref ref="corvus"/>
</category>
</log4j:configuration>
```

<table>
<thead>
<tr>
<th>XPath</th>
<th>Expected information</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>/log4j:configuration/category/priority</code></td>
<td>The log level of core system logging. The available levels are debug, info, warn, error and fatal. If you set the value as debug, all logs will be printed.</td>
</tr>
<tr>
<td><code>/log4j:configuration/category/appender-ref@ref</code></td>
<td>The name of the appender element to be used for logging. The appender element specifies how to generate log files. In the above example, the appender named <code>corvus</code> is used. The settings of the appender are specified by the referenced <code>appender</code> element.</td>
</tr>
<tr>
<td><code>/log4j:configuration/appender@class</code></td>
<td>The appender specified by the appender configuration element. Apache Log4j provides a series of appenders, such as <code>RollingFileAppender</code> and <code>DailyRollingFileAppender</code>.</td>
</tr>
<tr>
<td><code>/log4j:configuration/appender@name</code></td>
<td>The name of the appender configuration element. <code>/log4j:configuration/category/appender-ref@ref</code> should reference the appender configuration element by this name.</td>
</tr>
<tr>
<td><code>/log4j:configuration/appender/param[@name='File']/@value</code> (i.e. The value attribute of the param element under the appender element, whose name attribute is <code>File</code>)</td>
<td>The path of the core system log from this appender.</td>
</tr>
<tr>
<td><code>/log4j:configuration/appender/param[@name='Encoding']/@value</code> (i.e. The value attribute of the param element under the appender element, whose name attribute is <code>Encoding</code>)</td>
<td>The encoding to be used for the log file.</td>
</tr>
<tr>
<td><code>/log4j:configuration/appender/param[@name='MaxFileSize']/@value</code> (i.e. The value attribute of the param element under the appender element, whose name attribute is <code>MaxFileSize</code>)</td>
<td>If the size of a log file has grown to exceed this limit, a new log file will be written and the old log file will be backed up. An index will be appended to the name of the old log file. (e.g. <code>corvus.log.1</code>).</td>
</tr>
<tr>
<td><code>/log4j:configuration/appender/param[@name='MaxBackupIndex']/@value</code> (i.e. The value attribute of the param element under the appender element, whose name attribute is <code>MaxBackupIndex</code>)</td>
<td>The maximum number of log files that will be backed up. For example, if it is set to 10, the maximum number of backed up log files will be 10 and their filenames will be <code>xxx.log.1</code>, <code>xxx.log.2</code>, ..., <code>xxx.log.10</code>.</td>
</tr>
<tr>
<td><code>/log4j:configuration/appender/layout/param[@name='ConversionPattern']/@value</code></td>
<td>The pattern used when writing the log file.</td>
</tr>
</tbody>
</table>

**Hermes plugin properties**
AS2 plugin

In the directory `<HERMES_2_PLUGINS_LOCATION>/corvus-as2/conf/hk/hku/cecid/edi/as2/conf` there are some configuration files for Hermes’s AS2 plugin. Which configuration file you should edit depends on the property:

<table>
<thead>
<tr>
<th>Properties</th>
<th>Configuration file</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log file location and level of logging</td>
<td>as2.log.properties.xml</td>
</tr>
<tr>
<td>Connection to message database</td>
<td>as2.module.core.xml</td>
</tr>
<tr>
<td>Location of keystore for signing outgoing messages</td>
<td></td>
</tr>
<tr>
<td>Location of message repository</td>
<td></td>
</tr>
</tbody>
</table>

Log file location and level of logging

To change the location of the log file, you will need to modify the XML file named `as2.log.properties.xml`.

```xml
  <appender name="stdout" class="org.apache.log4j.ConsoleAppender">
    <layout class="org.apache.log4j.PatternLayout">
      <param name="ConversionPattern" value="%d{yyyy-MM-dd HH:mm:ss} [%-12.12t] (%r) [%5p] %c{1}:%L - %m%n"/>
    </layout>
  </appender>
  <appender class="org.apache.log4j.RollingFileAppender" name="as2">
    <param name="File" value="/home/hermes2/logs/as2.log"/>
    <param name="Encoding" value="UTF-8"/>
    <param name="MaxFileSize" value="5MB"/>
    <param name="MaxBackupIndex" value="1"/>
    <layout class="org.apache.log4j.PatternLayout">
      <param name="ConversionPattern" value="%d{yyyy-MM-dd HH:mm:ss} [%-12.12t] (%r) [%5p] %c{1}:%L - %m%n"/>
    </layout>
  </appender>
  <category name="hk.hku.cecid.edi.as2">
    <priority value="debug"/>
    <appender-ref ref="as2"/>
  </category>
</log4j:configuration>
```
<table>
<thead>
<tr>
<th>XPath</th>
<th>Expected information</th>
</tr>
</thead>
<tbody>
<tr>
<td>/log4j:configuration/category/priority</td>
<td>The log level of the AS2 plugin logging. The available levels are debug, info, warn, error and fatal. If you set the value as debug, all logs will be printed.</td>
</tr>
<tr>
<td>/log4j:configuration/category/appender-ref@ref</td>
<td>The name of the appender element to be used for logging. The appender element specifies how to generate log files. In the above example, the appender named as2 is used. The settings of the appender are specified by the referenced appender element.</td>
</tr>
<tr>
<td>/log4j:configuration/appender@class</td>
<td>The appender specified by this appender configuration element. Apache Log4j provides a series of appenders, such as RollingFileAppender and DailyRollingFileAppender.</td>
</tr>
<tr>
<td>/log4j:configuration/appender@name</td>
<td>The name of this appender configuration element. /log4j:configuration/category/appender-ref@ref should reference the appender configuration element by this name.</td>
</tr>
<tr>
<td>/log4j:configuration/appender/param[@name='File']/@value (i.e. The value attribute of the param element under the appender element, whose name attribute is File)</td>
<td>The path of the AS2 log of this appender.</td>
</tr>
<tr>
<td>/log4j:configuration/appender/param[@name='Encoding']/@value (i.e. The value attribute of the param element under the appender element, whose name attribute is Encoding)</td>
<td>The encoding to be used for the log file.</td>
</tr>
<tr>
<td>/log4j:configuration/appender/param[@name='MaxFileSize']/@value (i.e. The value attribute of the param element under the appender element, whose name attribute is MaxFileSize)</td>
<td>If the size of a log file has grown to exceed this limit, another new log file will be written and the old log file will be backed up. An index will be appended to the name of the old log file (e.g. as2.log.1).</td>
</tr>
<tr>
<td>/log4j:configuration/appender/param[@name='MaxBackupIndex']/@value (i.e. The value attribute of the param element under the appender element, whose name attribute is MaxBackupIndex)</td>
<td>The maximum number of log files that will be backed up. For example, if it is set to 10, the maximum number of backed up log files will be 10 and their filenames will be xxx.log.1, xxx.log.2, ..., xxx.log.10.</td>
</tr>
<tr>
<td>/log4j:configuration/appender/layout/param[@name='ConversionPattern']/@value</td>
<td>The pattern used when writing the log file.</td>
</tr>
</tbody>
</table>

### Connection to message database

```xml
<module>
  ...
  <component id="daofactory" name="AS2 DAO Factory">
    <class>
      hk.hku.cecid.piazza.commons.dao.ds.SimpleDSDAOFactory
    </class>
    <parameter name="driver" value="org.postgresql.Driver" />
    <parameter name="url" value="jdbc:postgresql://localhost:5432/as2" />
    <parameter name="username" value="corvus" />
  </component>
</module>
```
<parameter name="password" value="corvus" />
<parameter name="pooling" value="true" />
<parameter name="maxActive" value="30" />
<parameter name="maxIdle" value="10" />
<parameter name="maxWait" value="-1" />
<parameter name="testOnBorrow" value="true" />
<parameter name="testOnReturn" value="false" />
<parameter name="testWhileIdle" value="false" />
<parameter name="validationQuery" value="SELECT now()" />
<parameter name="config" value="hk/hku/cecid/edi/as2/conf/as2.dao.xml" />
</component>
...
</module>
### XPath

<table>
<thead>
<tr>
<th>XPath</th>
<th>Expected information</th>
</tr>
</thead>
</table>
| /module/component[@id='daofactory']/class | The Java class to use when establishing a database connection. You can select:  
- `hk.hku.cecid.piazza.commons.dao.ds.SimpleDSDAOFactory`, if you want AS2 to manage the database connection pool  
- `hk.hku.cecid.piazza.commons.dao.ds.DataSourceDAOFactory`, if you want the application server to manage the database connection pool, which is accessible through the Java Naming and Directory Interface (JNDI) name. |

Belows are fields you need to fill in if you are using SimpleDSDAOFactory

<table>
<thead>
<tr>
<th>XPath</th>
<th>Expected information</th>
</tr>
</thead>
<tbody>
<tr>
<td>/module/component[@id='daofactory']/parameter[@name='driver']/@value</td>
<td>The JDBC driver that should be used. The driver for Postgres is provided by default. The driver should be placed in the directory <code>&lt;TOMCAT_HOME&gt;/webapps/corvus/WEB-INF/lib</code>, where we suppose the web application repository is configured as <code>&lt;TOMCAT_HOME&gt;/webapps</code>.</td>
</tr>
<tr>
<td>/module/component[@id='daofactory']/parameter[@name='url']/@value</td>
<td>The URL for establishing the database connection. Please refer to the documentation of the JDBC driver for the syntax. For PostgreSQL, the syntax is <code>jdbc:postgresql://&lt;IP or hostname of the database&gt;:/message database name for AS2</code>.</td>
</tr>
<tr>
<td>/module/component[@id='daofactory']/parameter[@name='username']/@value</td>
<td>The username to connect to the database.</td>
</tr>
<tr>
<td>/module/component[@id='daofactory']/parameter[@name='password']/@value</td>
<td>The password for the username specified.</td>
</tr>
<tr>
<td>/module/component[@id='daofactory']/parameter[@name='pooling']/@value</td>
<td>The boolean value (true/false) specifying if connection pooling should be used.</td>
</tr>
<tr>
<td>/module/component[@id='daofactory']/parameter[@name='maxActive']/@value</td>
<td>The maximum number of active threads.</td>
</tr>
<tr>
<td>/module/component[@id='daofactory']/parameter[@name='maxIdle']/@value</td>
<td>The maximum number of threads that can remains idle.</td>
</tr>
<tr>
<td>/module/component[@id='daofactory']/parameter[@name='maxWait']/@value</td>
<td>The maximum amount of time (milliseconds) that the pool will wait (when there are no available connections) for a connection to be returned before throwing an exception, or <code>-1</code> to wait indefinitely.</td>
</tr>
<tr>
<td>/module/component[@id='daofactory']/parameter[@name='testOnBorrow']/@value</td>
<td>Parameter used by system during testing, please keep it unchanged</td>
</tr>
<tr>
<td>/module/component[@id='daofactory']/parameter[@name='testOnReturn']/@value</td>
<td>Parameter used by system during testing, please keep it unchanged</td>
</tr>
<tr>
<td>/module/component[@id='daofactory']/parameter[@name='testWhileIdle']/@value</td>
<td>Parameter used by system during testing, please keep it unchanged</td>
</tr>
<tr>
<td>/module/component[@id='daofactory']/parameter[@name='validateQuery']/@value</td>
<td>Parameter used by system during testing, please keep it unchanged</td>
</tr>
<tr>
<td>/module/component[@id='daofactory']/parameter[@name='config']/@value</td>
<td>Additional configuration files that will be used by the plugin. You should just leave it as is.</td>
</tr>
</tbody>
</table>

Belows are fields you need to fill in if you are using DataSourceDAOFactory

<table>
<thead>
<tr>
<th>XPath</th>
<th>Expected information</th>
</tr>
</thead>
<tbody>
<tr>
<td>datasource</td>
<td>The JNDI name of the data source for connecting to the message database, e.g. <code>java:/comp/env/jdbc/as2db</code></td>
</tr>
</tbody>
</table>
Location of keystore for signing outgoing messages

```xml
<module id="as2.core" name="Corvus AS2" version="1.0">
...
</module>

<component id="keystore-manager" name="AS2 Key Store Manager">
  <class>hk.hku.cecid.piazza.commons.security.KeyStoreManager</class>
  <parameter name="keystore-location" value="corvus.p12"/>
  <parameter name="keystore-password" value="password"/>
  <parameter name="key-alias" value="corvus"/>
  <parameter name="key-password" value="password"/>
  <parameter name="keystore-type" value="PKCS12"/>
  <parameter name="keystore-provider" value="org.bouncycastle.jce.provider.BouncyCastleProvider"/>
</component>
...
</module>
```

<table>
<thead>
<tr>
<th>XPath</th>
<th>Expected information</th>
</tr>
</thead>
<tbody>
<tr>
<td>/module/component[@id='keystore-manager']/parameter[@name='keystore-location']/@value</td>
<td>The path of the keystore for signing outgoing messages.</td>
</tr>
<tr>
<td>/module/component[@id='keystore-manager']/parameter[@name='keystore-password']/@value</td>
<td>The password for accessing the keystore.</td>
</tr>
<tr>
<td>/module/component[@id='keystore-manager']/parameter[@name='key-alias']/@value</td>
<td>The alias of the private key for a digital signature.</td>
</tr>
<tr>
<td>/module/component[@id='keystore-manager']/parameter[@name='key-password']/@value</td>
<td>The password protecting the private key for a digital signature.</td>
</tr>
<tr>
<td>/module/component[@id='keystore-manager']/parameter[@name='keystore-type']/@value</td>
<td>The keystore format. It is either PKCS12 or JKS.</td>
</tr>
</tbody>
</table>

Location of the message repository

Outgoing Repository:

```xml
<module id="as2.core" name="Corvus AS2" version="1.0">
...
</module>

<component id="outgoing-payload-repository" name="AS2 Outgoing Payload Repository">
  <class>hk.hku.cecid.edi.as2.module.PayloadRepository</class>
  <parameter name="location" value="/home/hermes2/repository/as2-outgoing-repository"/>
  <parameter name="type-edi" value="application/EDIFACT"/>
  <parameter name="type-x12" value="application/EDI-X12"/>
  <parameter name="type-eco" value="application/edi-consent"/>
  <parameter name="type-xml" value="application/XML"/>
</component>
...
</module>
```
<table>
<thead>
<tr>
<th>XPath</th>
<th>Expected information</th>
</tr>
</thead>
<tbody>
<tr>
<td>/module/component[id='outgoing-payload-repository']/class</td>
<td>The Java class responsible for handling outgoing payload. You should just leave it as is.</td>
</tr>
<tr>
<td>/module/component[id='outgoing-payload-repository']/parameter[@name='location']/@value</td>
<td>The directory that will store the outgoing payload. E.g., /home/hermes2/repository/as2-outgoing-repository</td>
</tr>
<tr>
<td>/module/component[id='outgoing-payload-repository']/parameter[@name='type-edi']/@value</td>
<td>You should leave these fields as is.</td>
</tr>
<tr>
<td>/module/component[id='outgoing-payload-repository']/parameter[@name='type-x12']/@value</td>
<td></td>
</tr>
<tr>
<td>/module/component[id='outgoing-payload-repository']/parameter[@name='type-eco']/@value</td>
<td></td>
</tr>
<tr>
<td>/module/component[id='outgoing-payload-repository']/parameter[@name='type-xml']/@value</td>
<td></td>
</tr>
</tbody>
</table>

```xml
<module id="as2.core" name="Corvus AS2" version="1.0">
   ...
   <component id="incoming-payload-repository" name="AS2 Incoming Payload Repository">
      <class>hk.hku.cecid.edi.as2.module.PayloadRepository</class>
      <parameter name="location" value="/home/hermes2/repository/as2-incoming-repository" />
      <parameter name="type-edi" value="application/EDIFACT" />
      <parameter name="type-x12" value="application/EDI-X12" />
      <parameter name="type-eco" value="application/edi-consent" />
      <parameter name="type-xml" value="application/XML" />
   </component>
   ...
</module>
```
### Expected information

<table>
<thead>
<tr>
<th>XPath</th>
<th>Expected information</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>/module/component[id='incoming-payload-repository']/class</code></td>
<td>The Java class responsible for handling incoming payloads. You should just leave it as is.</td>
</tr>
<tr>
<td><code>/module/component[id='outgoing-payload-repository']/parameter[@name='location']/@value</code></td>
<td>The directory that will store the outgoing payload. E.g., <code>/home/hermes2/repository/as2-incoming-repository</code></td>
</tr>
<tr>
<td><code>/module/component[id='outgoing-payload-repository']/parameter[@name='type-edi']/@value</code></td>
<td>You should leave these fields as is.</td>
</tr>
<tr>
<td><code>/module/component[id='outgoing-payload-repository']/parameter[@name='type-x12']/@value</code></td>
<td></td>
</tr>
<tr>
<td><code>/module/component[id='outgoing-payload-repository']/parameter[@name='type-eco']/@value</code></td>
<td></td>
</tr>
<tr>
<td><code>/module/component[id='outgoing-payload-repository']/parameter[@name='type-xml']/@value</code></td>
<td></td>
</tr>
</tbody>
</table>

Original Message Repository (a temporary message repository used when Hermes is composing or receiving AS2 messages):

