Q1. What is the public WSDL for?

A1. The published (public) WSDL is for production.

A conformance WSDL is provided with the vendor package.

Q2. Why is the EDT Service not responding?

A2. Known or scheduled outages will be communicated.

You can also forward details to [HSC.MCEDT.Conformance.MoH@Ontario.ca](mailto:HSC.MCEDT.Conformance.MoH@Ontario.ca).

Q3. Does the ministry provide sample code?

A3. No

Q4. What file naming convention should be used?

A4. Please refer to the technical specifications.

<http://health.gov.on.ca/en/pro/publications/ohip/docs/techspec_mcedt_ebs.pdf>

Q5. Do I need to populated the MSA header elements

A5. No, EDT uses IDP.

Q6. Can the ministry provide help with the configuration of the platform I am using and/or assist with debugging?

A6. No.

Q7. Why am I receiving “General System Error; contact your technical support or software vendor”?

A7. Please forward details to [HSC.MCEDT.Conformance.MoH@Ontario.ca](mailto:HSC.MCEDT.Conformance.MoH@Ontario.ca).

Q8. Who can answers questions about available service methods?

A8. Please refer to the technical specifications.

<http://health.gov.on.ca/en/pro/publications/ohip/docs/techspec_mcedt_ebs.pdf>

Q9. Is MOH ID the same as ServiceUserMUID element in the IDP header.

A9. Those terms are synonymous.

Q10 How many results are returned in the list method?

A10. List method results are returned one page at a time, to a maximum 50 items per page.

Q11. Who created the audit ID?

A11. An audit ID is generated by the send of the request.

Please refer to the technical specifications.

<http://health.gov.on.ca/en/pro/publications/ohip/docs/techspec_mcedt_ebs.pdf>

Q12. What are the steps to download new documents available for a service user?

A12. - send getTypeList request

- if returned access type is DOWNLOAD or BOTH, send List request with status DOWNLOADABLE

- when received number of resourceID's, send Download request

Q13. What is the best way to avoid downloading files that have already been downloaded and only download the new files?

A13. It is the responsibility of the application to determine and track what file have already been downloaded.

Q14. Does the list method return the results set in ascending order by the create timestamp or modify timestamp fields?

A14. The list method return order is by create timestamp, descending (newest first).

Q15. How does the authentication work?

A15. A provider registers with our Identity Provider (IPD), GoSecure. The ministry trusts GoSecure and grants access based on that trust.

Q16. How do I use that account?

A16. The account (email address) and password are components of the digital signature.

Q17. What do I do with the ARM files provided in the Conformance and Production WSDL Zip files?

A17. Import the ARM files into the key store and trust store that you plan on distributing with your application.

Q18. There are a three ARM files how are they used?

A18. The go-pki\_cacert.arm is the CA signing certificate for the (OPS) GO-PKI Certificate Authority. It signs the certificate used by the service for encryption and verification. The public key for the ministry, included in the certificate we return in a response, is signed by the GO-PKI CA.

The Entrust L1C Chain Certificate.arm is the Entrust certificates constitute the certificate signer chain that authenticates the service’s SSL certificate. The L1C one is an intermediate signer (the immediate signer of the EBS SSL certificate).

The Entrust.netCertificationAuthority(2048).arm is the Entrust root CA signing certificate.

Q19. How do I get the public key for my clients?

A19. You can use a CA Authority that is known to us or a self-signed certificate. This should be placed in the key store and/or trust store so the private key can be used in the decryption process of the response we send.

Q20. I am having difficulty decrypting the response you sent. How is it constructed?

A20. The response is encrypted with a unique symmetric key (secret key). It is returned in the response message as the EncryptedKey->CipherData->CipherValue.

The secret key is returned encrypted, using the public key retrieved from the certificate that was used to sign the incoming message so the corresponding private key must be used to decrypt it.

All bits of the public key are used.

The secret key is encrypted using an RSA cipher with PKCS1 padding. The secret key itself is 128 bits long, but encrypts to 128 bytes then Base64 encodes to 172 bytes (octets).

The initialization vector is the first 16 bytes/octets of the cipher value in the body. To recover the IV, Base64 decode the CipherValue and take the first 16 bytes from it; the remainder is the encrypted message.

The response message encryption scheme is AES cipher with CBC block mechanism and PKCS5 padding.

Q21. I understand it is in the Technical specifications but what are the methods used for?

A21. The getTypeList method shows the functions that that operator can perform. The list method shows the associated files for the account; these are sorted in descending order by creation date (newest to oldest). The upload method provides the ministry with a file. Update changes the content of the upload file. The delete method hides the file from the ministry. The submit method tells the ministry to process the file. The download method provides a way for you to make the file a local copy. The info provides details about a file.

Q22. Do we need to exchange private keys?

A22. We presently use asymmetric keys so we have no need for your private key and you have no need for any of our private keys.

Q23. Which keys should I use for encryption/decryption?

A23. In general terms the sending party uses the receiving party’s public key to encrypt. So you send the transaction/request to us using the keys provided (our public info/keys) and we respond (send) using (in general) the public key you provided in your request.

Q24. Which keys do I use for authentication?

A24. In general terms the sending party uses the sending party’s private key to digitally sign a message. So you send the transaction/request to us signed by your private key and we authenticate using the public key you provided in your request.

Q25. Where should I place these keys?

A25. These should be added to your client’s / application’s key and trust stores.

Q26. Is there a document that explicitly outlines how authentication is accomplished?

A26. Both the EBS and the MCEDT tech spec should be used together, since the EBS spec (<http://www.health.gov.on.ca/en/pro/publications/ohip/docs/techspec_ebs.pdf> ) has some general items for all applications, and the MCEDT is the specific EBS application.

The security model headers (IDP and MSA) will not be used together. If you are using an IDP credential set, for authentication, you would not include the MSA header in the message. The EBS tech spec has an example of a SOAP header for the IDP model in appendix H (page 33).