GRANTS.GOV℠

FIND. APPLY. SUCCEED.℠

APPLICANT SYSTEM-TO-SYSTEM INTEGRATION TEST PLAN

Last Updated: June 13, 2007

Table of Contents

List of Tables

Section 1. Overview

This document defines the test plan between Grants.gov and Grantee Organizations that want to use the applicant system-to-system interface to submit applications for Federal grant funding opportunities. The procedures and steps included within this document define an application-level test of the system in a production-like environment. The plan is intended to be executed by the Grantee Organization operating on its own with minimal assistance from Grants.gov.

Assumptions:

The Grantee Organization has reviewed the integration resources that have been provided at http://www.grants.gov/techlib/ApplicantWebServicesIntegration.pdf.

The Grantee Organization has installed and tested the Web Services Reference Implementation (RI) application, provided as part of the integration resources, on their test server.

The Grantee Organization will conduct initial testing within the confines of the Grants.gov test environment using test procedures and tools (e.g., the certificate provided with the RI) to establish mutual authentication.

Subsequent testing will be conducted using the Grantee Organization's actual signed certificate prior to production.

A Grantee Organization has the technical expertise with web services to take on such an endeavor. Accordingly, technical assistance provided by the Grants.gov staff shall be minimal. Requests for assistance may be forwarded to the Grants.gov Contact Center at support@grants.gov or call 1-800-518-4726.

Objectives

The main purpose of this procedure is to establish the conditions for a trusted exchange of data between Grants.gov and the Grantee Organization undertaking the test. This document provides a "road map" for Grantee Organization personnel that explains how system-to-system integration with Grants.gov will be performed using a string of system-to-system tests using web services. This procedure is also intended to clarify the expectations of the individuals who will be participating in the testing process.

The sections of the document are defined as follows:

Section 1 – Overview

Section 2 – Preliminary Steps in Preparing to Integrate with Grants.gov

Section 3 – Testing Process

Section 4 – Test Cases

Section 5 – Registering a CA Signed Certificate

Section 6 – Transition to Production

Section 7 – Acronyms

Section 2. Preliminary Steps in Preparing to Integrate with Grants.gov

The steps outlined below propose an iterative approach to a Grantee Organization's system-to-system integration with Grants.gov. The Grantee Organization should complete the following steps prior to the start of its system-to-system integration testing with Grants.gov.

Obtain and review the latest global, form, and attachment schemas posted at http://at07.apply.grants.gov/system/MetaGrantApplication.

Analyze/understand the Applicant Integration Web Services Description Language (WSDL) document that is included with the RI. The RI is posted at http://www.grants.gov/agencies/areference_implementation.jsp and describes the following four (4) operations:

1. GetOpportunityList
2. SubmitApplication
3. GetApplicationList
4. GetApplicationStatusDetail

Design, develop, and implement the SOAP *Client* Web Service components for all of the operations defined in the WSDL document (listed above).

The development of the components outlined above need not take into account security considerations such as the use of HTTPS and server certificate(s) when developing against the RI. Security concerns will be addressed when connecting to Grants.gov's secure acceptance testing environment. Detailed information on Grants.gov security for web services can be found in the *Web Services Security* document included with the RI.

Test the Grantee Organization Web Services system against the Web Services RI (available on http://www.grants.gov/agencies/areference_implementation.jsp), which provides both client and server-side (sending and receiving) implementations of the four (4) Web Service operations defined in the WSDL.

Note: The system-to-system interaction for all four (4) operations will be initiated by the Grantee Organization system.

Finally, in preparation for the “official” integration testing with Grants.gov, the Grantee Organization shall obtain a server certificate. Grantee Organizations are required to use digital certificates that have been signed by a Certificate Authority (CA) such as VeriSign or Entrust (see the *Web Services Security* document for a complete list). The Grantee Organization’s public certificate will identify their system and determine what data may be accessed via web services.

Section 3. Testing Process

This section describes the testing steps, planned schedule, and participants from both the Grantee Organization and Grants.gov personnel.

The following table describes the steps that will be taken during testing with a Grantee Organization system and the planned test duration. The test scenarios referred to in the table below are described in **Section 4**.