```xml
<module id="as2.core" name="Corvus AS2" version="1.0">
  ...
  <component id="original-message-repository" name="AS2 Original Message Repository">
    <class>hk.hku.cecid.edi.as2.module.MessageRepository</class>
    <parameter name="location" value="/home/hermes2/repository/as2-message-repository" />
    <parameter name="is-disabled" value="false" />
  </component>
  ...
</module>
```

### Expected information

<table>
<thead>
<tr>
<th>XPath</th>
<th>Expected information</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>/module/component[id='original-payload-repository']/class</code></td>
<td>The Java class responsible for handling original messages. You should just leave it as is.</td>
</tr>
<tr>
<td><code>/module/component[id='original-payload-repository']/parameter[@name='location']/@value</code></td>
<td>The directory that will store outgoing payloads. E.g., <code>/home/hermes2/repository/as2-message-repository</code></td>
</tr>
<tr>
<td><code>/module/component[id='original-payload-repository']/parameter[@name='is-disabled']/@value</code></td>
<td>This flag indicates if the original message should be stored locally.</td>
</tr>
</tbody>
</table>
Hermes Documentation, Release 2.2

ebMS plugin

In the directory `<HERMES_2_PLUGINS_LOCATION>/corvus-ebms/conf/hk/hku/cecid/ebms/spa/conf`, there are some configuration files for Hermes’s ebMS plugin. The configuration file you should edit depends on the property:

<table>
<thead>
<tr>
<th>Properties</th>
<th>Configuration file</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log file location and level of logging</td>
<td>log4j.properties.xml</td>
</tr>
<tr>
<td>Connections to message database</td>
<td>ebms.module.xml</td>
</tr>
<tr>
<td>Location of keystore for signing outgoing messages</td>
<td></td>
</tr>
<tr>
<td>Location of keystore for S/MIME decryption (incoming messages)</td>
<td></td>
</tr>
</tbody>
</table>

Log file location and level of logging

To change the location of the log file, you will need to modify the XML file named `log4j.properties.xml`

```xml
  <appender name="stdout" class="org.apache.log4j.ConsoleAppender">
    <layout class="org.apache.log4j.PatternLayout">
      <param name="ConversionPattern" value="%d{yyyy-MM-dd HH:mm:ss} [%-12.12t] %5p [%c{3}] %m%n"/>
    </layout>
  </appender>
  <appender name="ebms" class="org.apache.log4j.RollingFileAppender">
    <param name="File" value="/home/hermes2/logs/ebms.log"/>
    <param name="Encoding" value="UTF-8"/>
    <param name="MaxFileSize" value="5MB"/>
    <param name="MaxBackupIndex" value="1"/>
    <layout class="org.apache.log4j.PatternLayout">
      <param name="ConversionPattern" value="%d{yyyy-MM-dd HH:mm:ss} [%-12.12t] %5p %c{3} %m%n"/>
    </layout>
  </appender>
  <category name="hk.hku.cecid.ebms">
    <priority value="debug"/>
    <appender-ref ref="ebms"/>
  </category>
</log4j:configuration>
```
<table>
<thead>
<tr>
<th>XPath</th>
<th>Expected information</th>
</tr>
</thead>
<tbody>
<tr>
<td>/log4j:configuration/category/priority</td>
<td>The log level of the ebMS plugin logging. The available levels are debug, info, warn, error and fatal. If you set the value as debug, all logs will be printed.</td>
</tr>
<tr>
<td>/log4j:configuration/category/appender-ref@ref</td>
<td>The name of the appender element to be used for logging. The appender element specifies how to generate log files. In the above example, the appender named RollingFileAppender is used. The settings of the appender are specified by the referenced appender element.</td>
</tr>
<tr>
<td>/log4j:configuration/appender@class</td>
<td>The appender specified by this appender configuration element. Apache Log4j provides a series of appenders, such RollingFileAppender and DailyRollingFileAppender.</td>
</tr>
<tr>
<td>/log4j:configuration/appender@name</td>
<td>The name of this appender configuration element. /category/appender-ref@ref should reference the appender configuration element by this name.</td>
</tr>
<tr>
<td>/log4j:configuration/appender/param[@name='File']/@value</td>
<td>The path of the ebMS log of this appender.</td>
</tr>
<tr>
<td>/log4j:configuration/appender/param[@name='Encoding']/@value</td>
<td>The encoding to be used for the log file.</td>
</tr>
<tr>
<td>/log4j:configuration/appender/param[@name='MaxFileSize']/@value</td>
<td>If the size of a log file has grown to exceed this limit, another log file will be written and the old log file will be backed up. An index will be appended to the name of the old log file (e.g. ebms.log.1).</td>
</tr>
<tr>
<td>/log4j:configuration/appender/param[@name='MaxBackupIndex']/@value</td>
<td>The maximum number of log files that will be backed up. For example, if it is set to 10, the maximum number of backed up log files will be 10 and their filenames will be xxx.log.1, xxx.log.2, ..., xxx.log.10.</td>
</tr>
<tr>
<td>/log4j:configuration/appender/layout/param[@name='ConversionPattern']/@value</td>
<td>The pattern used when writing the log file.</td>
</tr>
</tbody>
</table>

**Connection to message database**

```xml
<module>
  ...
  <component id="daofactory" name="System DAO Factory">
    <class>hk.hku.cecid.piazza.commons.dao.ds.SimpleDSDAOFactory</class>
    <parameter name="driver" value="org.postgresql.Driver" />
    <parameter name="url" value="jdbc:postgresql://localhost:5432/ebms" />
    <parameter name="username" value="corvus" />
    <parameter name="password" value="corvus" />
    <parameter name="pooling" value="true" />
    <parameter name="maxActive" value="30" />
  </component>
</module>
```
<parameter name="maxIdle" value="10" />
<parameter name="maxWait" value="-1" />
<parameter name="testOnBorrow" value="true" />
<parameter name="testOnReturn" value="false" />
<parameter name="testWhileIdle" value="false" />
<parameter name="validationQuery" value="SELECT now()" />
<parameter name="config">hk/hku/cecid/ebms/spa/conf/ebms.dao.xml</parameter>
...
</module>
**XPath**

<table>
<thead>
<tr>
<th>Expected information</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Java class to use when establishing a database connection. You can select:</td>
</tr>
<tr>
<td>• <code>hk.hku.cecid.piazza.commons.dao.ds.SimpleDSDAOFactory</code>, if you want ebMS to manage the database connection pool.</td>
</tr>
<tr>
<td>• <code>hk.hku.cecid.piazza.commons.dao.ds.DataSourceDAOFactory</code>, if you want the application server to manage the database connection pool, which is accessible through the Java Naming and Directory Interface (JNDI) name.</td>
</tr>
</tbody>
</table>

Below are fields you need to fill in if you are using SimpleDSDAOFactory

<table>
<thead>
<tr>
<th>Expected information</th>
</tr>
</thead>
<tbody>
<tr>
<td>The JDBC driver that should be used. The driver for Postgres is provided by default. The driver should be placed in the directory <code>&lt;TOMCAT_HOME&gt;/webapps/corvus/WEB-INF/lib</code>, where we suppose the web application repository is configured as <code>&lt;TOMCAT_HOME&gt;/webapps</code>.</td>
</tr>
<tr>
<td>The URL for establishing the database connection. Please refer to the documentation of the JDBC driver for the syntax. For PostgreSQL, the syntax is <code>jdbc:postgresql://&lt;IP or hostname of the database&gt;/&lt;message database name for AS2&gt;</code></td>
</tr>
<tr>
<td>The username to connect to the database.</td>
</tr>
<tr>
<td>The password for the username specified.</td>
</tr>
<tr>
<td>The boolean value (true/false) specifying if connection pooling should be used.</td>
</tr>
<tr>
<td>The maximum number of active threads.</td>
</tr>
<tr>
<td>The maximum number of threads that can remains idle.</td>
</tr>
<tr>
<td>The maximum amount of time (milliseconds) that the pool will wait (when there are no available connections) for a connection to be returned before throwing an exception, or -1 to wait indefinitely.</td>
</tr>
<tr>
<td>Parameter used by system during testing, please keep it unchanged</td>
</tr>
<tr>
<td>Parameter used by system during testing, please keep it unchanged</td>
</tr>
<tr>
<td>Parameter used by system during testing, please keep it unchanged</td>
</tr>
<tr>
<td>Parameter used by system during testing, please keep it unchanged</td>
</tr>
<tr>
<td>Additional configuration files that will be used by the plugin. You should just leave it as is.</td>
</tr>
</tbody>
</table>

Below are fields you need to fill in if you are using DataSourceDAOFactory

<table>
<thead>
<tr>
<th>Expected information</th>
</tr>
</thead>
<tbody>
<tr>
<td>The JNDI name of the data source for connecting to the message database, e.g. <code>java:/comp/env/jdbc/ebmsdb</code></td>
</tr>
</tbody>
</table>
Location of keystore for signing outgoing messages

```xml
<module id="ebms.main" name="Ebms Plugin" version="1.0">
  ...
  <component id="keystore-manager-for-signature" name="Key Store Manager for Digital Signature">
    <class>hk.hku.cecid.piazza.commons.security.KeyStoreManager</class>
    <parameter name="keystore-location" value="/home/hermes2/plugins/corvus-ebms/security/corvus.p12"/>
    <parameter name="keystore-password" value="password"/>
    <parameter name="key-alias" value="corvus"/>
    <parameter name="key-password" value="password"/>
    <parameter name="keystore-type" value="PKCS12"/>
    <parameter name="keystore-provider" value="org.bouncycastle.jce.provider.BouncyCastleProvider"/>
  </component>
  ...
</module>
```

<table>
<thead>
<tr>
<th>XPath</th>
<th>Expected information</th>
</tr>
</thead>
<tbody>
<tr>
<td>/module/component[@id='keystore-manager-for-signature']/parameter[@name='keystore-location']/@value</td>
<td>The path of the keystore for signing outgoing messages.</td>
</tr>
<tr>
<td>/module/component[@id='keystore-manager-for-signature']/parameter[@name='keystore-password']/@value</td>
<td>The password for accessing the keystore.</td>
</tr>
<tr>
<td>/module/component[@id='keystore-manager-for-signature']/parameter[@name='key-alias']/@value</td>
<td>The alias of the private key for digital signature.</td>
</tr>
<tr>
<td>/module/component[@id='keystore-manager-for-signature']/parameter[@name='key-password']/@value</td>
<td>The password protecting the private key for digital signature.</td>
</tr>
<tr>
<td>/module/component[@id='keystore-manager-for-signature']/parameter[@name='keystore-type']/@value</td>
<td>The keystore format. It is either PKCS12 or JKS.</td>
</tr>
</tbody>
</table>

Location of keystore for S/MIME decryption (incoming messages)

```xml
<module id="ebms.main" name="Ebms Plugin" version="1.0">
  ...
  <component id="keystore-manager-for-decryption" name="Key Store Manager for Decryption (ebMS over SMTP)">
    <class>hk.hku.cecid.piazza.commons.security.KeyStoreManager</class>
    <parameter name="keystore-location" value="/home/hermes2/plugins/corvus-ebms/security/corvus.p12"/>
    <parameter name="keystore-password" value="password"/>
    <parameter name="key-alias" value="corvus"/>
    <parameter name="key-password" value="password"/>
    <parameter name="keystore-type" value="PKCS12"/>
    <parameter name="keystore-provider" value="org.bouncycastle.jce.provider.BouncyCastleProvider"/>
  </component>
  ...
</module>
```
<table>
<thead>
<tr>
<th>XPath</th>
<th>Expected information</th>
</tr>
</thead>
<tbody>
<tr>
<td>/module/ component[@id='keystore-manager-for-decryption']/</td>
<td>The path of the keystore for decrypting incoming messages with S/MIME encryption.</td>
</tr>
<tr>
<td>parameter[@name='keystore-location']/@value</td>
<td></td>
</tr>
<tr>
<td>/module/ component[@id='keystore-manager-for-decryption']/</td>
<td>The password for accessing the keystore</td>
</tr>
<tr>
<td>parameter[@name='keystore-password']/@value</td>
<td></td>
</tr>
<tr>
<td>/module/ component[@id='keystore-manager-for-decryption']/</td>
<td>The alias of the private key for the decryption.</td>
</tr>
<tr>
<td>parameter[@name='key-alias']/@value</td>
<td></td>
</tr>
<tr>
<td>/module/ component[@id='keystore-manager-for-decryption']/</td>
<td>The password protecting the private key for digital signatures.</td>
</tr>
<tr>
<td>parameter[@name='key-password']/@value</td>
<td></td>
</tr>
<tr>
<td>/module/ component[@id='keystore-manager-for-decryption']/</td>
<td>The keystore format. It is either PKCS12 or JKS.</td>
</tr>
<tr>
<td>parameter[@name='keystore-type']/@value</td>
<td></td>
</tr>
</tbody>
</table>

See also

- Developing Hermes Applications
- OASIS ebXML Message Service Specification 2.0
- MIME-based Secure Peer-to-Peer Business Data Interchange over the Internet Using HTTP AS2

Using Hermes API

Introduction

Hermes has implemented web services to communicate with external applications. The main advantages of using web services are reducing the coupling between external applications and Hermes, and to allow external applications to integrate with Hermes seamlessly using any programming languages that support sending SOAP Messages with Attachments or calling REST APIs. This article helps developers writing a client which talks to Hermes via web services based on SOAP or REST APIs on HTTP.

For more information on the installation and partnerships of Hermes, please refer to Installing Hermes and The First Step respectively.

To choose whether to use SOAP or REST APIs in your application, you may refer to Understanding SOAP and REST Basics and Differences for guidance.
Overview

Here is a brief summary about the communication architecture between Hermes and external applications. The core of Hermes can run on any J2EE compliant web server as a servlet. The core itself provides neither any web services or HTTP listeners, nor any functionality related to messaging. All features in Hermes are derived from the core using SPA (Simple Plugin Architecture).

One of the core SPAs, called Main Plugin (shown below in the core SPA layer), provides an HTTP context listener that accepts HTTP requests at the specified context path (extension point) for external invocation. The protocol-specific SPA ebMS and AS2 plugins (shown below in the external SPA layer) make use of this listener to provide all SOAP and REST web services.
In the default Hermes installation, each of ebMS 2.0 and AS2 plugins supports the following registered web services in Hermes:

3.7. Using Hermes API
Table 3.1: ebMS 2.0 Hermes API

<table>
<thead>
<tr>
<th>Functionality</th>
<th>REST(ebMS)¹</th>
<th>SOAP(ebMS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send message</td>
<td>POST:/corvus/api/message/send/ebms</td>
<td>/corvus/httpd/ebms/sender</td>
</tr>
<tr>
<td>List received message ID</td>
<td>GET:/corvus/api/message/receive/ebms</td>
<td>/corvus/httpd/ebms/receiver_list</td>
</tr>
<tr>
<td>Download received message payload</td>
<td>POST:/corvus/api/message/receive/ebms</td>
<td>/corvus/httpd/ebms/receiver</td>
</tr>
<tr>
<td>Get message status</td>
<td>GET:/corvus/api/message/send/ebms</td>
<td>/corvus/httpd/ebms/status</td>
</tr>
<tr>
<td>Reset message status</td>
<td>POST:/corvus/api/message/redownload/ebms</td>
<td>/corvus/httpd/ebms/permitdl</td>
</tr>
<tr>
<td>Query message with parameters</td>
<td>GET:/corvus/api/message/history/ebms</td>
<td>/corvus/httpd/ebms/msg_history</td>
</tr>
<tr>
<td>Add partnership</td>
<td>POST:/corvus/api/partnership/ebms</td>
<td>NIL</td>
</tr>
<tr>
<td>Delete partnership</td>
<td>DELETE /corvus/api/partnership/ebms/{pid}</td>
<td>NIL</td>
</tr>
<tr>
<td>Update partnership</td>
<td>POST:/corvus/api/partnership/ebms</td>
<td>NIL</td>
</tr>
<tr>
<td>Get partnerships</td>
<td>GET:/corvus/api/partnership/ebms</td>
<td>NIL</td>
</tr>
</tbody>
</table>

Note:

- To make an REST API request, the simplest way is to use curl as a command line REST client, or Postman as a GUI based client.
- To enhance the security of Hermes REST API, HTTP Basic Authentication is enabled for the Rest API. Please place the base64 encoded username:password in the HTTP Header as below: HTTP Header:Authorization = basic base64encode[username:pwd] where the username and pwd are defined in tomcat-users.xml mentioned in Tomcat installation.

Table 3.2: AS2 Hermes API

<table>
<thead>
<tr>
<th>Functionality</th>
<th>REST(AS2)¹</th>
<th>SOAP(AS2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send Message</td>
<td>POST:/corvus/api/message/send/as2</td>
<td>/corvus/httpd/as2/sender</td>
</tr>
<tr>
<td>List received message ID</td>
<td>GET:/corvus/api/message/receive/as2</td>
<td>/corvus/httpd/as2/receiver_list</td>
</tr>
<tr>
<td>Download received message payload</td>
<td>POST:/corvus/api/message/receive/as2</td>
<td>/corvus/httpd/as2/receiver</td>
</tr>
<tr>
<td>Get message status</td>
<td>GET:/corvus/api/message/send/as2</td>
<td>/corvus/httpd/as2/status</td>
</tr>
<tr>
<td>Query message with parameters</td>
<td>GET:/corvus/api/message/history/as2</td>
<td>/corvus/httpd/as2/msg_history</td>
</tr>
<tr>
<td>Add partnership</td>
<td>POST:/corvus/api/partnership/as2</td>
<td>NIL</td>
</tr>
<tr>
<td>Delete partnership</td>
<td>DELETE /corvus/api/partnership/as2/{pid}</td>
<td>NIL</td>
</tr>
<tr>
<td>Update partnership</td>
<td>POST:/corvus/api/partnership/as2</td>
<td>NIL</td>
</tr>
<tr>
<td>Get partnerships</td>
<td>GET:/corvus/api/partnership/as2</td>
<td>NIL</td>
</tr>
</tbody>
</table>

Note:

- ebMS 2.0 Web Service

Send message

This is a web service interface for external parties to request Hermes to send an ebMS message to another Hermes or an ebMS compliant messaging gateway. The service provides a message identifier to the sender for future reference. This is the main channel for external applications to deliver ebMS messages using Hermes.
SOAP

Service endpoint: http://<HOST>:<PORT>/corvus/httpd/ebms/sender

Request message

Instead composing the entire ebMS messages, the sender simply needs to send a web service request to Hermes with key parameters including CPA_ID, Service and Action. These 3 key parameters identify the sending partnership in Hermes that will be used to configure the ebMS message.

The elements in the SOAP body use the namespace URI http://service.ebms.edi.cecid.hku.hk/.

A sample SOAP request is shown below.

