

JFSC Registry API Integration Guidelines

Integration Guidelines

Version 4.0 – 1 March 2021

Project Name:	JFSC Registry API Integration Guidelines		
Date:	01/03/2021	Release:	Version 4.0
Author(s):	Denis Philippe, Jonathan Flanagan, Kevin Kerrigan, Paul Kerrigan, Gary Walsh, Stephen Brandon		
Owner:	Jersey Financial Services Commission		

Revision History

Revision Date	Previous Revision Date	Summary of Changes	Changes Marked
24/04/2017	N/A	Initial circulation.	N/A
17/11/2017	24/04/2017	Updated to support BOC17z release.	N/A
01/09/2020	17/11/2017	The document is updated to include guidance for general API service integration. The context has been increased beyond the initial scope for Beneficial Ownership and Control API services.	N/A
01/03/2021	01/09/2021	The document is updated to reflect the specific API services available within the two planned release phases in 2021.	N/A

1	INTRODUCTION	4
1.1	STRUCTURE OF THIS DOCUMENT.....	5
1.2	INTEGRATION CHECKLIST	5
1.3	CONTACT	7
2	REGISTRY API MESSAGING	7
2.1	REGISTRY API MESSAGING AND SECURITY OVERVIEW	7
2.2	CONFIGURING REGISTRY API CLIENT APPLICATIONS	7
2.3	API VERSIONING	8
2.4	API SERVICE DOCUMENTATION.....	9
2.5	STATIC API SERVICES	9
3	REGISTRY API APPLICATION PROCESS	10
3.1	SUBMIT APPLICATION FORMS	11
3.2	SIGNING CERTIFICATE REGISTRATION	11
3.3	REGISTRY CLIENT API KEY	12
3.4	APPLICATION FOR CLIENT SIGNING CERTIFICATE	12
3.5	INTEGRATION TESTING.....	16
4	API SERVICE CALLS	18
4.1	REQUEST LIMITS.....	18
4.2	RESPONSE RATES.....	18

1 Introduction

The purpose of this document is to provide regulated service providers and technology providers with guidance on how to integrate with the Registry Application Programming Interface (“API”) channel.

The Registry API channel will provide an alternative route for regulated service providers to interact with the JFSC Companies Registry.

The role of the Registry API is to provide an efficient and secure channel for regulated service providers to exchange information with the JFSC and to ultimately ensure that the central registers remain current and accurate.

The Registry API roadmap plans for the phased implementation schedule with two releases planned for 01 March 2021 and 01 April 2021. On 1 March 2020, the Registry will deploy the following API services:

#	API Service	API Purpose
1	GetEntityInformation	Retrieve full entity data (public and private)
2	AmendAssociatedParty	Amend the associated parties for a registered entity
3	FileConfirmationStatement	File a confirmation statement / annual fee
4	ChangeRegisteredOffice	Change the registered office address
5	AmendShareCapital	Amend the share capital structure for a registered entity
6	CheckName	Check the register for similar reserved names or entity names
7	CheckSubmissionStatus	Check the current status of a submission
7	GetCountries	Retrieve a list of countries with their ISO 3166-1 alpha-2 code
9	UploadAttachment	Upload a file attachment for reference in subsequent filings

A subsequent release phase is scheduled for 1 April 2021 and will see the following API services deployed for Regulated Service Provider use:

#	API Purpose
1	Reservation Company
2	File Special Resolution - Dissolution
3	File Special Resolution - Change of Memorandum
4	File Special Resolution - Change of Article
5	File Special Resolution - Change of Name
6	File Prospectus
7	Correspondence

The Registry API security model is configured to accept SOAP based messages that are secured using message level encryption. This communication protocol ensures that information submitted to the Registry is secure, confidential and authenticated.

This document should provide the target audience with:

1. Details of the Registry API service, security model and how messages are securely exchanged with the JFSC
2. Detailed information regarding the process to apply for and receive the required security credentials to access the Registry API

3. The process of gaining access to the JFSC Registry API test environment and progressing to the Registry API production environment
4. Information regarding the structure of message schemas
5. The applicable business rules and validation that will be applied to messages during the processing of submissions across the Registry API
6. Information regarding the available channels to seek additional support and information during integration activities

The JFSC is mindful that external third parties may build middleware tools to provide an alternative option for regulated service providers that do not have the time or resource available to directly build their own API solutions.