Table 1. Test Steps and Schedule

Step Description Participants

Step	Description	Participants
1	If you need any assistance in starting the process, please contact Vince Sprouls at Vincent.Sprouls@hhs.gov.	Grantee Organization & Grants.gov SI Team
2	Obtain a CA signed certificate and register it with Grants.gov, see Section 5. Note: Detailed information on SSL, keystores, and digital certificates can be found in the Web Services Security document	Grantee Organization & Grants.gov SI Team
3	Perform Test Scenarios 1.1 over https using the keystore provided in the RI (applicant-s2s-keystore.jks) or your CA signed certificate. This step will verify connectivity between Grants.gov and the Grantee Organization system.	Grantee Organization
4	* Using the keystore provided in the RI or your CA signed certificate, perform Test Scenarios 2.1 - 5.1 under Section 4, to test the *GetOpportunityList*, *SubmitApplication*, *GetApplicationList*, and *GetApplicationStatusDetail* web services. *	Grantee Organization

Section 4. Test Cases

The following provides the test cases for Grantee Organization system-to-system integration testing with Grants.gov. Please refer to the Grantee Organization Integration Design Specification document for detailed information about each of the functions below. The document can be found at http://www.grants.gov/techlib/ApplicantWebServicesIntegration.pdf.

As additional functionalities are added to the web services, the Grants.gov team will test these components with the Grantee Organizations that are ready at that time, and will communicate the added system capabilities to all Grantee Organizations in a timely manner.

Grants.gov has designed five (5) test cases to conduct with Grantee Organization users. These test cases will cover all functionalities scheduled for the May/June launch:

Test Case 1: Conduct Connectivity Test
Test Case 2: Retrieve an Opportunity List
Test Case 3: Submit a Grant Application
Test Case 4: Retrieve a List of Submitted Applications
Test Case 5: Get Detailed Application Status

Test Case 1 – Conduct Connectivity Test

Objective: The purpose of Test Case 1 is to validate proper web services connectivity between the Grantee Organization and the Grants.gov site over SSL with mutual authentication. The Grantee Organization IT representative should install the keystore provided in the RI (applicants2s-keystore.jks). Microsoft .NET users will need to convert the keystore to a compatible keystore format before installation (PKCS 12 is the most common format). In order to demonstrate this connectivity, the Grants.gov team created the test scenario described below. This test is standardized and the results will be the same for all Grantee Organization testers.

Test Scenario 1.1 – Perform Connectivity Test – GetApplicationList

Inputs: Grantee Organization system to issue a *GetApplicationListRequest* message with FilterType = Status and FilterValue = blank (a blank value defaults to all records) using a SOAP client that is configured to use the RI's digital certificate. The message must be transmitted using a SOAP client over **SSL** with **mutual authentication**.

Expected Result: Grants.gov system will retrieve a predefined list of applications from its database and send that list to the Grantee Organization system in a *GetApplicationListResponse* message.

Test Procedure:

1. Invoke the web services client that generates the *GetApplicationListRequest* SOAP message and sends the message to the end point.

2. The Grants.gov web services application will process the request message and will reply in one of two ways:

With a SOAP message containing a predefined list of applications
With a SOAP fault message containing known errors

Possible Reasons for Failure:

1. Your application is unable to locate the RI keystore.

Solution: Verify that the file path to the RI keystore is correctly defined in your SSL configuration.

2. The request was sent to the incorrect end point or the port number (446) was not specified.

Solution: Verify that the end point was set correctly.

3. Your certificate truststore does not contain the Entrust root certificates. Entrust is the CA that Grants.gov uses to sign its server certificates and their root certificates must be present in order to validate the Grants.gov certificates.

Solution: Obtain the Entrust root certificates from http://www.entrust.net/developer/index.cfm and import them into your application's certificate truststore or use the truststore (cacerts file) that is included with the RI.

4. The SOAP request message was improperly formatted.

Solution: Verify that the SOAP request that was sent corresponds to the message that is described in the *Applicant Integration Document.*

5. The FilterValue was improperly set to "All" or some other invalid entry.

Solution: Verify that no value was provided for the FilterValue element.

Test Case 2 –Retrieve an Opportunity List

Objective: The purpose of this test case is to retrieve a list of available opportunities via the Grants.gov web services.

Test Scenario 2.1 – Get List of Opportunities

Inputs: The Grantee Organization system will issue a *GetOpportunityListRequest* message with a CFDANumber = 00.000 (if applicable, OpportunityID and/or CompetitionID may also be used in later tests). The message must be transmitted using a SOAP client over **SSL** with **mutual authentication**.