```xml
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
    <tns:cpaId xmlns:tns="http://service.ebms.edi.cecid.hku.hk/">[CPA_Id]</tns:cpaId>
    <tns:fromPartyType xmlns:tns="http://service.ebms.edi.cecid.hku.hk/">[From_Party_Type]</tns:fromPartyType>
    <tns:toPartyId xmlns:tns="http://service.ebms.edi.cecid.hku.hk/">[To_Party_Id]</tns:toPartyId>
    <tns:toPartyType xmlns:tns="http://service.ebms.edi.cecid.hku.hk/">[To_Party_Type]</tns:toPartyType>
    <tns:refToMessageId xmlns:tns="http://service.ebms.edi.cecid.hku.hk/">[Reference_Message_Id]</tns:refToMessageId>
    <tns:serviceType xmlns:tns="http://service.ebms.edi.cecid.hku.hk/">[Service_Type]</tns:serviceType>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>

<!-- Attached payloads... -->
```

The descriptions of the elements in the SOAP body are as follows:
### Hermes Documentation, Release 2.2

**Element**  | **Mandatory** | **Description** |
--- | --- | --- |
<cpaId>, <service>, <action> | Yes | They are the CPA Id, Service and Action elements in the ebMS messages sent by Hermes. These three fields are used to identify the partnership used to send and receive the ebMS messages by the sending and receiving parties respectively. **These are required to identify a registered partnership in Hermes.** |
<convId> | Yes | This corresponds to the conversation id element in the ebMS messages sent by Hermes. |
<fromPartyId> | Yes | This identifies the sender. [ebMS v2.0 3.1.1] It corresponds to the PartyId element in From element of ebMS messages sent by Hermes. |
<fromPartyType> | Yes | This identifies the domain of the sender. It corresponds to the type attribute of PartyId in the From element of ebMS messages sent by Hermes. |
<toPartyId> | Yes | This identifies the receiver. [ebMS v2.0 3.1.1] It corresponds to the PartyId element in To element of ebMS messages sent by Hermes. |
<toPartyType> | Yes | This identifies the domain of the receiver. It corresponds to the type attribute of PartyId in the From element of ebMS messages sent by Hermes. |
<refToMessageId> | No | This corresponds to the RefToMessageId of ebMS messages sent by Hermes. |
<serviceType> | No | A type identifier for the ebXML service defined in the partnership. |

### Response message

The elements inside the SOAP body uses namespace URI [http://service.ebms.edi.cecidi.hku.hk/](http://service.ebms.edi.cecidi.hku.hk/).

A sample SOAP response is shown below:

```xml
  xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/encoding/">
  <SOAP-ENV:Header/>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

In the SOAP request message, the `<message_id>` element is the *message* identifier assigned by Hermes in
the sending party. The sending application can use it for later reference and status tracking with Get message status web service.

REST

Request message

```
$ curl -X POST --data '{"partnership_id":"<partnership_id>", "from_party_id":"<from>", "to_party_id":"<to>", "conversation_id":"<conv>", "payload":"<payload>"}' http://<HOST>:<PORT>/corvus/api/message/send/ebms
```

Response message

```
{
  "id": "<message_id>"
}
```

For the detailed specification of this REST API, please refer to HERMES RESTful OpenAPI Specification.

List received message ID

This web service is used by the application of the receiving party to retrieve message identifiers of received and processed ebMS messages that have not been downloaded. These message identifiers will be used to retrieve message payloads with Download received message payload web service.

SOAP

Service endpoint: http://<HOST>:<PORT>/corvus/httpd/ebms/receiver_list

Request message

The elements in the SOAP body use the namespace URI http://service.ebms.edi.cecid.hku.hk/.

A sample SOAP request is shown below:

```xml
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
    <tns:cpaId xmlns:tns="http://service.ebms.edi.cecid.hku.hk/">[CPA_Id]</tns:cpaId>
    <tns:fromPartyType xmlns:tns="http://service.ebms.edi.cecid.hku.hk/">[From_Party_Type]</tns:fromPartyType>
    <tns:toPartyId xmlns:tns="http://service.ebms.edi.cecid.hku.hk/">[To_Party_Id]</tns:toPartyId>
    <tns:toPartyType xmlns:tns="http://service.ebms.edi.cecid.hku.hk/">[To_Party_Type]</tns:toPartyType>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```
The descriptions of the elements in the SOAP body are as follows:

<table>
<thead>
<tr>
<th>Element</th>
<th>Mandatory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;cpaId&gt;,</td>
<td>Yes</td>
<td>The CPA Id, Service and Action elements in ebMS messages sent by Hermes. These fields identify the partnership used to send ebMS messages. These are required to query the list of available messages.</td>
</tr>
<tr>
<td>&lt;convId&gt;</td>
<td>No</td>
<td>Only the identifiers of messages with a matching Conversation Id will be retrieved.</td>
</tr>
<tr>
<td>&lt;fromPartyId&gt;</td>
<td>No</td>
<td>Only the identifiers of messages with a matching From Party Id will be retrieved.</td>
</tr>
<tr>
<td>&lt;fromPartyType&gt;</td>
<td>No</td>
<td>Only the identifiers of messages with a matching From Party Type will be retrieved.</td>
</tr>
<tr>
<td>&lt;toPartyId&gt;</td>
<td>No</td>
<td>Only the identifiers of messages with a matching To Party Id will be retrieved.</td>
</tr>
<tr>
<td>&lt;toPartyType&gt;</td>
<td>No</td>
<td>Only the identifiers of messages with a matching To Party Type will be retrieved.</td>
</tr>
<tr>
<td>&lt;numOfMessages&gt;</td>
<td>No</td>
<td>The maximum number of message identifiers retrieved by this request.</td>
</tr>
</tbody>
</table>

Response message

The elements inside the SOAP body use the namespace URI http://service.ebms.edi.cecid.hku.hk/.

A sample SOAP response is shown below:

```xml
  xmlns:messageIds="http://service.ebms.edi.cecid.hku.hk/"
  <messageIds>
    <messageId>[downloadable_message_id]</messageId>
    <messageId>[downloadable_message_id]</messageId>
    <messageId>[downloadable_message_id]</messageId>
  </messageIds>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Each element in the messageIds represents the message identifier of an ebMS message received by Hermes.

Please note that a message is considered to be downloaded only when the message body has been downloaded by Download received message payload SOAP web service. If your application never calls Download received message payload SOAP web service to download the messages, the same set of message identifiers will always be retrieved.

REST

Request message
REST response message

```
{
    "message_ids": [
        {
            "id": "<message_id>",
            "timestamp": 1234567890,
            "status": "<status>"
        }
    ]
}
```

Please note that a message is considered to be downloaded when the message id is returned by this REST API call.

For the detailed specification of this REST API, please refer to HERMES RESTful OpenAPI Specification.

### Download received message payload

This web service is used by the application of the receiving party to retrieve message payloads of received ebMS messages. After the message payloads have been downloaded, the message will be marked as received, and its message identifier will no longer be retrieved by *List received message ID* web service.

#### SOAP

**Service endpoint:** http://<HOST>:<PORT>/corvus/httpd/ebms/receiver

**Request message**

The elements in the SOAP body use the namespace URI http://service.ebms.edi.cecid.hku.hk/.

A sample SOAP request is shown below:

```
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

The `<messageId>` element contains a message identifier which obtained from *List received message ID* web service.

**Response message**

The element inside the SOAP body is using namespace URI http://service.ebms.edi.cecid.hku.hk/.

A sample SOAP response is shown below:
If a payload is associated with the message identifier, the <hasMessage> element will have the value true. If the received ebMS message has payloads, the response message will have one or more SOAP attachments. Each SOAP attachment has a content type, which is set by the sending application.

Please note that a message is considered to be downloaded when the message is returned by this SOAP request.

**REST**

**Request message**

```bash
```

**Response message**

```json
{
    "id": "<message_id>",
    "cpa_id": "<cpa>",
    "service": "<service>",
    "action": "<action>",
    "from_party_id": "<from>",
    "to_party_id": "<to>",
    "conversation_id": "<conv>",
    "timestamp": 1234567890,
    "status": "<status>",
    "payloads": [
        "payload": "<content>"
    ]
}
```

For the detailed specification of this REST API, please refer to HERMES RESTful OpenAPI Specification.

**Get message status**

This web service is used by the application of the sending party to retrieve the status of a delivered ebMS message. The message status is a two-character code indicating the progress of an ebMS message. It provides a tracking service to monitor ebMS messages requested from Hermes.

**SOAP**

Service endpoint: http://<HOST>:<PORT>/corvus/httpd/ebms/status
Request message

The elements in the SOAP body use the namespace URI http://service.ebms.edi.cecid.hku.hk/.

A sample SOAP request is shown below:

```xml
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
    </SOAP-ENV:Body>
  </SOAP-ENV:Envelope>
```

The `<messageId>` element contains a message identifier obtained from Send message web service response or List received message ID web service.

Response message

The element inside the SOAP body is using namespace URI http://service.ebms.edi.cecid.hku.hk/.

A sample SOAP response is shown below:

```xml
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
    <messageInfo xmlns="http://service.ebms.edi.cecid.hku.hk/">
      <status>[status]</status>
      <statusDescription>[statusDescription]</statusDescription>
      <ackMessageId>[ackMessageId]</ackMessageId>
      <ackStatus>[ackStatus]</ackStatus>
      <ackStatusDescription>[ackStatusDescription]</ackStatusDescription>
    </messageInfo>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

The descriptions of the elements in the SOAP body are as follows:

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;status&gt;</td>
<td>The current status of the ebMS message.</td>
</tr>
<tr>
<td>&lt;statusDescription&gt;</td>
<td>A text description of the current status.</td>
</tr>
<tr>
<td>&lt;ackMessageId&gt;</td>
<td>The message identifier of the associated acknowledgment (if any).</td>
</tr>
<tr>
<td>&lt;ackStatus&gt;</td>
<td>The current status of the associated acknowledgment (if any).</td>
</tr>
<tr>
<td>&lt;ackStatusDescription&gt;</td>
<td>A text description of the associated acknowledgment (if any).</td>
</tr>
</tbody>
</table>

REST

Request message

```
```

Response message

```json
{
   "message_id": "<message_id>",
   "status": "<status>"
}
```

For the detailed specification of this REST API, please refer to HERMES RESTful OpenAPI Specification.
Reset message status

This web service is used by the application of the receiving party to reset the status of a downloaded ebMS message from DL (delivered) to PS (processed), so that it can be redownloaded again.

SOAP

Service endpoint: http://<HOST>:<PORT>/corvus/httpd/ebms/permitdl

Request message

The elements in the SOAP body use the namespace URI http://service.ebms.edi.cecid.hku.hk/.

A sample SOAP request is shown below:

```xml
   xmlns:tns="http://service.ebms.edi.cecid.hku.hk/">
   <tns:messageId>
       [The_message_id_you_want_to_redownload]
   </tns:messageId>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

The <messageId> element contains a message identifier obtained from the ebMS sender web service response or the ebMS receiver list web service.

Response message

The element inside the SOAP body is using namespace URI http://service.ebms.edi.cecid.hku.hk/.

A sample SOAP response is shown below:

```xml
   xmlns:message="http://service.ebms.edi.cecid.hku.hk/">
   <message_id>
       [newly_created_message_id]
   </message_id>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

In the SOAP request message, the <message_id> element is the message identifier where they are the same if reset status successfully.

REST

Request message

```bash
```

Response message

```json
{
    "id": "<message_id>
}
```

For the detailed specification of this REST API, please refer to HERMES RESTful OpenAPI Specification.
Query message with parameters

This web service is used by the application of the sending or receiving party to query messages according to specific parameters.

SOAP

Service endpoint: http://<HOST>:<PORT>/corvus/httpd/ebms/msg_history

Request message

The elements in the SOAP body use the namespace URI http://service.ebms.edi.cecid.hku.hk/.

A sample SOAP request is shown below:

```xml
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
    <tns:messageBox xmlns:tns="http://service.ebms.edi.cecid.hku.hk/">[Message_Box]
      ...
    </tns:messageBox>
      ...
    </tns:status>
    <tns:messageId xmlns:tns="http://service.ebms.edi.cecid.hku.hk/">[Message_Id]
      ...
    </tns:messageId>
    <tns:conversationId xmlns:tns="http://service.ebms.edi.cecid.hku.hk/">[Conversation_Id]
      ...
    </tns:conversationId>
    <tns:cpaId xmlns:tns="http://service.ebms.edi.cecid.hku.hk/">[CPA_Id]</tns:cpaId>
    <tns:service xmlns:tns="http://service.ebms.edi.cecid.hku.hk/">[Defined_Service_with_trading_party]
      ...
    </tns:service>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```
Response message

The element `<messageList>` inside the SOAP body uses the namespace URI `http://service.ebms.edi.cecid.hku.hk/`.

A sample SOAP response is shown below:

```xml
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
    <messageList xmlns="http://service.ebms.edi.cecid.hku.hk/">
      <messageElement>
        <messageId> messageId </messageId>
        <messageBox> message_box_containing_this_message </messageBox>
      </messageElement>
      <messageElement>
        <messageId> messageId </messageId>
        <messageBox> message_box_containing_this_message </messageBox>
      </messageElement>
      ...<messageElement>
      ...<messageElement>
    </messageList>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

The descriptions of the elements in the SOAP body are as follows:

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;messageList&gt;</code></td>
<td>A list of retrieved message elements (if any).</td>
</tr>
<tr>
<td><code>&lt;messageElement&gt;</code></td>
<td>A complex element containing <code>messageId</code> and <code>messageBox</code> values of a retrieved message.</td>
</tr>
<tr>
<td><code>&lt;messageId&gt;</code></td>
<td>The message identifier of a retrieved message.</td>
</tr>
<tr>
<td><code>&lt;messageBox&gt;</code></td>
<td>The message box of a retrieved message.</td>
</tr>
</tbody>
</table>

REST

Request message

```bash
```

Response message

```json
{
    "message_ids": [
        {
            "id": "<id>",
            "cpa_id": "<cpa_id>",
            "service": "<service>",
            "action": "<action>",
            "conversation_id": "<conversation_id>",
            "message_box": "<message_box>",
            "timestamp": "<timestamp>",
            "status": "<status>"
        }
    ]
}
```
For the detailed specification of this REST API, please refer to HERMES RESTful OpenAPI Specification.