The JFSC is unable to endorse nor promote any middleware provider; however, we will be providing external service providers with access to the Registry API Zoho Portal. Any further enquiries under this heading should be directed to the middleware providers directly.

It is important to note that the infrastructure and API security model that was deployed in 2017 to support the population of the central register of beneficial owners and controllers remains current and provides the base for the Registry API.

New message schemas for each service will be provided (via the new Zoho collaboration portal) where external service providers will be invited to review and provide input. The existing BOC API service schema will be updated, and we are not intending on providing a backward compatible version of this schema due to the significant changes that will be present in the message schema.

Further information will be provided on the schedule for release and the different infrastructure environments that will be made available for testing and sign-off.

1.1 Structure of this Document

The main sections of the document are highlighted as follows with the specified objective:

Section	Objective
Introduction	Provides an introduction and overview of the Registry API services including an outline of the future API delivery schedule.
Registry API Technical Summary	Provides a technical summary of the Registry API component including the underlying messaging security model and the API services available.
Registry API Application Process	Provides detailed guidelines on the application process to achieve access to integrate with the Registry API.

1.2 Integration Checklist

The following checklist is provided as an aide memoire to guide the regulated service providers and the wider technology community with their API integration preparation.

#	Item	
1	Business has undertaken a readiness assessment with respect to the format and quality of data held internally	☐

2	Regulated Service Provider understands the Registry API services available and has defined the architecture and strategy of how they will integrate with their business processes and back office IT systems	☐
3	Regulated Service Provider understands the underlying Registry API security model; specifically, the security elements (Registry Client API Key, Client Signing Certificate, Registry API Root CA certificate) that they need to procure in order to integrate and transmit test submissions across the Registry API	☐
4	Regulated Service Provider understands the application process to apply for the pre-required security elements (Registry Client API Key, Client Signing Certificate, Registry API Root CA certificate)	☐
5	Regulated Service Provider has reviewed, accepted and submitted to the Registry an Application form and Registry API Terms of Use signed by an authorised individual	☐
6	Regulated Service Provider application is successfully accepted by the JFSC and the Regulated Service Provider receives a. Link (URL) to apply for Test Client Signing Certificate and Test Registry API Root CA certificate b. Test Registry Client API Key	☐
7	Regulated Service Provider successfully completes the process and receives the Client Signing Certificate and the Registry API Root CA certificate	☐
8	Regulated Service Provider completes integration of their API client (or integration with third party middleware solution) and communicates to Registry that they are ready to undertake integrity testing	☐
9	Regulated Service Provider successfully completes integration testing and automatically receives a. Link (URL) to apply for Production Client Signing Certificate and Production Registry API Root CA certificate b. Production Registry Client API Key	☐
10	Regulated Service Provider is live on the Registry API Production environment and commences live filings with support from the JFSC as appropriate	☐

It is also appreciated that regulated service providers may request access to the JFSC test environment to further evaluate the API channel and related services.

In the scenario that an Intermediary or Third-Party Middleware Provider requires access to implement their Registry API solution, the JFSC will accept applications for access to the JFSC Registry API test environment only. All applications for access to the JFSC Registry API production environment must be requested directly by the Regulated Service Provider.

1.3 Contact

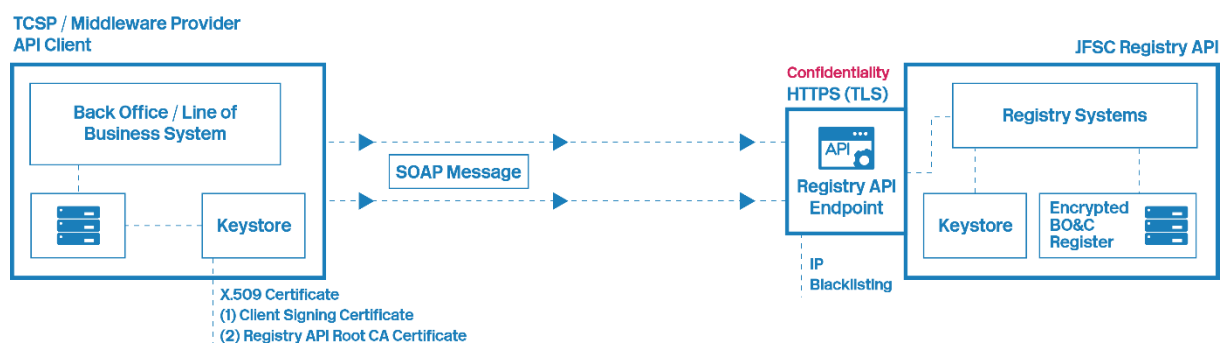
Any questions or clarifications regarding this document should be directed to the Registry API team by email at registryAPI@jerseyfsc.org

2 Registry API Messaging

2.1 Registry API Messaging and Security Overview

The Registry API accepts SOAP messages that are secured using message level encryption. This protocol ensures that the information that is sent to the Registry is secure and confidential and cannot be intercepted or altered.