Note: Initially, the SOAP client should be configured to use the keystore that was included with the RI (applicant-s2s-keystore.jks). Once Section 5 has been completed, the Grantee Organization may reconfigure their client application to use their own CA signed certificate/keystore.

Expected Results: Grants.gov will retrieve a list of all opportunities that correspond to the CFDA number specified in the *GetOpportunityListRequest* and return the list to the client system in a *GetOpportunityListResponse* message. The response should contain the two opportunity numbers listed below (more opportunities may be included):

APP-S2S-TEST-RR
APP-S2S-TEST-SF424

Test Procedure:

1. Invoke your web services client that generates the *GetOpportunityListRequest* SOAP message and sends the message to the end point.

2. The Grants.gov web services application will process the request message and will reply in one of two ways:

With a list of all the opportunities that match the request. For each opportunity, the following details will be returned: CFDA Number, OpportunityID, CompetitionID, OpeningDate, ClosingDate, SchemaURL, and InstructionURL.

With a SOAP fault message containing known errors.

Possible Reasons for Failure:

1. The request was sent to the incorrect end point or the port number (446) was not specified.

Solution: Verify that the end point was set correctly.

2. The SOAP request message was improperly formatted.

Solution: Verify that the SOAP request that was sent corresponds to the message that is described in the *Applicant Integration Document.*

3. Your CA reply has not been imported into your keystore*.

Solution: Please see the Web Services Security document for instructions on importing your CA Reply.

*This only applies to testers who have completed Section 5 and are attempting to use their own CA signed certificate/keystore for the first time.

Test Case 3 – Submit a Grant Application

Objective: The purpose of this test is for the Grantee Organization to submit a grant application for an opportunity available on Grants.gov. *Since this is the most critical web service, it is recommended that this test case is repeated numerous times with a variety of applications.*

Test Scenario 3.1 – Submit Application

Input: The Grantee Organization system will issue a *SubmitApplicationRequest* message that contains the application XML and any attachments. The message must be transmitted using a SOAP client over **SSL** with **mutual authentication**. The application XML contained in the body of the SOAP message should conform to one of the opportunity schema that was retrieved in Test Scenario 2.1.

Expected Results: Grants.gov will accept the submitted application and return a *SubmitApplicationResponse* message that contains a Grants.gov Tracking Number and a Received Date/Time stamp.

Test Procedure:

1. Create an XML document that conforms to one of the opportunity schemas that was returned in Test Scenario 2.1 The Grantee Organization must validate the XML against the schema, before invoking their web services client that generates the *SubmitApplicationRequest* SOAP message and sends

it to the end point.

2. The Grants.gov web services application will process the request message and will reply in one of two ways:

With a Grants.gov Tracking Number and Received Date/Time stamp.
With a SOAP fault message containing known errors.

Possible Reasons for Failure:

1. The request was sent to the incorrect end point or the port number (446) was not specified.

Solution: Verify that the end point was set correctly.

2. The SOAP request message was improperly formatted.

Solution: Verify that the SOAP request that was sent corresponds to the message that is described in the *Applicant Integration Document.*

3. The application XML was malformed or invalid.

Solution: Grants.gov will return a SOAP fault that contains and describes the validation error. The tester should correct the XML and revalidate the document against the **latest** Grants.gov schemas before resubmitting the application. The latest form schemas may be obtained from the Grants.gov website.

Test Case 4 – Retrieve a List of Submitted Applications

Objective: The purpose of this test case is to verify the retrieval of the list of submitted applications and their statuses.

Test Scenario 4.1 – Get List of Validated Applications

Inputs: Grantee Organization has successfully submitted one or more applications in Test Scenario 3.1. The Grantee Organization system will issue a *GetApplicationListRequest* message with FilterType = Status and FilterValue =**Validated** using the SOAP client over **SSL** with **mutual authentication**.

Expected Results: Grants.gov will return a list of all validated applications to the Grantee Organization system via a GetApplicationListResponse message. The received list should contain all of the applications that were submitted in Test Scenario 3.1 and successfully completed the Grants.gov validation. The received application list should also include the Grants.gov Tracking Numbers assigned to each application along with the application’s

Opportunity Number, Competition ID, CFDA Number, Received Date/Time, Grants.gov Application Status, Submission Title, and Agency Tracking Number (if applicable).