**Add partnership**

The ebMS Add Partnership web service is used by the application of the sending and receiving party to create partnership. For further details about ebMS partnership, please refer to *Setting Up ebMS 2.0 Partnerships*.

**REST**

**Request message**

```bash
```

**Response message**

```json
{
  "id": "<partnership_id>
}
```

**Delete partnership**

The ebMS delete Partnership web service is used by the application of the sending and receiving party to delete partnership.

**REST**

**Request message**

```bash
$ curl -X DELETE http://<HOST>:<PORT>/corvus/api/partnership/ebms/<partnership_id>
```

**Response message**

```json
{
  "id": "<partnership_id>",
  "success": true
}
```

**Update partnership**

The ebMS update Partnership web service is used by the application of the sending and receiving party to update partnership. For further details about ebMS partnership, please refer to *Setting Up ebMS 2.0 Partnerships*. 
REST

Request message

```
$ curl -X POST --data '{"id":"<partnership_id>"","cpa_id":"<cpa>"","service":"<service>"","action":"<action>","transport-endpoint":"http://<RECEIVER_HOST>:<RECEIVER_PORT>/corvus/httpd/ebms/inbound"}'
http://<SENDER_HOST>:<SENDER_PORT>/corvus/api/partnership/ebms
```

Response message

```
{
  "id": "<partnership_id>"
}
```

Get partnerships

The ebMS get Partnership web service is used by the application of the sending and receiving party to get all partnership details.

REST

Request message

```
$ curl -X GET http://<HOST>:<PORT>/corvus/api/partnership/ebms
```

Response message

```
{
  "partnerships": [
    {
      "id": "<partnership_id>",
      "cpa_id": "<cpa>",
      "service": "<service>",
      "action": "<action>",
      "disabled": false,
      "ack_requested": null,
      "signed_ack_requested": null,
      "duplicate_elimination": null,
      "message_order": null,
      "retries": 0,
      "retry_interval": 0,
      "sign_requested": false,
      "sign_certificate": null
    }
  ]
}
```
AS2 Web Service

Send Message

This web service is used by the application of the sending party to request Hermes to send an AS2 message to another Hermes or a compatible messaging gateway. The service returns a message identifier to the application for future reference.

SOAP

Service endpoint: http://<HOST>[:<PORT>/corvus/httpd/as2/sender

Request message

The elements in the SOAP body use the namespace URI http://service.as2.edi.cecid.hku.hk/.

A sample SOAP request is shown below:

```xml
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
    <tns:as2_from xmlns:tns="http://service.ebms.edi.cecid.hku.hk/">[as2_from]</tns:as2_from>
    <tns:as2_to xmlns:tns="http://service.ebms.edi.cecid.hku.hk/">[as2_to]</tns:as2_to>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
<!-- Attached payloads... -->
```

The descriptions of the elements in the SOAP body are as follows:
### Hermes Documentation, Release 2.2

<table>
<thead>
<tr>
<th>Element</th>
<th>Mandatory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;as2_from&gt;,&lt;as2_to&gt;</code></td>
<td>Yes</td>
<td>The values of the From and To fields in AS2 messages sent through the partnership by Hermes. These fields are used to identify the sending partnership. <strong>These are required to identify the message destination.</strong></td>
</tr>
</tbody>
</table>
| `<type>`            | Yes       | A three-character code indicating the content type of the sent payload. The available codes are:  
  - `edi`, for the content type `application/EDIFACT`.  
  - `x12`, for the content type `application/EDI-X12`.  
  - `eco`, for the content type `application/edi-consent`.  
  - `xml`, for the content type `application/XML`.  
  - `bin`, for the content type `application/octet-stream`.  
  For other values, Hermes will assume the content type of the payload is `application/deflate`, which means that the payload is compressed by Zip. |

**Response message**

The elements inside the SOAP body use the namespace URI `http://service.as2.edi.cecid.hku.hk/`. A sample SOAP response is shown below:

```xml
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
    <message_id xmlns="http://service.as2.edi.cecid.hku.hk/">[newly_created_message_Id]</message_id>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

The `<message_id>` element is the identifier of the sent message that can be used for later reference and status tracking with `Get message status` web service.

**REST**

**Request message**

```
$ curl -X POST --data '{ "as2_from": <as2_from>, "as2_to": <as2_to>, "type": <type>, "payload": <payload>}' http://<HOST>:<PORT>/corvus/api/message/send/as2
```

**Response message**

---

Note: To try the REST API, the simplest way is to use curl as a command line REST client, or Postman as a GUI based client is a useful tool too.

For the detailed specification of this REST API, please refer to HERMES RESTful OpenAPI Specification.

### List received message ID

This web service is used by the application of the receiving party to retrieve message identifiers of received AS2 messages which have not been downloaded by the application. The message identifiers will be used to retrieve message payloads using *Download received message payload* web service.

**SOAP**

Service endpoint: http://<HERMES_HOST>:<HERMES_PORT>/corvus/httpd/as2/receiver_list

**Request message**

The elements in the SOAP body use the namespace URI http://service.as2.edi.cecid.hku.hk/.

A sample SOAP request is shown below:

```xml
    <SOAP-ENV:Header/>
    <SOAP-ENV:Body>
        <tns:as2_from xmlns:tns="http://service.ebms.edi.cecid.hku.hk/">[as2_from]</tns:as2_from>
        <tns:as2_to xmlns:tns="http://service.ebms.edi.cecid.hku.hk/">[as2_to]</tns:as2_to>
    </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

The descriptions of the elements in the SOAP body are as follows:

<table>
<thead>
<tr>
<th>Element</th>
<th>Mandatory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;as2_from&gt;, &lt;as2_to&gt;, &lt;as2_to&gt;</td>
<td>Yes</td>
<td>The values of the From and To fields in AS2 messages sent through the partnership by Hermes. These fields are used to identify the sending partnership. These are required to query messages associated with the specified partnership.</td>
</tr>
<tr>
<td>&lt;numOfMessages&gt;</td>
<td>No</td>
<td>The maximum number of message identifiers retrieved by this request.</td>
</tr>
</tbody>
</table>

**Response message**

The elements inside the SOAP body use the namespace URI http://service.as2.edi.cecid.hku.hk/.
A sample SOAP response is shown below:

```
  <SOAP-ENV:Body>
    <messageIds xmlns="http://service.as2.edi.cecid.hku.hk/">
      <messageId>[downloadable_message_id]</messageId>
      <messageId>[downloadable_message_id]</messageId>
    </messageIds>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Each `<downloadable_message_id>` element in the response message represents the identifier of an AS2 message received by Hermes.

Please note that a message is considered to be downloaded only when the message body has been downloaded by `Download received message payload` SOAP web service. If your application never calls `Download received message payload` SOAP web service to download the messages, the same set of message identifiers will always be retrieved.

**REST**

**Request message**

```
$ curl -X GET http://<HOST>:<PORT>/corvus/api/message/receive/as2?partnership_id=<partnership_id>
```

**REST response message**

```
{
  "message_id": [
    {
      "id": "<message_id>",
      "timestamp": 1234567890,
      "status": "<status>"
    }
  ]
}
```

Please note that a message is considered to be downloaded when the message id is returned by this REST API call.

For the detailed specification of this REST API, please refer to HERMES RESTful OpenAPI Specification.

**Download received message payload**

This web service is used by the application of the receiving party to retrieve the message payloads of received AS2 messages. After the payloads have been downloaded, the message will be marked as received, and the message identifier of the message will no longer be retrieved by the AS2 receiver list service.
SOAP


Request message

The elements in the SOAP body use the namespace URI http://service.as2.edi.cecid.hku.hk/.

A sample SOAP request is shown below:

```xml
    xmlns:tns="http://service.as2.edi.cecid.hku.hk/"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <SOAP-ENV:Header/>
    <SOAP-ENV:Body>
        <tns:messageId [id_of_message_to_download]/>
    </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Response message

The element inside the SOAP body is using namespace URI http://service.as2.edi.cecid.hku.hk/.

A sample SOAP response is shown below:

```xml
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <SOAP-ENV:Header/>
    <SOAP-ENV:Body>
        <hasMessage xmlns="http://service.as2.edi.cecid.hku.hk/"[true_if_payload_in_message]/>
    </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

If a payload is associated with the message identifier, then <hasMessage> will have the value true. If the received AS2 message has payloads, the response message will have one or more SOAP attachments. Each SOAP attachment has a content type, which is set by the sender application.

Please note that a message is considered to be downloaded when the message is returned by this SOAP request.

REST

Request message

$ curl -X POST --data '
"id": "<message_id"
http://<HOST>:<PORT>/corvus/api/message/receive/as2

Response message

```json
{
    "id": "<id>",
    "as2_from": "<as2_from>",
    "as2_to": "<as2_to>",
    "timestamp": 1234567890,
    "status": "<status>",
    "payloads": [
        { "payload": "<payload>" }
    ]
```
For the detailed specification of this REST API, please refer to HERMES RESTful OpenAPI Specification.

**Get message status**

This web service is used by the application of the sending party to retrieve the message status of a sent or received AS2 message respectively.

**SOAP**


**Request message**

The elements in the SOAP body use the namespace URI http://service.as2.edi.cecid.hku.hk/.

A sample SOAP request is shown below:

```xml
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

**Response message**

The element `<messageInfo>` inside the SOAP body is using the namespace URI http://service.as2.edi.cecid.hku.hk/.

A sample SOAP response is shown below:

```xml
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
    <messageInfo xmlns="http://service.as2.edi.cecid.hku.hk/">
      <status>[status]</status>
      <statusDescription>[statusDescription]</statusDescription>
      <mdnMessageId>[mdnMessageId]</mdnMessageId>
      <mdnStatus>[mdnStatus]</mdnStatus>
      <mdnStatusDescription>[mdnStatusDescription]</mdnStatusDescription>
    </messageInfo>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

The descriptions of the elements in the SOAP body are as follows:

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;status&gt;</code></td>
<td>The current status of the AS2 message.</td>
</tr>
<tr>
<td><code>&lt;statusDescription&gt;</code></td>
<td>A text description of the current status.</td>
</tr>
<tr>
<td><code>&lt;mdnMessageId&gt;</code></td>
<td>The message identifier of the associated receipt (if any).</td>
</tr>
<tr>
<td><code>&lt;mdnStatus&gt;</code></td>
<td>The current status of the associated receipt.</td>
</tr>
<tr>
<td><code>&lt;mdnStatusDescription&gt;</code></td>
<td>A text description of the associated receipt.</td>
</tr>
</tbody>
</table>
**REST**

**Request message**

```
$ curl -X GET http://<HOST>:<PORT>/corvus/api/message/send/as2?id=<message_id>
```

**Response message**

```
{
    "message_id": "<message_id>",
    "status": "<status>"
}
```

For the detailed specification of this REST API, please refer to HERMES RESTful OpenAPI Specification.

**Query message with parameters**

This web service is used by the application of the sending or receiving party to query messages according to specific parameters.

**SOAP**

**Service endpoint:** http://<HOST>:<PORT>/corvus/httpd/as2/msg_history

**Request message**

The elements in the SOAP body use the namespace URI http://service.as2.edi.cecid.hku.hk/.

A sample SOAP request is shown below:
Response message

The element `<messageList>` in the SOAP body uses the namespace URI http://service.as2.edi.cecid.hku.hk/.

A sample SOAP response is shown below:

```xml
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
    <messageList xmlns="http://service.as2.edi.cecid.hku.hk/">
      <messageElement>
        <messageId>[message_id]</messageId>
        <messageBox>[message_box_containing_this_message]</messageBox>
      </messageElement>
      <messageElement>
        <messageId>[message_id]</messageId>
        <messageBox>[message_box_containing_this_message]</messageBox>
      </messageElement>
      <messageElement>...</messageElement>
      <messageElement>...</messageElement>
    </messageList>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

The descriptions of the elements in the SOAP body are as follows:

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;messageList&gt;</code></td>
<td>The list of retrieved message elements.</td>
</tr>
<tr>
<td><code>&lt;messageElement&gt;</code></td>
<td>A complex element containing the <code>messageId</code> and <code>messageBox</code> values of the retrieved message.</td>
</tr>
<tr>
<td><code>&lt;messageId&gt;</code></td>
<td>The message identifier of the retrieved message.</td>
</tr>
<tr>
<td><code>&lt;messageBox&gt;</code></td>
<td>The message box of the retrieved message.</td>
</tr>
</tbody>
</table>

**REST**

Request message

```
$ curl -X GET http://<HOST>:<PORT>/corvus/api/message/history/as2?message_id=<message_id>&message_box=<message_box>&as2_from=<as2_from>&as2_to=<as2_to>&status=<status>&limit=<limit>
```
Response message

```
{
  "message_ids": [
    {
      "id": "<message_Id>",
      "as2_from": "<as2_from>",
      "as2_to": "<as2_to>",
      "message_box": "<message_box>",
      "timestamp": 1234567890,
      "status": "<status>"
    }
  ]
}
```

For the detailed specification of this REST API, please refer to HERMES RESTful OpenAPI Specification.

### Add partnership

The AS2 Add Partnership web service is used by the application of the sending and receiving party to create partnership. For further details about AS2 partnership, please refer to Setting Up AS2 Partnerships.

**REST**

#### Request message

```bash
$ curl -X POST --data '{"id":"<partnership_id>", "as2_from":"<as2_from>", "as2_to":"<as2_to>", "disabled":true/false, "sync_reply": "string", "subject": "subject", "recipient_address": "recipient_address", "hostname_verified": true, "receipt_address": "receipt_address", "receipt_requested": true, "outbound_sign_required": true, "outbound_encrypt_required": true, "outbound_compress_required": true, "receipt_sign_required": true, "inbound_sign_required": true, "inbound_encrypt_required": true, "algorithm": "sha1/md5", "encrypt_algorithm": "3des/rc2", "mic_algorithm": "sha1/md5", "encrypt_certificate": "cert_path", "verify_certificate": "cert_path"}'
```

http://<SENDER_HOST>:<SENDER_PORT>/corvus/api/partnership/as2

#### Response message

```
{
  "id": "<partnership_id>"
}
```

### Delete partnership

The AS2 delete Partnership web service is used by the application of the sending and receiving party to delete partnership.

**REST**

#### Request message
### Update partnership

The ebMS update Partnership web service is used by the application of the sending and receiving party to update partnership. For further details about AS2 partnership, please refer to [Setting Up AS2 Partnerships](#).

#### REST

**Request message**

```bash
$ curl -X POST --data '{"id": "<partnership_id>", "as2_from": "<as2_from>", "as2_to": "<as2_to>", "disabled": "<true/false>", "sync_reply": "<string>", "subject": "<subject>", "recipient_address": "<recipient_address>", "hostname_verified": "<Yes/No>", "receipt_address": "<receipt_address>", "receipt_requested": "<Yes/No>", "outbound_sign_required": "<Yes/No>", "outbound_encrypt_required": "<Yes/No>", "outbound_compress_required": "<Yes/No>", "receipt_sign_required": "<Yes/No>", "inbound_sign_required": "<Yes/No>", "inbound_encrypt_required": "<Yes/No>", "retries": "<no_of_retries>", "retry_interval": "<retry_interval>", "sign_algorithm": "<sha1/md5>", "encrypt_algorithm": "<3des/rc2>", "mic_algorithm": "<sha1/md5>", "outbound_sign_required": "<Yes/No>", "encrypt_certificate": "<cert_path>", "verify_certificate": "<cert_path>"}' http://<SENDER_HOST>:<SENDER_PORT>/corvus/api/partnership/as2
```

**Response message**

```json
{
  "id": "<partnership_id>",
}
```

### Get partnerships

The AS2 get Partnership web service is used by the application of the sending and receiving party to get all partnership details.