In order to communicate with the Registry API you must be capable of sending and receiving SOAP messages that are secured using x.509 certificates.



The above diagram depicts the high-level interaction between a client and the Registry API. Each client will be required to install both a Client Signing Certificate to digitally sign the messages sent to the Registry and a Registry API Root CA certificate to encrypt messages being sent to the Registry API.

All communication with the Registry API will be over a secure HTTPS channel (using TLS 1.2). This will provide additional levels of security for the transmission of messages between the client and the Registry API.

The process of obtaining the required certificates is documented in section 3.

2.2 Configuring Registry API Client Applications

It is outside the scope of this document to provide guidance on the approach and strategy to implement your API Client, however the below guidance is provided to support you with the configuration of your API Client Application to comply with the Registry API security model.

To connect with the API, allowing for message encryption and digital signing, the application must be properly configured. The following configuration is an example of the configuration for a .NET application.

```

<system.serviceModel>
  <bindings>
    <wsHttpBinding>
      <binding name="WSHttpBinding_ISubmissionWebServices" maxReceivedMessageSize="2000000">
        <security mode="TransportWithMessageCredential">
          <transport clientCredentialType="None" />
          <message clientCredentialType="Certificate" establishSecurityContext="false" />
        </security>
      </binding>
    </wsHttpBinding>
  </bindings>
  <client>
    <endpoint address="https://myreg-stg.api.jerseyfsc.org/SubmissionWebServices.svc"
      behaviorConfiguration="customBehavior" binding="wsHttpBinding"
      bindingConfiguration="WSHttpBinding_ISubmissionWebServices"
      contract="myregSubmissionAPIServices.ISubmissionWebServices"
      name="WSHttpBinding_ISubmissionWebServices" />
  </client>
  <behaviors>
    <endpointBehaviors>
      <behavior name="customBehavior">
        <clientCredentials>
          <clientCertificate findValue="d9edabcdefg012334oiuyth83737mnbvcx" x509FindType="FindByThumbprint"
            storeLocation="LocalMachine" storeName="My" />
          <serviceCertificate>
            <authentication certificateValidationMode="ChainTrust" revocationMode="NoCheck"/>
          </serviceCertificate>
        </clientCredentials>
      </behavior>
    </endpointBehaviors>
  </behaviors>
</system.serviceModel>

```

The endpoint behaviour section is configured to locate the client certificate based on the certificate's subject name. The certificate can be located using multiple different values such as thumbprint, issuer name etc.

Once properly configured to locate the client certificate, the application will be able to connect to the API.

If you require any further assistance in completing the above steps, please contact a JFSC API team member at registryAPI@jerseyfsc.org



2.3 API Versioning

The API will be versioned using semantic versioning. This will mean that each release will take the format: MAJOR.MINOR.PATCH.

Type	Description
MAJOR	When a non-backward compatible API change has been released.
MINOR	Backward compatible changes (new functionality or removed functionality) have been made to the API.
PATCH	Backward compatible bug fixes have been applied to the API.

Our principle is that the previous two versions of the API will be maintained. The time that each version will be maintained will be dependent on the nature of the change. For example, a breaking change that requires new information to be added to adhere to a policy change. The previous version will only be maintained for a limited period, to allow clients to upgrade, without allowing too many invalid submissions.

Before any change to the API, clients will be presented with a set of release notes. The updated API and documentation will be made available for integration testing in the test environment before it is pushed into the production environment.

2.4 API Service Documentation

Full details on the information required for each of the API services will be provided in the 'JFSC Registry API Manual' available on **Zoho > Manuals**

2.5 Static API Services

To assist with initial development and integration with the API services a static 'stub' endpoint will be made available for API consumers. A small number of sample services will be exposed with example 'request' and example 'response' messages. The static endpoint does not require the use of a client certificate or an assigned API key to use its services.