Solution: Verify that the Filter Value was properly set to "Validated" and that at least one application was successfully validated in Test Scenario 3.1. You may check for validated applications by repeating Test Scenario 1.1 to obtain a list of all of the applications and their statuses.

Note: When using the keystore provided with the RI, applications submitted by other Grantee Organizations will appear in the list returned by Grants.gov. This should not occur when using your organization's own CA signed certificate.

Test Procedure:

1. Invoke your web services client that generates the *GetApplicationListRequest* SOAP message and sends the message to the end point.

2. The Grants.gov web services application will process the request message and will reply in one of two ways:

With a list of **all validated** applications that were submitted by the Grantee Organization.

With a SOAP fault message containing known errors.

Possible Reasons for Failure:

1. The request was sent to the incorrect end point or the port number (446) was not specified.

Solution: Verify that the end point was set correctly.

2. The SOAP request message was improperly formatted.

Solution: Verify that the SOAP request that was sent corresponds to the message that is described in the *Applicant Integration Document.*

3. No results were returned.

Test Scenario 4.2 – Get List of Rejected Applications

Inputs: Grantee Organization has submitted one or more applications in Test Scenario 3.1 that include an incorrect DUNS# (e.g., 999999999). The Grantee Organization system will issue a *GetApplicationListRequest* message with a FilterType = Status and FilterValue = **Rejected with Errors** using their SOAP client over **SSL** with **mutual authentication**.

Note: When using the keystore provided with the RI, applications submitted by other Grantee Organizations will appear in the list returned by Grants.gov. This should not occur when using your organization's own CA signed certificate.

Expected Results: Grants.gov will return a list of all of the rejected applications to the Grantee Organization system via a *GetApplicationListResponse* message.

The received list should contain only those applications that were submitted and rejected in Test Scenario 3.1. The list should also include the Grants.gov Tracking Numbers assigned to each application along with the application's Opportunity Number, Competition ID, CFDA Number, Received Date/Time, Grants.gov Application Status, Submission Title, and Agency Tracking Number (if applicable).

Test Procedure:

1. Invoke your web services client that generates the *GetApplicationListRequest* SOAP message and sends the message to the end point.

2. The Grants.gov web services application will process the request message and will reply in one of two ways:

With a list of **all rejected** applications that were submitted by the Grantee Organization.

With a SOAP fault message containing known errors.

Possible Reasons for Failure:

1. The request was sent to the incorrect end point or the port number (446) was not specified.

Solution: Verify that the end point was set correctly.

2. The SOAP request message was improperly formatted.

Solution: Verify that the SOAP request that was sent corresponds to the message that is described in the *Applicant Integration Document.*

3. No results were returned.

Solution: Verify that the FilterValue was set to “Rejected with Errors” and that at least one invalid DUNS number was submitted in Test Scenario 3.1. You may check to see if any applications had been rejected by repeating Test Scenario 1.1 to obtain a list of all of the applications and their statuses.

Test Case 5 – Get Detailed Application Status

Objective: The purpose of this test is for the Grantee Organization to retrieve a more detailed description of a particular application’s status.

Test Scenario 5.1 – Retrieve Detailed Application Error Status

Inputs: The Grantee Organization system will issue a *GetApplicationStatusDetailRequest* message that contains one of the Grants.gov Tracking Numbers from the list obtained in Test Scenario 4.2. The message must be transmitted using a SOAP client over **SSL** with **mutual authentication**.

Expected Results: The Grants.gov system will return a *GetApplicationStatusDetailResponse* that contains a detailed description of why the application failed the Grants.gov validation process.

Test Procedure:

1. Invoke your web services client that generates the *GetApplicationStatusDetailRequest* SOAP message and send the message to the end point.

2. The Grants.gov web services application will process the request message and will reply in one of two ways:

With a Grants.gov Tracking Number and Detailed Error Description.
With a SOAP fault message containing known errors.

Possible Reasons for Failure:

1. The request was sent to the incorrect end point or the port number (446) was not specified.

Solution: Verify that the end point was set correctly.

2. The SOAP request message was improperly formatted.

Solution: Verify that the SOAP request that was sent corresponds to the message that is described in the *Applicant Integration Document.*

3. No detailed error messages were returned.

Solution: Verify that the Grants.gov Tracking Number submitted matches one of the tracking numbers returned in Test Scenario 4.2.