#### REST

**Request message**

```bash
$ curl -X GET http://<HOST>:<PORT>/corvus/api/partnership/as2
```

**Response message**

```json
{
  "partnerships": [ ]
}
```
"id": "<partnership_id>",
"as2_from": "<as2_from>",
"as2_to": "<as2_to>",
"disabled": true,
"sync_reply": "<sync_reply>",
"subject": "<subject>",
"recipient_address": "<recipient_address>",
"hostname_verified": "<yes_or_no>",
"receipt_address": "<receipt_address>",
"receipt_requested": "<yes_or_no>",
"outbound_sign_required": "<yes_or_no>",
"outbound_encrypt_required": "<yes_or_no>",
"outbound_compress_required": "<yes_or_no>",
"receipt_sign_required": "<yes_or_no>",
"inbound_sign_required": "<yes_or_no>",
"inbound_encrypt_required": "<yes_or_no>",
"retries": 2,
"retry_interval": 10,
"sign_algorithm": "<sha1_or_md5>",
"encrypt_algorithm": "<3des_or_rc2>",
"mic_algorithm": "<sha1_or_md5>",
"encrypt_certificate": "<cert_path>",
"verify_certificate": "<cert_path>"
}

Note:

- If error occurs when processing REST API request, it will return an error JSON response.

```
{
    "code": "<error code>",
    "message": "<error description>"
}
```

Table 3.3: Error code and message

<table>
<thead>
<tr>
<th>Error code</th>
<th>Error Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>10000</td>
<td>ERROR_UNKNOWN</td>
</tr>
<tr>
<td>10001</td>
<td>ERROR_MISSING_REQUIRED_PARAMETER</td>
</tr>
<tr>
<td>10002</td>
<td>ERROR_PROTOCOL_UNSUPPORTED</td>
</tr>
<tr>
<td>10003</td>
<td>ERROR_READING_DATABASE</td>
</tr>
<tr>
<td>10004</td>
<td>ERROR_WRITING_DATABASE</td>
</tr>
<tr>
<td>10005</td>
<td>ERROR_READING_REQUEST</td>
</tr>
<tr>
<td>10006</td>
<td>ERROR_PARSING_REQUEST</td>
</tr>
<tr>
<td>10007</td>
<td>ERROR_RECORD_ALREADY_EXIST</td>
</tr>
<tr>
<td>10008</td>
<td>ERROR_DATA_NOT_FOUND</td>
</tr>
<tr>
<td>10009</td>
<td>ERROR_WRITING_MESSAGE</td>
</tr>
<tr>
<td>10010</td>
<td>ERROR_SENDING_MESSAGE</td>
</tr>
<tr>
<td>10011</td>
<td>ERROR_EXTRACTING_PAYLOAD_FROM_MESSAGE</td>
</tr>
<tr>
<td>10012</td>
<td>ERRORUNKNOWN_ACTION</td>
</tr>
</tbody>
</table>

3.9. AS2 Web Service
See also

- *The First Step*
- *Setting Up ebMS 2.0 Partnerships*
- *Setting Up AS2 Partnerships*
- *HERMES RESTful OpenAPI Specification*

Using Sample Clients

These sample Java clients demonstrate Hermes messaging flow. They provide a set of sample code for writing web service client applications connecting to Hermes.

Maintaining partnerships

A partnership must be registered on Hermes to send messages since partnerships contain information about your trading partner. A separate partnership is required to receive messages.

If you want to know more about partnership, please refer to the section *What is an ebMS 2.0 partnership?* and *What is an AS2 partnership?*

Let’s take a look at the program parameters.

<table>
<thead>
<tr>
<th>Command</th>
<th>partnership-xml</th>
<th>config-xml</th>
<th>log-path</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>as2-partnership</strong></td>
<td>partnership-xml</td>
<td>config-xml</td>
<td>log-path</td>
</tr>
<tr>
<td>partnership-xml</td>
<td>The filepath of the partnership configuration file. Default is <code>&lt;HERMES2_HOME&gt;/config/as2-partnership.xml</code>.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>config-xml</td>
<td>The filepath of the message configuration file. Default is <code>&lt;HERMES2_HOME&gt;/config/as2-partnership/as2-request.xml</code>.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>log-path</td>
<td>The filepath of the logger to log query result or error. Default is <code>&lt;HERMES2_HOME&gt;/logs/as2-partnership.log</code>.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command</th>
<th>partnership-xml</th>
<th>config-xml</th>
<th>log-path</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ebms-partnership</strong></td>
<td>partnership-xml</td>
<td>config-xml</td>
<td>log-path</td>
</tr>
<tr>
<td>partnership-xml</td>
<td>The filepath of the partnership configuration file. Default is <code>&lt;HERMES2_HOME&gt;/config/ebms-partnership.xml</code>.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>config-xml</td>
<td>The filepath of the message configuration file. Default is <code>&lt;HERMES2_HOME&gt;/config/ebms-partnership/ebms-request.xml</code>.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>log-path</td>
<td>The filepath of the logger to log query result or error. Default is <code>&lt;HERMES2_HOME&gt;/logs/ebms-partnership.log</code>.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

config-xml

Here is sample content of the config-xml files. These files are named *ebms-request.xml* and *as2-request.xml*, and placed under `<HERMES2_HOME>/config/ebms-partnership` and `<HERMES2_HOME>/config/as2-partnership` respectively.
Configuration file for ebMS:

```xml
<?xml version='1.0' encoding='UTF-8'?>
<ebms-admin-request>
  <config>
    <!-- The user name for logging H2O administrative area -->
    <username>corvus</username>
    <!-- The password for logging H2O administrative area -->
    <password>corvus</password>
  </config>
  <managePartnershipEndpoint>http://localhost:8080/corvus/admin/ebms/partnership/managePartnershipEndpoint</managePartnershipEndpoint>
  <params>
    <!-- The partnership operation you want to execute, only used by EBMSPartnershipSender. The allowed enumeration of this tag are listed below:
    0 - Adding partnership
    1 - Deleting partnership
    2 - Updating partnership -->
    <partnershipOperation>0</partnershipOperation>
  </params>
</ebms-admin-request>
```

Configuration file for AS2:

3.10. Using Sample Clients
partnership-xml

Sample content of the partnership-xml files are shown below. For more details, please refer to the articles *Setting Up ebMS 2.0 Partnerships* and *Setting Up AS2 Partnerships*.

Sample ebMS partnership:
Sample AS2 partnership:
ebMS

We have created two sample programs, `ebms-send` and `ebms-history`, to demonstrate how to communicate with Hermes web services.

Sending an ebMS message

`ebms-send` is a sample program to demonstrate how to upload an ebMS message to Hermes using the sender web service in the ebMS plugin. You can pack your payload as a SOAP message and send it to this service at the endpoint http://<HOST>:<PORT>/corvus/httpd/ebms/sender.

The elements in a SOAP request are shown below:

```xml
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```
For more information on the elements in the SOAP body of a send request, please refer to the section *ebMS Send Message Web Service*.

Before sending an ebMS message, please make sure a partnership is registered. Please refer to the section *Maintaining Partnerships* for more information.

Let’s take a look at the program parameters.

```
 ebms-send [partnership-xml] [config-xml] [log-path] [payload-path]
```

- **partnership-xml**: The filepath of the partnership configuration file. Default is `<HERMES2_HOME>/config/ebms-partnership.xml`.
- **config-xml**: The filepath of the message configuration file. Default is `<HERMES2_HOME>/config/ebms-send/ebms-request.xml`.
- **log-path**: The filepath of the logger to log query result or error. Default is `<HERMES2_HOME>/logs/ebms-send.log`.
- **payload (optional)**: The filepath of the payload attached in the message. Default is `<HERMES2_HOME>/config/ebms-send/testpayload`.

**config-xml**

Here is sample content of the config-xml file. This file is named `ebms-request.xml`, and placed under `<HERMES2_HOME>/config/ebms-send`. 

```
<tns:fromPartyType xmlns:tns="http://service.ebms.edi.cecid.hku.hk/">[From_Party_Type]</tns:fromPartyType>
<tns:toPartyType xmlns:tns="http://service.ebms.edi.cecid.hku.hk/">[To_Party_Type]</tns:toPartyType>
<tns:refToMessageId xmlns:tns="http://service.ebms.edi.cecid.hku.hk/">[Reference_Message_Id]</tns:refToMessageId>
<tns:serviceType xmlns:tns="http://service.ebms.edi.cecid.hku.hk/">[Service_Type]</tns:serviceType>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```
The following table explains the use of each element:

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;sendEndpoint&gt;</td>
<td>Refers to the address of the ebMS send service. It should be <code>http://&lt;HOST&gt;:&lt;PORT&gt;/corvus/httpd/ebms/sender</code></td>
</tr>
<tr>
<td>&lt;conversationId&gt;</td>
<td>Identifies which conversation this message belongs to. This is required for Hermes to create a valid message.</td>
</tr>
<tr>
<td>&lt;fromPartyId&gt; &lt;fromPartyType&gt; &lt;toPartyId&gt; &lt;toPartyType&gt;</td>
<td>Identifies the sender and receiver. These are required for Hermes to retrieve the message destination.</td>
</tr>
<tr>
<td>&lt;refToMessageId&gt;</td>
<td>The message id that is targeted to respond to.</td>
</tr>
<tr>
<td>&lt;serviceType&gt;</td>
<td>A type identifier for the ebXML service defined in the partnership.</td>
</tr>
</tbody>
</table>

You only need to change `<sendEndpoint>` to contain the correct address.

**partnership-xml**

Another configuration file needed is `partnership-xml`, which is named `ebms-partnership.xml` and placed under `<HERMES2_HOME>/config` by default.
Sample content is shown below:

```xml
<partnerhip>
  <ebms>
    <id>ebms-loopback</id>
    <!-- Mandatory, this is shared by different samples for sending, querying and receiving ebMS message -->
    <soap:soapId>/soapId</soap:soapId>
    <!-- Mandatory, this is shared by different samples for sending, querying and receiving ebMS message -->
    <service>http://localhost:8080/services/http://ebms/inbound</service>
    <!-- Mandatory, this is shared by different samples for sending, querying and receiving ebMS message -->
    <action>http://action/action</action>
  </ebms>
  <!-- partnerhip only -->
  <disabled>false</disabled>
  <syncReplyMode>true</syncReplyMode>
  <transportProtocolHttp>transportProtocol</transportProtocolHttp>
  <docRequested>false</docRequested>
  <ackRequested>true</ackRequested>
  <dupElimination>never</dupElimination>
  <actor></actor>
  <messageOrder:Next guaranted</messageOrder>
  <version:Duration></version:Duration>
  <retryCount>3</retryCount>
  <retryInterval>3600</retryInterval>
  <signRequested>false</signRequested>
  <digestAlgo:sha1</digestAlgo:sha1>
  <enc:Algorithm:rsa</enc:Algorithm:rsa>
  <enc:Algorithm:rsa</enc:Algorithm:rsa>
  <encryptedRequestMessage:encryptedRequestMessage>
  </ebms>
</partnerhip>
```

The mandatory elements are necessary to construct a SOAP message according to the WSDL. For more information, please read the article *Setting Up ebMS 2.0 Partnerships*.

Once you have configured these parameters correctly, the program can be executed. A message id will be displayed if the program has successfully executed.

Here is sample output from the program:
ebMS history query

*ebms-history* demonstrates the use of the message history web service (*msg-history*) in the ebMS plugin. There are several criteria defined for message history queries. By passing these criteria to Hermes through SOAP messages, the target results can be retrieved.

The message history service endpoint is `http://<HOST>:<PORT>/corvus/httpd/msg_history`.

The required elements in a SOAP request are as follows:

```xml
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
    <tns:messageBox xmlns:tns="http://service.ebms.edi.cecid.hku.hk/">
      <Message_Box/>
    </tns:messageBox>
    <tns:status xmlns:tns="http://service.ebms.edi.cecid.hku.hk/">
      <Message_Status/>
    </tns:status>
    <tns:messageId xmlns:tns="http://service.ebms.edi.cecid.hku.hk/">
      <Message_Id/>
    </tns:messageId>
    <tns:conversationId xmlns:tns="http://service.ebms.edi.cecid.hku.hk/">
      <Conversation_Id/>
    </tns:conversationId>
    <tns:cpaId xmlns:tns="http://service.ebms.edi.cecid.hku.hk/">
      <CPA_Id/>
    </tns:cpaId>
    <tns:service xmlns:tns="http://service.ebms.edi.cecid.hku.hk/">
      <Defined_Service_with_trading_party/>
    </tns:service>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```
Let’s take a look at the program parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-xml</td>
<td>The filepath of the message configuration file. Default is ./config/ebms-history/ebms-request.xml.</td>
</tr>
<tr>
<td>log-path</td>
<td>The filepath of the logger to log query result or error. Default is ./logs/ebms-history.log.</td>
</tr>
</tbody>
</table>

**config-xml**

Here is sample content of the config-xml. This config-xml is named ebms-request.xml, and placed under <HERMES2_HOME>/config/ebms-history. There are several elements listed as search criteria. You can use the wildcard % in the values, and you can comment out unwanted elements.
Program operation

If the query is successfully executed, the result will look like:

After the messages are displayed by the program, you can perform further action on a selected message. If the selected message is placed under OUTBOX, the program will query its current status. If the message is placed under INBOX, the program will download the payload(s) if available.

Retrieving message payloads

There is a receiver web service provided by the ebMS plugin to retrieve messages. The receiver service endpoint is http://<HOST>:<PORT>/corvus/httpd/ebms/receiver.

The required elements in a SOAP request are as follows:

```xml
<SOAP-ENV:Header/>
<SOAP-ENV:Body>
<tns:messageId xmlns:tns="http://service.ebms.edi.cecid.hku.hk/" <MessageId/>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```
The message id is the only criteria needed to retrieve the payload of the target message. However, the payload is only available once. If the payload of a message has already been downloaded, the program cannot retrieve it again.

The program will ask for a folder path to store the payload with the filename `ebms.<MessageId>.Payload.<IndexofPayload>`.

---

**Check outgoing message status**

To check the status of outgoing messages, the program uses the status web service provided in the ebMS plugin. This service cannot check the status of incoming messages.

The required elements in a SOAP request are as follows:

```xml
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
    <tns:messageId xmlns:tns="http://service.ebms.edi.cced.hku.hk/"><MessageId/></tns:messageId>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

The program lists the message status along with a simple description:
AS2

We created similar sample programs for AS2 as well. The programs `as2-send` and `as2-history` are used to demonstrate how to communicate with Hermes web services through AS2 SOAP messages.

Sending an AS2 message

`as2-send` is a sample program to demonstrate how to upload a message to Hermes using the Sender Web Service in the AS2 plugin. You can pack your payload as a SOAP message and send it to this service with the endpoint `http://<HOST>:<PORT>/corvus/httpd/as2/sender`.

The required elements in a SOAP request are shown below:

```xml
<SOAP-ENV:Envelope
  xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:tns="http://service.ebms.edi.cecid.hku.hk/"
>
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
    <tns:as2_from
      xmlns:tns="http://service.ebms.edi.cecid.hku.hk/"
    >
      <as2_from/>
    </tns:as2_from>

    <tns:as2_to
      xmlns:tns="http://service.ebms.edi.cecid.hku.hk/"
    >
      <as2_to/>
    </tns:as2_to>

    <tns:type
      xmlns:tns="http://service.ebms.edi.cecid.hku.hk/"
    >
      <type/>
    </tns:type>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```
<as2_from> and <as2_to> contain the partnership information and <type> contains the content type of the payload.

Before sending an AS2 message, please check a partnership is registered. Please refer to the section *Maintaining Partnerships* for more information.

Let's take a look at the program parameters.

```
as2-send [partnership-xml] [config-xml] [log-path] [payload-path]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>partnership-xml</td>
<td>The filepath of the partnership configuration file. Default is &lt;HERMES2_HOME&gt;/config/as2-partnership.xml.</td>
</tr>
<tr>
<td>config-xml</td>
<td>The filepath of the message configuration file. Default is &lt;HERMES2_HOME&gt;/config/as2-send/as2-request.xml.</td>
</tr>
<tr>
<td>log-path</td>
<td>The filepath of the logger to log query result or error. Default is &lt;HERMES2_HOME&gt;/logs/as2-send.log.</td>
</tr>
<tr>
<td>payload (optional)</td>
<td>The filepath of the payload attached in the message. Default is &lt;HERMES2_HOME&gt;/config/as2-send/testpayload.</td>
</tr>
</tbody>
</table>

**config-xml**

Below is sample content of the config-xml file. This file is named as2-request.xml, and placed under <HERMES2_HOME>/config/as2-send.
The elements are explained in the table below:

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;sendEndpoint&gt;</code></td>
<td>Refer to the address of the AS2 sender web service. It should be <code>http://&lt;HOST&gt;:&lt;PORT&gt;/corvus/httpd/as2/sender</code>.</td>
</tr>
<tr>
<td><code>&lt;type&gt;</code></td>
<td>Specify the content type. For more information, please refer to AS2 Sender Web Service. Only <code>&lt;sendEndpoint&gt;</code> has to be changed to contain the correct address.</td>
</tr>
</tbody>
</table>

**partnership-xml**

Another configuration file is the `partnership-xml`, which is named `as2-partnership.xml` and placed under `<HERMES2_HOME>/config` folder by default.

Sample content is shown below:
<as2From> and <as2To> are required to construct a SOAP message according to the WSDL. For more information, please refer to Setting Up AS2 Partnerships.

Once you have configured these parameters, you can execute the program. A message id will be returned if the program has been successfully executed. Below is a sample output from the program.
AS2 history query

`as2-history` is a demo program that utilizes the message history web service in the AS2 plugin. The web service is called `msg-history`. There are several criteria defined for message history queries. By passing these criteria to Hermes 2 through SOAP messages, you can retrieve your target messages.

The message history web service endpoint is `http://<HOST>:<PORT>/corvus/httpd/as2/msg_history`.

The required elements in a SOAP request are shown as below:

```xml
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
    <tns:as2To xmlns:tns="http://service.ebms.edi.cecid.hku.hk/">[AS2_To_Party]</tns:as2To>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```
Using this service, you can search for messages by message properties as well as partnership information.

