S2S Guide for eRA Web Services

1 Background

The System-to-System (S2S) interface provides eRA Web Services as a means for systems to interact via direct requests to eRA systems (such as iEdison) to perform various business functions. The authentication and authorization technique eRA uses is to require applications that call an eRA Web Service to present a
client certificate. The following steps are required for a client system to be configured to access eRA Web Services:

1. Procure a certificate from a supported certificate provider.
2. Register the certificate with eRA.
3. Configure a calling program that uses the certificate to access eRA Web Services.

Further information regarding these steps is provided in the following sections.

2 Procuring a Certificate

Secure Sockets Layer (SSL) is supported in eRA Web Services with the following certificate providers:

- Comodo
- DigiCert
- Entrust
- GoDaddy
- VeriSign
- Thawte
- GeoTrust

The client intending to access eRA Web Services is responsible for contacting one of these providers and procuring a certificate, or reusing an existing certificate they may already have from one of these providers. eRA recommends having a unique, separate certificate installed for production and non-production environments (if needed). Consumers of eRA Web Services must keep track of the certificate expiration date, as eRA does not maintain its clients' certificate expiration information.

To verify that a certificate is valid for accessing eRA Web Services, install it using an Internet Explorer (IE) browser by following these steps:

- Ensure the certificate is located on the server where it will be installed, and know the password associated with the certificate.
- Open IE, select the **Tools** menu, and then select **Internet Options**.
- Next select the **Content** tab, and then select **Certificates**.
- Select **Import** and follow the instructions to import the new certificate into the browser.
- Once this is completed, type in the URL for the eRA Web Service you will be using; this will prompt you for your certificate. If the Web Service Description Language (WSDL) or Web Application Design Language (WADL) appears, the certificate has been successfully installed and is valid for accessing eRA Web Services. Note that the certificate will still need to be registered with eRA before it can be used to actually call a service.

3 Registering the Certificate

In order to use a new certificate with eRA Web Services please access the Manage System Account tab via the eRA User Administration Module at
https://public.era.nih.gov/ams/account/searchAccounts.do
and complete the registration process.

The serial number and the name of the certificate provider will be needed to register. After registering the certificate, verify its registration using a tool like SoapUI to call the eRA Web Service and troubleshoot any problems with the registration.

4 Configuring the Calling Program

The certificate needs to be properly installed on the local machine that will be calling the Web Service in order to pass authentication. How this is done will vary by platform, but note that for Windows-based machines, the client certificate is only available for user accounts in the Administrators group and for the user who installed the client certificate. Therefore, you must grant access to the client certificate for the user account that is used to run the calling program.

The calling program will need to be coded to use the certificate when accessing eRA Web Services. Details regarding this will vary based on the technology used in the calling program. The URL to use to access the eRA Web Service can be retrieved from the respective technical user guide of the service. All eRA Web Services are offered as standards-based web services and published via WSDL or WADL, allowing client stubs to be auto-generated.

5 Troubleshooting Service Issues

Issue Type	Error Message	Possible Cause
Connectivity Issues	UnknownHostException Not found (HTTP 404 error) SSLPeerUnverifiedException	The full URL for the Web Service is incorrect. (Verify the URL that is being called.) The Service is not operational. (Verify that the Service is operational using the WSDL in the browser or using a tool like SoapUI to verify messages.) The certificate has not been obtained or configured properly in the calling program.
Mapping Issues	SOAP response containing a HTTP 500: “Mapping doesn’t exist for certificate”	Verify that the serial number and authority in AMS match the certificate on the caller’s server.
Authorization Issues	SOAP response containing a HTTP 500: “User <XYZ> is not authorized to access this operation”	Verify that the roles in AMS have been granted for this certificate.

Issue Type	Error Message	Possible Cause
Invalid XML Issues	SOAP response containing a HTTP 500: “databinding” exception	Caller passed a request message that does not conform to the XML defined in the WSDL (e.g., required element missing, invalid data type for element). Please check the XML again and resubmit the call to the Web Service.
Unhandled Exceptions	SOAP response containing a system exception	For help resolving this issue, please contact the eRA Helpdesk with the date/time of the call, serial number, certificate authority, and the name of the Web Service.
Use of wildcard certificates not permitted	Error loading WSDL There was something wrong with the WSDL you are trying to import Error loading [https://services.external.era.nih.gov/iedison/services/officer?wsdl]: org.[apache.xmlbeans.XmlException:javax.net.ssl.SSLHandshakeException: Received fatal alert: handshake failure	The use of a wildcard certificate is not permitted