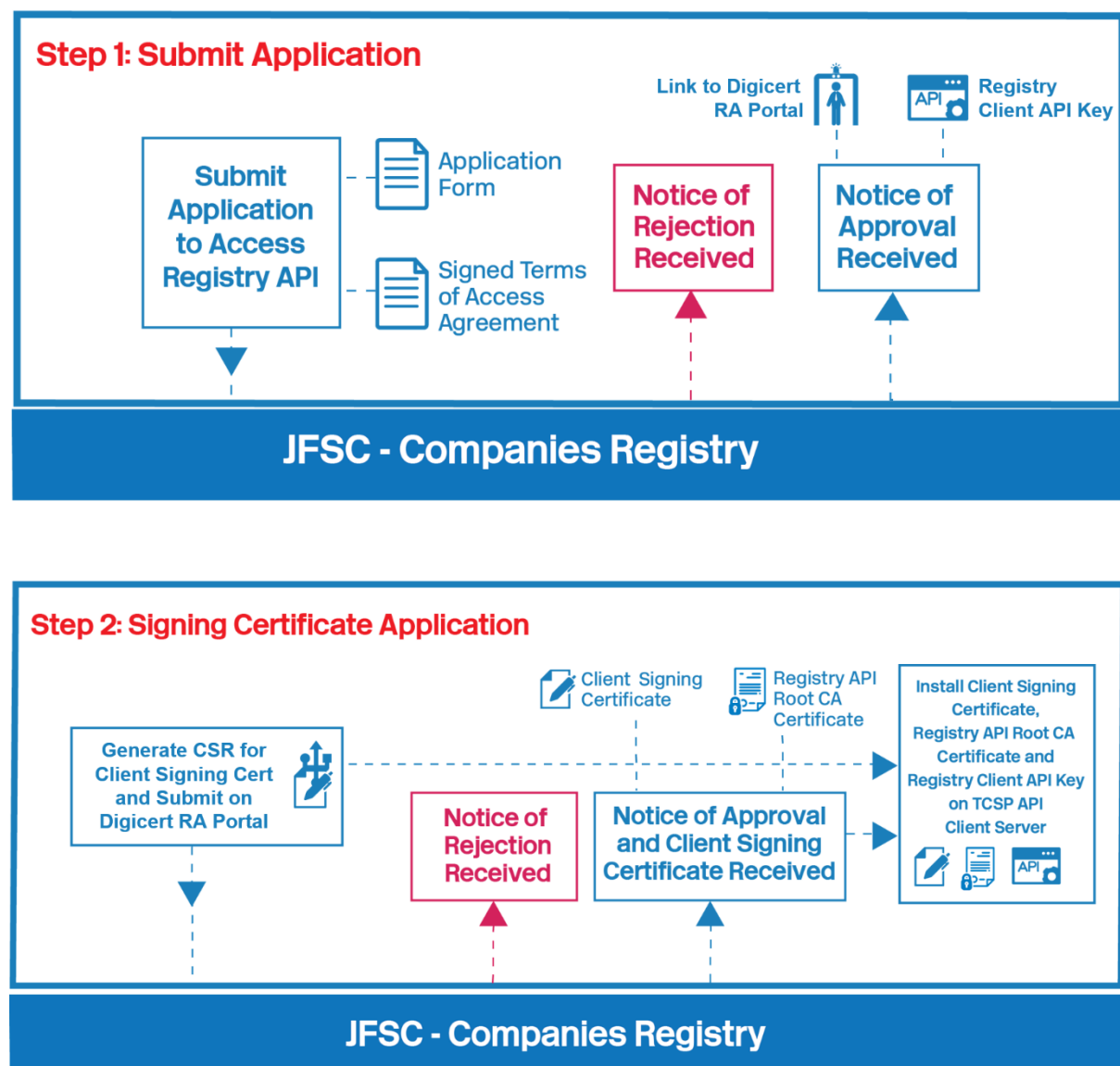
3 Registry API Application Process

This section outlines the process of applying for access to integrate with the Registry API.

There are two distinctive steps involved in the API application process:

Step 1 comprises of the Regulated Service Provider/Middleware provider submitting an application form requesting access to the Registry API. This includes the submission of the signed Application Form in agreement with the Terms of Use documentation. Step 1 results in a Client Registry API key being sent to the Regulated Service Provider and a link to commence Step 2.

Step 2 relates to the application to receive a Client Signing Certificate. The Regulated Service Provider/Middleware provider submits this application online via a Certification Authority partner. Upon successful approval, both a Client Signing Certificate and the Registry API root CA certificate are sent to the Regulated Service Provider/Middleware provider.