Let’s take a look at the program parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-xml</td>
<td>The filepath of the message configuration file. Default is <code>&lt;HERMES2_HOME&gt;/config/as2-history/as2-request.xml</code>.</td>
</tr>
<tr>
<td>log-path</td>
<td>The filepath of the logger to log query result or error. Default is <code>&lt;HERMES2_HOME&gt;/logs/as2-history.log</code>.</td>
</tr>
</tbody>
</table>

**config-xml**

Below is sample content of the config-xml file. This file is named `as2-request.xml`, and placed under `<HERMES2_HOME>/config/as2-history`. There are several elements available to use as searching criteria. You can use the wildcard character `%` in the values and comment the unwanted elements.
Program operation

If the query has been executed successfully, the result will look like:

![Console output showing message retrieval](image)

Messages are listed in ascending order of the message timestamp (i.e. the earliest message will be listed with index 0). After the results are listed, you can select a message. If the message is placed under OUTBOX, the program will query its current status. If the message is placed under INBOX, the program will download the payload if available.

Retrieve message payload

There is a receiver service provided by the AS2 plugin for retrieving messages. The receiver service endpoint is http://<HOST>:<PORT>/corvus/httpd/as2/receiver.

The required elements in a SOAP request are as follows:

```xml
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
    <tns:messageId xmlns:tns="http://service.as2.edi.cecid.hku.hk/" [Message_Id]>
      <!--tns:messageId-->
    </SOAP-ENV:Body>
  </SOAP-ENV:Envelope>
```
You can specify the id of your target message in the SOAP message to retrieve its payload. However, the payload is only available once. If the payload has already been downloaded, the program cannot retrieve it again.

As shown above, the program will ask for a folder to store the payload(s) with filename `as2.<MessageId> Payne.theros.Payload.<IndexofPayload>.

**Check outgoing message status**

To check the status of outgoing messages, the program uses the status web service provided in the AS2 plugin. This service cannot check the status of incoming messages.

The required elements in a SOAP request are the following:

```xml
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
    <tns:messageId xmlns:tns="http://service.as2.edi.cecid.hku.hk/" [Message_ID]>
      <tns:messageId>
    </SOAP-ENV:Body>
  </SOAP-ENV:Envelope>
```

Here is sample output from the program:

3.10. **Using Sample Clients** 115
The program will display the message status along with a simple description.

See also

- The First Step
- Setting Up ebMS 2.0 Partnerships
- Setting Up AS2 Partnerships
- Using Hermes API

Configuring Secure Messaging

Sign and Verify Message

In order to store a private key for message signing, a keystore is needed. Under current implementation, only PKCS12 keystore is supported. If Hermes was installed using the installer, there are keystore files placed in the folder called security under both ebMS and AS2/AS2 Plus plugins.

To enable message signing, you need to configure the plugin with a corresponding keystore. You can set the default keystore settings when running the installer or you can create a new customized keystore. To learn more about generating a keystore, please refer to Generate a PKCS12 Keystore and Certificate.
Sender configuration

To instruct Hermes to perform message signing with the correct private key, the corresponding Keystore Manager should be configured with the correct parameters.

Here are descriptions of the parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>keystore-location</td>
<td>Absolute file path pointing to the keystore file.</td>
</tr>
<tr>
<td>keystore-password</td>
<td>Password to access to keystore.</td>
</tr>
<tr>
<td>key-alias</td>
<td>Name of the private key.</td>
</tr>
<tr>
<td>key-password</td>
<td>Password to retrieve the private key. (PKCS12 standard: key-password is equal to keystore-password)</td>
</tr>
<tr>
<td>keystore-type</td>
<td>The type of the keystore. This must be PKCS12.</td>
</tr>
<tr>
<td>keystore-provider</td>
<td>The class provider to handle the keystore. org.bouncycastle.jce.provider.BouncyCastleProvider</td>
</tr>
</tbody>
</table>

ebMS Sender Settings

Open the configuration file named ebms.module.xml that is placed in the conf folder of the ebMS plugin. A component named keystore-manager-for-signature is defined to manage the keystore.

```xml
<component id="keystore-manager-for-signature"
    name="Key Store Manager for Digital Signature">
    <class>hk.hku.cecid.piazza.commons.security.KeyStoreManager</class>
    <parameter name="keystore-location" value="<Hermes Home>/plugins/corvus-ebms/security/corvus.p12"/>
    <parameter name="keystore-password" value="password"/>
    <parameter name="key-alias" value="corvus"/>
    <parameter name="key-password" value="password"/>
    <parameter name="keystore-type" value="PKCS12"/>
    <parameter name="keystore-provider" value="org.bouncycastle.jce.provider.BouncyCastleProvider"/>
</component>
```

AS2/AS2 Plus Sender Settings

Open the configuration file named as2.module.core.xml that is placed in the conf folder of the AS2/AS2 Plus plugin. A component named keystore-manager is defined to manage the keystore.

```xml
<component id="keystore-manager" name="AS2 Key Store Manager">
    <class>hk.hku.cecid.piazza.commons.security.KeyStoreManager</class>
    <parameter name="keystore-location" value="corvus.p12"/>
    <parameter name="keystore-password" value="password"/>
    <parameter name="key-alias" value="corvus"/>
    <parameter name="key-password" value="password"/>
    <parameter name="keystore-type" value="PKCS12"/>
    <parameter name="keystore-provider" value="org.bouncycastle.jce.provider.BouncyCastleProvider"/>
</component>
```
Receiver configuration

For a receiver to verify the signature, a public certificate should be provided by the sender through the partnership maintenance page.

Set the value of Signing Required to true. For detailed settings of the partnership, please refer to Setting Up AS2 Partnerships or Setting Up ebMS 2.0 Partnerships.

Send Messages Through HTTPS

SSL server authentication

To enable server authentication in Tomcat, a truststore and a keystore have to be configured in Hermes and Tomcat respectively.

On the sending side, a truststore is defined in corvus.properties.xml, which is where the certificates of trusted servers are stored. When the sending Hermes tries to establish a secure connection, the receiving Hermes will provide a public certificate for the sender to identify their identity. If this certificate is self-signed, it should be added to the truststore defined on the sending side.

On the receiving side, a keystore is defined in the server.xml of Tomcat. The keystore contains its paired private key and public certificate. If the keystore is self-signed, the certificate has to be exported, then imported to the truststore of the sending Hermes.

The details of this procedure are shown below. For information about how to create a keystore and generate a public certificate, please refer to the section Generate a PKCS12 Keystore and Certificate.

Sender configuration

As mentioned before, a truststore needs to be configured. In this example, a JKS keystore is used as a truststore as it is much simpler to import a self-signed certificate.

If there is no keystore file found, Keytool can be used to create a new keystore:

```
keytool -importcert -file {filepath-and-name-of-certificate} -alias {key-alias} -keystore {filepath-and-name-of-keystore} -storetype jks -storepass {password}
```

The program will display the certificate information and ask for confirmation. Enter yes after verifying the details.
Open corvus.properties.xml. The definition of the truststore can be found under the environment component.

Here are descriptions of the parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>trustStore</td>
<td>The absolute file path to the keystore.</td>
</tr>
<tr>
<td>trustStorePass</td>
<td>The password to access the keystore.</td>
</tr>
<tr>
<td>trustStoreType</td>
<td>The type of the keystore. Both PKCS12 and JKS are supported.</td>
</tr>
</tbody>
</table>

If asynchronous replies are enabled for the receiving partnership, the same configuration needs to be made for Hermes on both sides, however the roles are reversed.

**Receiver configuration**

Once a keystore has been created, server.xml needs to be modified to specify the keystore parameters.

1. Uncomment the connector definition on port 8443.
2. Add the following attributes for keystore configuration.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>keystoreFile</td>
<td>An absolute file path to the keystore file.</td>
</tr>
<tr>
<td>keystorePass</td>
<td>The password to access the keystore.</td>
</tr>
<tr>
<td>keystoreType</td>
<td>The type of keystore. Both PKCS12 and JKS are supported.</td>
</tr>
<tr>
<td>keyalias</td>
<td>Optional. If the keystore contains more than one key pair, specify the target key-pair with an alias.</td>
</tr>
<tr>
<td>clientAuth</td>
<td>Set this to false to indicate only Server Authentication is needed.</td>
</tr>
</tbody>
</table>

**SSL client authentication**

In addition to server authentication, client authentication can also be applied to Hermes to achieve secure connections for message deliveries.

Once the server authentication is complete, the receiving Hermes will ask for the identity of the sending Hermes. The sender will provide a public certificate to the receiver, which will be compared to the trusted certificates in the truststore.
Sender configuration

To store the private key and public certificate pair that identifies the sender, a keystore is needed. Here are descriptions of the parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>javax.net.ssl.keyStore</td>
<td>The absolute file path to the keystore.</td>
</tr>
<tr>
<td>javax.net.ssl.keyStorePassword</td>
<td>The password to access the keystore.</td>
</tr>
<tr>
<td>javax.net.ssl.keyStoreType</td>
<td>The type of the keystore.</td>
</tr>
</tbody>
</table>

Receiver configuration

In order to store trusted certificates, a truststore needs to be declared in the server.xml of Tomcat. Here are descriptions of the attributes:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>keystoreFile</td>
<td>The absolute file path to the keystore.</td>
</tr>
<tr>
<td>keystorePass</td>
<td>The password to access the keystore.</td>
</tr>
<tr>
<td>keystoreType</td>
<td>The type of the keystore. Both PKCS12 and JKS are supported.</td>
</tr>
<tr>
<td>clientAuth</td>
<td>Set this to true to enforce client authentication.</td>
</tr>
</tbody>
</table>

Generate a PKCS12 Keystore and Certificate

To create a keystore and certificate, Keytool or OpenSSL can be used.

Using Keytool

Keytool is provided with Java SDK.

1. Invoke keytool with parameters.

```
keytool -genkey -alias {key-alias} -keyalg RSA -keystore {filepath-and-name-of-keystore} -storetype pkcs12 -storepass {password} -keypass {password}
```

The same password value is used for keypass and storepass in this command.
2. Input more detailed information.

After entering the information, a keystore will be created. It can be verified using `Keytool`.

```
keytool -list -keystore {filepath-and-name-of-keystore} -storetype pkcs12
```

The password specified in the `storepass` attribute is needed to access the keystore.

3. Export certificate.

The private key has been generated and stored in the keystore, but a public certificate is still needed for the receiver to verify signatures.

```
keytool -exportcert -alias {key-alias} -keystore {filepath-and-name-of-keystore} -storetype pkcs12 -file {filepath-and-name-of-certificate}
```

Enter the password specified in the `storepass` attribute to access the keystore.
The certificate can be verified with the following command:

```bash
dir$ keytool -printcert -file {filepath-and-name-of-certificate}
```

Using OpenSSL

OpenSSL can be found [here](#).

1. Generate private key.
   
   Invoke `openssl` to enter the OpenSSL environment, then execute the following:

   ```bash
genrsa -out {filepath-and-name-of-key} {length-in-bits}
```
2. Generate certificate signing request.

```
req -new -key {filepath-and-name-of-key} -out {filepath-and-name-of-signing-request}
```

```
OpenSSL> req -new -key cecid.key -out cecid.csr
You are about to be asked to enter information that will be incorporated into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.' the field will be left blank.
-----
Country Name (2 letter code) [AU]:K
  string is too short, it needs to be at least 2 bytes long
Country Name (2 letter code) [AU]:HK
State or Province Name (full name) [Some-State]:Hong Kong
Locality Name (eg, city) []:city
Organization Name (eg, company) [Internet Widgits Pty Ltd]:CECID
Organizational Unit Name (eg, section) []:cecid
Common Name (eg, YOUR name) []:cecid.hku.hk
Email Address []:info@cecid.hku.hk
```  


```
x509 -req -days {number-of-days-valid} -in {filepath-and-name-of-signing-request} -signkey {filepath-and-name-of-key} -sha1 -out {filepath-and-name-of-certificate}
```

```
OpenSSL> x509 -req -days 1000 -in cecid.csr -signkey cecid.key -sha1 -out cecid.cer
Signature ok
subject=/C=HK/ST=Hong Kong/L=city/O=CECID/OU=cecid/CN=cecid.hku.hk/emailAddress=info@cecid.hku.hk
Getting Private key
OpenSSL>
```  

4. Export to keystore in PKCS12 format.

3.11. Configuring Secure Messaging
Supported Parameters

The following key pair algorithms and signature algorithms have been tested:

**Key pair algorithm (keyalg)**

<table>
<thead>
<tr>
<th>keyalg</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSA</td>
<td>Generates keypairs for the Digital Signature Algorithm</td>
</tr>
<tr>
<td>RSA¹</td>
<td>Generates keypairs for the RSA algorithm (Signature/Cipher)</td>
</tr>
</tbody>
</table>

¹ RSA has been tested with `keysize= 1024, 2048, 4096.`
Signature algorithm (sigalg)

The signature algorithm with SHA-* and the RSA encryption algorithm as defined in the OSI Interoperability Workshop, using the padding conversions described in PKCS1.

- SHA1 with RSA
- SHA256 with RSA
- SHA512 with RSA
- MD5 with RSA
- MD2 with RSA
- SHA1 with DSA
- DSA with SHA-1 signature algorithm which uses the SHA-1 digest algorithm and DSA to create and verify DSA digital signatures as defined in FIPS PUB 186.
Parameter combinations

The following combinations of algorithms and parameters have been tested with ebMS and AS2:

### ebMS

<table>
<thead>
<tr>
<th>tool</th>
<th>Keytool</th>
<th>OpenSSL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1024</td>
<td>2048</td>
</tr>
<tr>
<td>keys</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SHA1</td>
<td>ok</td>
<td>ok</td>
</tr>
<tr>
<td>SHA256</td>
<td>ok</td>
<td>ok</td>
</tr>
<tr>
<td>MD5</td>
<td>not supported</td>
<td>ok</td>
</tr>
<tr>
<td>SHA512</td>
<td>not supported</td>
<td>ok</td>
</tr>
<tr>
<td>MD2</td>
<td>not supported</td>
<td>ok</td>
</tr>
</tbody>
</table>

### AS2

<table>
<thead>
<tr>
<th>tool</th>
<th>Keytool</th>
<th>OpenSSL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1024</td>
<td>2048</td>
</tr>
<tr>
<td>keys</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SHA1</td>
<td>ok</td>
<td>ok</td>
</tr>
<tr>
<td>SHA256</td>
<td>ok</td>
<td>ok</td>
</tr>
<tr>
<td>MD5</td>
<td>not supported</td>
<td>ok</td>
</tr>
<tr>
<td>SHA512</td>
<td>not supported</td>
<td>ok</td>
</tr>
<tr>
<td>MD2</td>
<td>not supported</td>
<td>ok</td>
</tr>
</tbody>
</table>

See also

- Wiki Public Key Infrastructure (Wiki)
- Public Key Infrastructure (FreeMagazine)

Developing Hermes Applications

Overview

This application development guide provides guidelines for developing Hermes messaging applications, which exchange messages reliably and securely with Hermes. A Hermes server provides web services for an application to communicate with another Hermes server. These web services allow the application to:

- Request Hermes to send a payload to another Hermes or a compatible messaging gateway on the receiver party;
- Retrieve the message identifier of a received message which has not retrieved yet;
• Retrieve the payloads of a message which is identified by its message identifier; and
• Obtain the message status of an outgoing or incoming message.

For information about installing Hermes and communicating with Hermes using an external application, please refer to *Installing Hermes* and *Using Hermes API*.