Section 5. Registering a CA Signed Certificate

This section describes the steps for registering a Grantee Organization’s CA signed certificate. Please note, as a precondition to the steps below, Grants.gov and the Grantee Organization must collaborate to create a Credential Provider test profile. The steps below should only be performed after testing with the RI keystore has been completed.

5.2 Obtain a CA Signed Certificate

1. Request a CA signature from a recognized CA. Please review the *Web Services Security* document (included with the RI) for detailed instructions on generating a certificate and a certificate signing request (CSR).

5.2 Create Applicant Account for CA Signed Certificate

1. Contact the Grants.gov SI team to request a test DUNS number for your Grantee Organization.

2. At the Grants.gov acceptance testing home page (http://at07web.grants.gov), select the *Get Started* option from the top menu navigation bar.

3. Select *Register with Grants.gov* option from the left menu navigation bar.

4. Enter a username and password on the registration screen and select the Register button. **NOTE:** The username entered **must** be the **decimal value** of your certificate's serial number.

5. The Authorized Organization Representative User Profile screen is displayed.

6. Enter the information requested on the form and the DUNS number provided by Grants.gov.

7. The registration success page is displayed. Select the Home button to return to the Grants.gov home page.

Section 6. Transition to Production

After a Grantee Organization has completed testing it should forward documented results to Grants.gov for review. Upon receiving acknowledgement from Grants.gov of successful completion of the test it should begin planning for moving their web services application into production. The Grantee Organizations should take the following steps to integrate with the Grants.gov production system:

Acquire a client digital certificate from a Certification Authority and forward a copy to Grants.gov.

Register the client certificate with Grants.gov production site (http://www.grants.gov).

Modify the Grantee Organization's web services application to point to the Grants.gov production environment (https://ws.grants.gov:446/). The production end point URLs can be found in the Grants.gov production WSDL posted at http://ws.grants.gov/wsdl/applicant/ApplicantIntegrationServices-V1.0.wsdl.

Verify on a continuing basis that the downloaded opportunity and forms schemas are the latest published. All of the latest production form schemas can be downloaded from the Grants.gov website.

Appendix A. Acronyms

Table 2. Acronyms

Acronym	Definition
CA	Certificate Authority
DUNS	Dun and Bradstreet Number
HTTPS	Hyper Text Transfer Protocol Secure Sockets
IV&V	Independent Validation and Verification
POC	Point of Contact
RI	Reference Implementation
SI	Systems Integrator
SOAP	Simple Object Access Protocol
SSL	Secure Sockets Layer
WSDL	Web Services Description Language
XML	eXtensible Markup Language

Expected Results: Windows SAVE confirmation screen appears for user-validation of files to be saved to a particular location on the user's hard-drive.

Test Scenario 1.3 – Submit Grant Application Package

Objective: Once submit button is pressed; the system shall display a submission verification message.

Inputs: User will click on SUBMIT button once all forms have been successfully completed.

Expected Results: Summary of application submission to Grants.gov confirmation receipt is displayed.

Test Scenario 1.4 – Submission Confirmation

Objective: The system shall prompt the user to verify the submitted information.

Input: Confirmation of YES/NO is required from user after receipt is displayed.

Expected Results: If YES is clicked, system will display a login screen for an ID and password to log into the system. If NO is clicked, the system will return the user back to the Grants Application Package Input Screen.

Test Scenario 1.5 – Submit Grant Application Package

Objective: The system shall prompt the applicant for login credentials (e.g., User ID & Password) prior to accepting any submission.

Inputs: User login credentials, valid ID/Password

Expected Results: APPLICATION RECEIPT screen where user can print the receipt, save the receipt or click CONTINUE ending the application process and bringing the user back the APPLY FOR GRANTS screen. Note: The user should record the Grants.gov Tracking Number for the verification of the submitted application later in the testing process.

Test Scenario 1.6 – Check Application Status

Objective: The system shall permit authorized users to obtain a list of packages that are queued for download by their agency/sub-agency.

Inputs: User accesses “For Grantors Only” option and clicks on Retrieve Submitted Applications.

Expected Results: System will display a Retrieve Submitted Application screen that contains information and the status of all the submitted applications. The user should check the Grants.gov Tracking Number that was recorded earlier against the list of the displayed applications.