### Application Integration with Hermes

The above figure shows a typical architecture for integrating client applications with Hermes servers. Two parties exchange business messages with Hermes through ebMS 2.0 or AS2 over a transport protocol, such as HTTP, HTTPS or SMTP.

On the sender side, a backend system produces business data to be transferred to the receiver party. The sender application extracts the data from the backend system and submit them to Hermes through a web service. The sender’s Hermes sends the data as payloads in a business message. Then, the application invokes a web service to check whether the message is delivered successfully.

On the receiver side, Hermes receives the message. The receiver application retrieves the message from Hermes, extracts the payloads from the message, and stores them into the receiver backend system.

The application interacts with Hermes using web services, i.e., SOAP or REST APIs. The benefits of using web services are as follows.

- **Implementation-independent.** Since the application interacts with Hermes using web services, the application can be implemented in any programming languages, as long as web services are supported.
• **Firewall-friendly.** The web services use HTTP as the transport protocol. The application calls Hermes via web services over HTTP; in this way, persistent and stateful connectivity between Hermes and the application is not required. Even when there is a firewall between Hermes and the application, they can communicate with each other as long as HTTP port between them are not blocked.

**Prerequisites**

The source code shown below comes from the Hermes loopback test. The sample code assumes Hermes is using localhost with port 8080 (i.e., the default port of Tomcat).

The sample code requires the following libraries:

- activation.jar
- mail.jar

**Import Java Packages in Web Service Client**

To call the Hermes SOAP web service, please import the following Java packages:

```java
import java.net.URL;
import java.net.MalformedURLException;
import javax.activation.DataHandler;
import javax.activation.FileDataSource;
import javax.xml.soap.AttachmentPart;
import javax.xml.soap.MessageFactory;
import javax.xml.soap.Name;
import javax.xml.soap.SOAPBody;
import javax.xml.soap.SOAPConnection;
import javax.xml.soap.SOAPConnectionFactory;
import javax.xml.soap.SOAPElement;
import javax.xml.soap.SOAPException;
import javax.xml.soap.SOAPFactory;
import javax.xml.soap.SOAPMessage;
```

**Writing ebMS Messaging Client**

**Send ebMS Message**

Create a SOAP message with the following 10 paremeters, and send it to Hermes as a web service request.

- `cpaId`: Collaboration Protocol Agreement ID
- `service`: Service
- `action`: Action
- `convId`: Conversation ID
- `fromPartyId`: Sender party ID
- `fromPartyType`: Sender party type
- `toPartyId`: Receiver party ID
- `toPartyType`: Receiver party type
- `refToMessageId`: Refer-to message Id
1. Define a namespace URI and prefix conforming to the WSDL, and define the endpoint URL of the ebMS sender web service.

```java
private String nsURI = "http://service.ebms.edi.cecid.hku.hk/";
private String nsPrefix = "tns";
private URL senderWSURL = "http://localhost:8080/corvus/httpd/ebms/sender";
```

2. Create a SOAP message factory and a SOAP message object.

```java
SOAPMessage request = MessageFactory.newInstance().createMessage();
```

3. Populate the SOAP body by filling in the required parameters such as:

```xml
<cpaId> ebmscpaid </cpaId>
<service> http://localhost:8080/corvus/httpd/ebms/inbound </service>
[action> action </action>
<convId> conversationId </convId>
<fromPartyId> fromPartyId </fromPartyId>
<fromPartyType> fromPartyType </fromPartyType>
<toPartyId> toPartyId </toPartyId>
<toPartyType> toPartyType </toPartyType>
<refToMessageId> refToMessageId </refToMessageId>
<serviceType> serviceType </serviceType>
```

To send an ebMS message, compose a sample SOAP request as below:

```java
SOAPBody soapBody = request.getSOAPBody();
soapBody.addChildElement(createElement("cpaId", nsPrefix, nsURI, cpaId));
soapBody.addChildElement(createElement("service", nsPrefix, nsURI, service));
soapBody.addChildElement(createElement("action", nsPrefix, nsURI, action));
soapBody.addChildElement(createElement("convId", nsPrefix, nsURI, conversationId));
soapBody.addChildElement(createElement("fromPartyId", nsPrefix, nsURI, fromPartyId));
soapBody.addChildElement(createElement("fromPartyType", nsPrefix, nsURI, fromPartyType));
soapBody.addChildElement(createElement("toPartyId", nsPrefix, nsURI, toPartyId));
soapBody.addChildElement(createElement("toPartyType", nsPrefix, nsURI, toPartyType));
soapBody.addChildElement(createElement("refToMessageId", nsPrefix, nsURI, refToMessageId));
soapBody.addChildElement(createElement("serviceType", nsPrefix, nsURI, serviceType));
```

The method `createElement` creates a SOAP element with the namespace prefix `nsPrefix`, the namespace URL `nsURI`, and the string value of the element.

The implementation of `createElement` is shown below:

```java
SOAPElement soapElement = SOAPFactory.newInstance().createElement(localName, nsPrefix, nsURI);
soapElement.addTextNode(value);
return soapElement;
```

4. Attach a payload to the SOAP message if necessary. Below example uses a purchase order XML as the payload, so the associated content type is `application/xml`.
5. Save the changes to the SOAP message.

```java
request.saveChange();
```

6. Send the SOAP request to Hermes and get the following SOAP response.

```java
SOAPMessage response = soapConn.call(request, senderWSURL);
SOAPBody responseBody = response.getSOAPBody();
```

7. Process the SOAP response, extract the identifier of the requested ebMS message, and print it to `System.out` if there is no SOAP fault.

```java
if (!responseBody.hasFault()){  
    SOAPElement messageIdElement = getFirstChild(responseBody, "message_id", nsURI);  
    System.out.println(messageIdElement == null ? null : messageIdElement.getValue());
} else {
    throw new SOAPException(responseBody.getFault().getFaultString());
}
```

The method `getFirstChild` gets the first element with the name `message_id` and the namespace URI `nsURI`. An existing `message_id` is a registered identifier, showing the message has been successfully submitted to Hermes.

Hermes translates the SOAP request into an ebMS message and saves the ebMS message in its persistent storage. Then, the sender Hermes delivers the ebMS message to the receiver Hermes specified in the SOAP request parameters, of which `cpaId`, `service` and `action` identify the partnership between the sender and receiver.

**List ebMS Messages**

Create a SOAP message with the following 9 parameters, and send it to Hermes as a web service request.

- `cpaId`: Collaboration Protocol Agreement ID
- `service`: Service
- `action`: Action
- `convId`: Conversation ID
- `fromPartyId`: Sender party ID
- `fromPartyType`: Sender party type
- `toPartyId`: Receiver party ID
- `toPartyType`: Receiver party type
- `numOfMessages`: Number of messages

1. Define a namespace URI and prefix conforming to the WSDL.
private String nsURI = "http://service.ebms.edi.cecid.hku.hk/";
private String nsPrefix = "tns";
private String URL receiverListWSURL = "http://localhost:8080/corvus/httpd/ebms/
  receiver_list";

2. Create a SOAP message factory and an SOAP message object.

SOAPMessage request = MessageFactory.newInstance().createMessage();

3. Populate the SOAP body by filling in the required parameters. For example:

```xml
<cpaId> ebmscpaid </cpaId>
<service> http://localhost:8080/corvus/httpd/ebms/inbound <service>
<action> action </action>
<convId> convId </convId>
<fromPartyId> fromPartyId </fromPartyId>
<fromPartyType> fromPartyType </fromPartyType>
<toPartyId> toPartyId </toPartyId>
<toPartyType> toPartyType </toPartyType>
<numOfMessages> 100 </numOfMessages>
```

Compose a sample SOAP request to list ebMS messages:

```java
SOAPBody soapBody = request.getSOAPBody();
soapBody.addChildElement(createElement("cpaId", nsPrefix, nsURI, cpaId));
soapBody.addChildElement(createElement("service", nsPrefix, nsURI, service));
soapBody.addChildElement(createElement("action", nsPrefix, nsURI, action));
soapBody.addChildElement(createElement("convId", nsPrefix, nsURI, conversationId));
soapBody.addChildElement(createElement("fromPartyId", nsPrefix, nsURI, fromPartyId));
soapBody.addChildElement(createElement("fromPartyType", nsPrefix, nsURI, fromPartyType));
soapBody.addChildElement(createElement("toPartyId", nsPrefix, nsURI, toPartyId));
soapBody.addChildElement(createElement("toPartyType", nsPrefix, nsURI, toPartyType));
soapBody.addChildElement(createElement("numOfMessages", nsPrefix, nsURI, numOfMessages));
```

The method `createElement` creates a SOAP element with the namespace `nsPrefix`, the namespace URL and the string value of the element.

The implementation of `createElement` is shown below:

```java
SOAPElement soapElement = SOAPFactory.newInstance().createElement(localName,
  nsPrefix, nsURI); soapElement.addTextNode(value); return soapElement;
```

4. Save changes to the SOAP message.

request.saveChange();

5. Send the SOAP request to Hermes and get the following SOAP response.

```java
SOAPMessage response = soapConn.call(request, receiverListWSURL);
SOAPBody responseBody = response.getSOAPBody();
```
Here is the SOAP response:

```xml
<soap-body>
  <messageIds>
    <messageId> ... </messageId>
    <messageId> ... </messageId>
    <messageId> ... </messageId>
    <messageId> ... </messageId>
  </messageIds>
</soap-body>
```

Process the SOAP response, extract the identifier of each requested message, and print it to System.out if there is no SOAP fault.

```java
if (!responseBody.hasFault()){
    SOAPElement messageIdsElement = getFirstChild(responseBody, "messageIds", nsURI);
    Iterator messageIdElementIter = getChildren(messageIdsElement, "messageId", nsURI);
    while (messageIdElementIter.hasNext()) {
        SOAPElement messageIdElement = (SOAPElement)messageIdElementIter.next();
        System.out.println(messageIdElement.getValue());
    }
} else {
    throw new SOAPException(responseBody.getFault().getFaultString());
}
```

The method `getFirstChild` gets the first element with the name `messageIds` and namespace `nsURI`. It then extracts every `messageId` which represents an available message awaiting for a further action.

**Retrieve ebMS Message**

Create a SOAP message with the identifier of the target message, and send it to Hermes as the web service request.

1. Define a namespace URI and prefix conforming to the WSDL.

```java
private String nsURI = "http://service.ebms.edi.cecid.hku.hk/";
private String nsPrefix = "tns";
private URL receiverWSURL = "http://localhost:8080/corvus/httpd/ebms/receiver";
```

2. Create a SOAP message factory and a SOAP message object.

```java
SOAPMessage request = MessageFactory.newInstance().createMessage();
```

3. Populate the SOAP body by filling in the required parameters.

```xml
<messageId> messageId </messageId>
```

Compose a sample SOAP request to retrieve an ebMS message:

```java
SOAPBody soapBody = request.getSOAPBody();
soapBody.addChildElement(createElement("messageId", nsPrefix, nsURI, messageId));
```

The method `createElement` creates a SOAP element with the namespace prefix `nsPrefix`, the namespace URL `nsURI`, and the string value of the element.

The implementation of `createElement` is shown below:
SOAPElement soapElement = SOAPFactory.newInstance().createElement(localName, nsPrefix, nsURI);
soapElement.addTextNode(value);
return soapElement;

4. Save the changes to the SOAP message.
request.saveChange();

5. Send the SOAP request to Hermes and get a SOAP response.
SOAPMessage response = soapConn.call(request, receiverWSURL);
SOAPBody responseBody = response.getSOAPBody();

Here is the SOAP response:

```xml
<soap-body>
  <hasMessage> ... </hasMessage>
</soap-body>
```

The attachment is formatted as a MIME part.

Process the SOAP response, and extract the payloads from the received ebMS message if available.

```java
if (!responseBody.hasFault()){
  SOAPElement hasMessageElement = getFirstChild(responseBody, "hasMessage", nsURI);
  ArrayList payloadsList = new ArrayList();
  if (hasMessageElement != null){
    Iterator attachmentPartIter = response.getAttachments();
    while(attachmentPartIter.hasNext()) {
      AttachmentPart attachmentPart = (AttachmentPart) attachmentPartIter.next();
      InputStream ins = attachmentPart.getDataHandler().getInputStream();
      // Do something I/O to extract the payload to physical file.
    }
  }
} else {
  throw new SOAPException(responseBody.getFault().getFaultString());
}
```

The method `getFirstChild` gets the first element with the name `hasMessage` and the namespace URI `nsURI`. The boolean value of `hasMessage` represents the existence of a payload in this message.

The payload is extracted from the attachment part, and written to the input stream. In this way, the data can be piped to a processor or saved as a file.

**Get ebMS Message Status**

Create a SOAP message with the identifier of the target message, and send it to Hermes as the web service request.

1. Define a namespace URI and prefix conforming to the WSDL.

```java
private String nsURI = "http://service.ebms.edi.cecid.hku.hk/";
private String nsPrefix = "tns";
private URL statusQueryWSURL = "http://localhost:8080/corvus/httpd/ebms/status";
```
2. Create a SOAP message factory and a SOAP message object.

   ```java
   SOAPMessage request = MessageFactory.newInstance().createMessage();
   ```

3. Populate the SOAP body by filling in the required parameters.

   ```xml
   <messageId> messageId </messageId>
   ```

   Compose a sample SOAP request to get the status of an ebMS message:

   ```java
   SOAPBody soapBody = request.getSOAPBody();
   soapBody.addChildElement(createElement("messageId", nsPrefix, nsURI, messageId));
   ```

   The method `createElement` creates a SOAP element with the namespace prefix `nsPrefix`, the namespace URL `nsURI` and the string value of the element.

   The implementation of `createElement` is shown below:

   ```java
   SOAPElement soapElement = SOAPFactory.newInstance().createElement(localName, nsPrefix, nsURI);
   soapElement.addTextNode(value);
   return soapElement;
   ```

4. Save the changes to the SOAP message.

   ```java
   request.saveChange();
   ```

5. Send the SOAP request to Hermes and get a SOAP response.

   ```java
   SOAPMessage response = soapConn.call(request, statusQueryWSURL);
   SOAPBody responseBody = response.getSOAPBody();
   ```

6. Here is the SOAP response:

   ```xml
   <soap-body>
   <MessageInfo>
   <status> The current status of message </status>
   <statusDescription> The current status description of message </statusDescription>
   <ackMessageId> The message id of acknowledgment / receipt if any </ackMessageId>
   <ackStatus> The status of acknowledgment / receipt if any </ackStatus>
   <ackStatusDescription> The status description of acknowledgment / receipt if any </ackStatusDescription>
   </MessageInfo>
   </soap-body>
   ```

   Process the SOAP response and extract the status information from the ebMS message if there is no SOAP fault.

   ```java
   if (!responseBody.hasFault()){
   SOAPElement messageInfoElement = getFirstChild(responseBody, "messageInfo", nsURI);
   System.out.println("Message Status : " + getFirstChild(messageInfoElement, "status", nsURI));
   System.out.println("Message Status Desc : " + getFirstChild(messageInfoElement, "statusDescription", nsURI));
   System.out.println("Ack Message Identifiers : " + getFirstChild(messageInfoElement, "ackMessageId", nsURI));
   System.out.println("Ack Status : " + getFirstChild(messageInfoElement, "ackStatus", nsURI));
   }``
```java
System.out.println("Ack Status Desc : " + getFirstChild(messageInfoElement,
    "ackStatusDescription", nsURI);} else {
    throw new SOAPException(responseBody.getFault().getFaultString());
}
```

The method `getFirstChild` gets the first element with the name `messageInfo` and the namespace URI `nsURI`. It then retrieves the status value from that element.

### Get ebMS Message History

Create a SOAP message with the following 7 parameters, and send it to Hermes as a web service request.

- **messageId**: Message ID
- **messageBox**: Message Box
- **conversationId**: Conversation ID
- **cpaId**: Collaboration Protocol Agreement ID
- **status**: Status
- **action**: Action
- **service**: Service

1. Define a namespace URI and prefix conforming to the WSDL.

   ```java
   private String nsURI = "http://service.ebms.edi.cecid.hku.hk/";
   private String nsPrefix = "tns";
   private URL msgHistoryWSURL = "http://localhost:8080/corvus/httpd/ebms/msg_history";
   ```

2. Create a SOAP message factory and a SOAP message object.

   ```java
   SOAPMessage request = MessageFactory.newInstance().createMessage();
   ```

3. Populate the SOAP body by filling in the required parameters.

   ```xml
   <messageId> messageId </messageId>
   <messageBox> messageBox </messageBox>
   <conversationId> conversationId </conversationId>
   <cpaId> cpaId </cpaId>
   <service> service </service>
   <action> action </action>
   <status> status </status>
   ```

Compose a sample SOAP request to get an ebMS message history:

```java
SOAPBody soapBody = request.getSOAPBody();
soapBody.addChildElement(createElement("messageId", nsPrefix, nsURI, messageId));
soapBody.addChildElement(createElement("messageBox", nsPrefix, nsURI, messageBox));
soapBody.addChildElement(createElement("conversationId", nsPrefix, nsURI, conversationId));
soapBody.addChildElement(createElement("cpaId", nsPrefix, nsURI, cpaId));
soapBody.addChildElement(createElement("service", nsPrefix, nsURI, service));
soapBody.addChildElement(createElement("fromPartyType", nsPrefix, nsURI, fromPartyType));
```
The method `createElement` creates a SOAP element with the namespace `nsPrefix`, the namespace URL `nsURI`, and the string value of the element.

The implementation of `createElement` is shown below:

```java
SOAPElement soapElement = SOAPFactory.newInstance().createElement(localName, nsPrefix, nsURI);
soapElement.addTextNode(value);
return soapElement;
```

4. Save the changes to the SOAP message.

```java
request.saveChange();
```

5. Send the SOAP request to Hermes and get the following SOAP response.

```java
SOAPMessage response = soapConn.call(request, msgHistoryWSURL);
SOAPBody responseBody = response.getSOAPBody();
```

6. Here is the SOAP response:

```xml
<soap-body>
  <messageList>
    <messageElement>
      <messageId>Message ID of this message</messageId>
      <messageBox>Message Box containing this message</messageBox>
    </messageElement>
    <messageElement>
      <messageId>Message ID of this message</messageId>
      <messageBox>Message Box containing this message</messageBox>
    </messageElement>
    ...
  </messageList>
</soap-body>
```

Process the SOAP response and iterate through the message history if there is no SOAP fault.

```java
if (!responseBody.hasFault()){
  SOAPElement msgList = SOAPUtilities.getElement(responseBody, "messageList", nsURI, 0);

  Iterator msgIterator = msgList.getChildElements();
  while (msgIterator.hasNext()){
    List elementList = new ArrayList();
    SOAPElement messageElement = (SOAPElement)msgIterator.next();
    Iterator elements = messageElement.getChildElements();
    // MessageId
    SOAPElement msgId = (SOAPElement)elements.next();
    // MessageBox
```
The method `getElement` gets the element with the name `messageList` and namespace URI `nsURI`. Then, a list of `messageElement` objects is extracted from `messageList`. Each `messageElement` object contains the values of `messageId` and `messageBox`.

**Writing AS2 Messaging Client**

**Send AS2 Message**

Create a SOAP message with the following 3 parameters, and send it to Hermes as a web service request.

- `as2_from`: AS2 sender
- `as2_to`: AS2 receiver
- `type`: Payload content type

1. Define a namespace URI and a prefix conforming to the WSDL.

```java
private String nsURI = "http://service.as2.edi.cecid.hku.hk/";
private String nsPrefix = "tns";
private URL senderWSURL = "http://localhost:8080/corvus/httpd/as2/sender";
```

2. Create a SOAP message factory and a SOAP message object.

```java
SOAPMessage request = MessageFactory.newInstance().createMessage();
```

3. Populate the SOAP body by filling in the required parameters.

```xml
<as2_from> as2from </as2_from>
<as2_to> as2to </as2_to>
<type> type </type>
```

Compose a sample SOAP request to send an AS2 message:

```java
SOAPBody soapBody = request.getSOAPBody();
soapBody.addChildElement(createElement("as2_from", nsPrefix, nsURI, this.as2From));
soapBody.addChildElement(createElement("as2_to", nsPrefix, nsURI, this.as2To));
soapBody.addChildElement(createElement("type", nsPrefix, nsURI, this.type));
```

The method `createElement` creates a SOAP element with the namespace prefix `nsPrefix`, the namespace URL `nsURI`, and the string value of the element.

The implementation of `createElement` is shown below:

```java
SOAPElement soapElement = SOAPFactory.newInstance().createElement(localName, nsPrefix, nsURI);
soapElement.addTextNode(value);
return soapElement;
```
4. Attach a payload if necessary. The following example uses a purchase order XML as the payload of the AS2 message, so the associated content type is application/xml.

```
AttachmentPart attachmentPart = request.createAttachmentPart();
FileDataSource fileDS = new FileDataSource(new File("purchase_order.xml"));
attachmentPart.setDataHandler(new DataHandler(fileDS));
attachmentPart.setContentType("application/xml");
request.addAttachmentPart(attachmentPart);
```

**Note:** Only one payload is allowed in the SOAP request for an AS2 message.

5. Save the changes to the SOAP message.
```
request.saveChange();
```

6. Send the SOAP request to Hermes and get the following SOAP response.
```
SOAPMessage response = soapConn.call(request, senderWSURL);
SOAPBody responseBody = response.getSOAPBody();
```

7. Process the SOAP response and extract the identifier of the AS2 message, and print it to System.out if there is no SOAP fault.
```
if (!responseBody.hasFault()){
    SOAPElement messageIdElement = getFirstChild(responseBody, "message_id", nsURI);
    System.out.println(messageIdElement == null ? null : messageIdElement.getValue());
} else {
    throw new SOAPException(responseBody.getFault().getFaultString());
}
```

The method `getFirstChild` gets the first element with the name `message_id` and the namespace URI `nsURI`.

The sender Hermes translates the SOAP request into an AS2 message which is stored in the file system, and then delivers the AS2 message to the receiver Hermes specified in the SOAP request parameters, of which `AS2From` and `AS2To` identify the partnership between the sender and the receiver.

### List AS2 Messages

Create a SOAP message with the following 3 parameters, and send it to Hermes as a web service request.

- **as2From**: AS2 sender
- **as2To**: AS2 receiver
- **numOfMessages**: Number of messages

1. Define a namespace URI and a prefix conforming to the WSDL.
```
private String nsURI = "http://service.as2.edi.cecid.hku.hk/";
private String nsPrefix = "tns";
private URL receiverListWSURL = "http://localhost:8080/corvus/httpd/as2/receiver_
       →list";
```

2. Create a SOAP message factory and a SOAP message object.
3. Populate the SOAP body by filling in the required parameters.

```java
SOAPMessage request = MessageFactory.newInstance().createMessage();

<as2_from> as2from </as2_from>
<as2_to> as2to </as2_to>
<numOfMessages> 100 </numOfMessages>
```

Compose a sample SOAP request to list AS2 messages:

```java
SOAPBody soapBody = request.getSOAPBody();
soapBody.addChildElement(createElement("as2From" , nsPrefix, nsURI, this.as2From));
soapBody.addChildElement(createElement("as2To" , nsPrefix, nsURI, this.as2To));
soapBody.addChildElement(createElement("numOfMessages", nsPrefix, nsURI, this.numOfMessages + "");
```

The method `createElement` creates a SOAP element with the namespace prefix `nsPrefix`, the namespace URL `nsURI` and the string value of the element.

The implementation of `createElement` is shown below:

```java
SOAPElement soapElement = SOAPFactory.newInstance().createElement(localName, nsPrefix, nsURI);
soapElement.addTextNode(value);
return soapElement;
```

4. Save the changes to the SOAP message.

```java
request.saveChange();
```

5. Send the SOAP request to Hermes and get the following SOAP response.

```java
SOAPMessage response = soapConn.call(request, senderWSURL);
SOAPBody responseBody = response.getSOAPBody();
```

Here is the SOAP response:

```xml
<soap-body>
  <messageIds>
    <messageId> ... </messageId>
    <messageId> ... </messageId>
    <messageId> ... </messageId>
    <messageId> ... </messageId>
  </messageIds>
</soap-body>
```

Process the SOAP response and extract the identifiers of the AS2 messages to `System.out` if there is no SOAP fault.

```java
if (!responseBody.hasFault()){
    SOAPElement messageIdsElement = getFirstChild(responseBody, "messageIds", nsURI);
    Iterator messageIdElementIter = getChildren(messageIdsElement, "messageId", nsURI);
    while(messageIdElementIter.hasNext()) {
        SOAPElement messageIdElement = (SOAPElement)messageIdElementIter.next();
        System.out.println(messageIdElement.toString());
    }
}
```
The method `getFirstChild` gets the first element with the name `messageIds` and the namespace URI `nsURI`. All children with the name `messageId` and the namespace URI `nsURI` are then extracted.

### Retrieve AS2 Message

Create a SOAP message with the identifier of the target message, and send it to Hermes as the web service request.

1. Define a namespace URI and a prefix conforming to the WSDL.

   ```java
   private String nsURI = "http://service.as2.edi.cecid.hku.hk/";
   private String nsPrefix = "tns";
   private URL receiverWSURL = "http://localhost:8080/corvus/httpd/as2/receiver";
   ```

2. Create a SOAP message factory and a SOAP message object.

   ```java
   SOAPMessage request = MessageFactory.newInstance().createMessage();
   ```

3. Populate the SOAP body by filling in the required parameters.

   ```xml
   <messageId> messageId </messageId>
   ```

   Compose a sample SOAP request to retrieve an AS2 message:

   ```java
   SOAPBody soapBody = request.getSOAPBody();
   soapBody.addChildElement(createElement("messageId", nsPrefix, nsURI, messageId));
   ```

   The method `createElement` creates a SOAP element with the namespace `nsPrefix`, the namespace URL `nsURI` and the string value of the element.

   The implementation of `createElement` is shown as below:

   ```java
   SOAPElement soapElement = SOAPFactory.newInstance().createElement(localName, 
   - nsPrefix, nsURI);
   soapElement.addTextNode(value);
   return soapElement;
   ```

4. Save the changes to the SOAP message.

   ```java
   request.saveChange();
   ```

5. Send the SOAP request to Hermes and get the following SOAP response.

   ```java
   SOAPMessage response = soapConn.call(request, receiverWSURL);
   SOAPBody responseBody = response.getSOAPBody();
   ```

6. Here is the SOAP response:

   ```xml
   <soap-body>
       <hasMessage> ... </hasMessage>
   </soap-body>
   ```
The attachment is formatted as a MIME part.

Process the SOAP response and extract the payload from the AS2 message if available.

```java
if (!responseBody.hasFault()){
    SOAPElement hasMessageElement = getFirstChild(responseBody, "hasMessage", nsURI);
    ArrayList payloadsList = new ArrayList();
    if (hasMessageElement != null){
        Iterator attachmentPartIter = response.getAttachments();
        while (attachmentPartIter.hasNext()) {
            AttachmentPart attachmentPart = (AttachmentPart) attachmentPartIter.next();
            InputStream ins = attachmentPart.getDataHandler().getInputStream();
            // Do something I/O to extract the payload to physical file.
        }
    } else {
        throw new SOAPException(responseBody.getFault().getFaultString());
    }
}
```

The method `getFirstChild` gets the first element with the name `hasMessage` and namespace URI `nsURI`. The boolean value of `hasMessage` represents the existence of a payload in this message.

The payload is extracted from the attachment part and sent to the input stream. The data can be piped to a processor or saved into a file.

**Get AS2 Message Status**

Create a SOAP message with the identifier of the target message, and send it to Hermes as a web service request.

1. Define a namespace URI and a prefix conforming to the WSDL.

```java
private String nsURI = "http://service.as2.edi.cecid.hku.hk/";
private String nsPrefix = "tns";
private URL statusQueryWSURL = "http://localhost:8080/corvus/httpd/as2/status";
```

2. Create a SOAP message factory and a SOAP message object.

```java
SOAPMessage request = MessageFactory.newInstance().createMessage();
```

3. Populate the SOAP body by filling in the required parameters.

```xml
<messageId> messageId </messageId>
```

Compose a sample SOAP request to get the status of an AS2 message:

```java
SOAPBody soapBody = request.getSOAPBody();
soapBody.addChildElement(createElement("messageId", nsPrefix, nsURI, messageId));
```

The method `createElement` creates a SOAP element with the namespace prefix `nsPrefix`, the namespace URL `nsURI` and the string value of the element.

The implementation of `createElement` is shown below:

```java
SOAPElement soapElement = SOAPFactory.newInstance().createElement(localName, nsPrefix, nsURI);
soapElement.addTextNode(value);
return soapElement;
```
4. Save the changes to the SOAP message.

   request.saveChange();

5. Send the SOAP request to get the status of an AS2 message and get the following SOAP response.

   SOAPMessage response = soapConn.call(request, statusQueryWSURL);
   SOAPBody responseBody = response.getSOAPBody();

6. Here is the SOAP response:

   <soap-body>
     <MessageInfo>
       <status> The current status of message </status>
       <statusDescription> The current status description of message </statusDescription>
       <mdnMessageId> The message id of acknowledgment / receipt if any </mdnMessageId>
       <mdnStatus> The status of acknowledgment / receipt if any </mdnStatus>
       <mdnStatusDescription> The status description of acknowledgment / receipt if any </mdnStatusDescription>
     </MessageInfo>
   </soap-body>

Process the SOAP response and extract the status of the AS2 message if there is no SOAP fault.

   if (!responseBody.hasFault()){
     SOAPElement messageInfoElement = getFirstChild(responseBody, "MessageInfo", nsURI);
     System.out.println("Message Status : " + getFirstChild(messageInfoElement, "status", nsURI));
     System.out.println("Message Status Desc : " + getFirstChild(messageInfoElement, "statusDescription", nsURI));
     try {
       getFirstChild(messageInfoElement, "mdnMessageId", nsURI);
       System.out.println("Ack Message Identifiers : ");
     } catch (Exception e) {
       System.out.println("Ack Status : " + getFirstChild(messageInfoElement, "mdnStatus", nsURI));
       System.out.println("Ack Status Desc : " + getFirstChild(messageInfoElement, "mdnStatusDescription", nsURI));
     }
   } else {
     throw new SOAPException(responseBody.getFault().getFaultString());
   }

The method getFirstChild gets the first element with the name MessageInfo and the namespace URI nsURI.

Get AS2 Message History

Create a SOAP message with the following 5 parameters, and send it to Hermes as the web service request.

- messageId: Message ID
- messageBox: Message box
- as2From: AS2 sender
- as2To: AS2 receiver
1. Define the namespace URI and a prefix conforming to the WSDL.

```java
private String nsURI = "http://service.as2.edi.cecid.hku.hk/";
private String nsPrefix = "tns";
private URL msgHistoryWSURL = "http://localhost:8080/corvus/httpd/as2/msg_history";
```

2. Create a SOAP message factory and a SOAP message object.

```java
SOAPMessage request = MessageFactory.newInstance().createMessage();
```

3. Populate the SOAP body by filling in the required parameters.

```xml
<messageId> messageId </messageId>
<messageBox> messageBox </messageBox>
<as2From> as2From </as2From>
<as2To> as2To </as2To>
<status> status </status>
```

4. Save the changes to the SOAP message.

```java
request.saveChange();
```

5. Send the SOAP request to Hermes to get an AS2 message history and get a SOAP response.

```java
SOAPMessage response = soapConn.call(request, receiverListWSURL);
SOAPBody responseBody = response.getSOAPBody();
```

Here is the SOAP response.

```xml
<soap-body>
  <messageList>
    <messageElement>
      <messageId> Message ID of this message </messageId>
      <messageBox> Message Box containing this message </messageBox>
    </messageElement>
  </messageList>
</soap-body>
```
Process the SOAP response and iterate through the AS2 message history if there is no SOAP fault.

```java
if (!responseBody.hasFault()){
    SOAPElement msgList = SOAPUtilities.getElement(responseBody, "messageList", nsURI, 0);
    Iterator msgIterator = msgList.getChildElements();
    while (msgIterator.hasNext()){
        List elementList = new ArrayList();
        SOAPElement messageElement = (SOAPElement)msgIterator.next();
        Iterator elements = messageElement.getChildElements();
        // MessageId
        SOAPElement msgId = (SOAPElement)elements.next();
        // MessageBox
        SOAPElement msgBox = (SOAPElement)elements.next();
        System.out.println("Message ID: " + (String)msgId.get(0) + "\t" +
                "Message Box: " + msgBox.get(0));
    }
}
```

The method `getElement` gets the element with the name `messageList` and the namespace URI `nsURI`. The `messageElement` objects are extracted from the `messageList` object. Each `messageElement` object contains the values of `messageId` and `messageBox`.

### References

#### Reference Documentation

- *The First Step*
- *Installing Hermes*
- *Using Hermes API*
- *Setting Up ebMS 2.0 Partnerships*
- *Setting Up AS2 Partnerships*
- *OASIS ebMS 2.0 Specification*
- *AS2 Specification*
Reference Source Code

- Hermes loopback test
Index

E
environment variable
JAVA_HOME, 6, 22

J
JAVA_HOME, 6, 22