3.1 Submit Application Forms

The applicant must agree to comply with the Terms of Use agreement and submit the application form to the JFSC Registry. Both documents are available for download on the Registry API Zoho portal.

1. Registry API Application Form (for Technology Service Providers)

The application form requires the applicant to provide mandatory organisational and IT representative details to enable the JFSC to validate the authenticity of the applicant. The application form will be available for download on the Registry API Zoho portal.

2. Terms of Use Agreement

The Terms of Use Agreement governs the Regulated Service Provider Registry API access and defines how they should interact with the Registry API. This agreement will be available for download on the Registry API Zoho portal.

The application form must be signed by an authorised signatory and emailed to registryAPI@jerseyfsc.org where the Registry team will review, record and validate the application.

A successful applicant will be notified via the email address provided on the application form. This email notification will also include a URL link to register for a TEST Client Signing Certificate on the Digicert RA (Registration Authority) Portal.

An unsuccessful applicant will be notified via the email address provided on the application form with the justification for rejection and appropriate instructions on how to proceed.

The Regulated Service Provider applicant must agree to comply the Terms of Use agreement and complete Part D, Registry API Channel, of the myRegistry Application Form and submit the application form to the JFSC Registry. The applicant will be required to provide the technical contact details of API development within their organisation.

3.2 Signing Certificate Registration

The successful applicant opens the URL link provided (ref. 3.1 above) and registers for a TEST Client Signing Certificate on the Digicert RA Portal by completing an online registration form outlined in section 3.4.

The JFSC API Administrator will authorise the applicants request should the required information be satisfactory and match the criteria provided in the application form.

A successful applicant will receive an email containing the TEST Client Signing Certificate and a Digicert Root Certificate which they will install on to their server as outlined in section 3.4.

An unsuccessful applicant will receive an email advising that their certificate request has been declined and a JFSC API Administrator will contact them with further information.

3.3 Registry Client API Key

The applicant will receive an encrypted email containing a Registry Client API Key that uniquely identifies the TSCP.

A JFSC API Administrator will contact the applicant by phone (on the number provided on the application form) with the password to decrypt the contents of the email.

The applicant adds the Registry Client API Key to the Regulated Service Provider's software for identification of each submission.

In the email, the Registry Client API key will be displayed in the following format:

Z3cMBddEcawCVBGH3erfs3.56W2xcVfVFqDrDRGb3fdseVBASSd

3.4 Application for Client Signing Certificate

In order to connect and communicate with the Registry API, you must first obtain a client certificate. This will be used to digitally sign your messages as they are sent to the API.

Complete the following steps to configure the Client Certificate:

1. Generate a Certificate Signing Request (CSR) on the server which will connect to the API. The byte size of the CSR must be **2048**
2. Visit the URL provided by the JFSC in the application approval email
3. Complete the application form (see the following section for help in completing the form)
4. Once the application for a certificate is approved by the Registry, you will receive a notification email to the email address provided in the application
5. Copy the contents of the email into new text files and name them with extension **.p7b** and place the files on the server which will connect to the API
6. Open the certificate management service
7. Import the Registry Client API key (as provided in the email) into the Personal certificate store
8. Import the Registry API Root CA certificate (as provided in the email) into the Trusted Root Certification Authorities store
9. Configure the client application settings to be able to locate the certificate required to communicate with the API

The following section details the steps involved in the Client Certificate application process.

The URL provided is accessible only through Internet Explorer, Microsoft Edge or Mozilla Firefox internet browsers. Once on the application page, you will be asked to provide the following information.

Field Name	Description
DNS Name*	(Mandatory field) This value should be set to "localhost".
Additional DNS Names	This field can be left blank; it is not required.
Common name*	(Mandatory field) Provide a clear description of the organisation and the level of the certificate. E.g. "Organisation name – Test Certificate"

Department	This field can be left blank; it is not required.
Email*	(Mandatory field) This is the email address the completed certificate will be sent to. Please ensure this is correct.
Comments	This field can be left blank; it is not required.
CSR*	(Mandatory field) You must provide the CSR as created in section 3.2.1. You can paste the value or upload a txt file with the contents of the CSR. The CSR should have been generated on the machine which will be used to connect to the API.

English ▼

Enroll:
Enrollment information
Next steps

Verify your information

Verify that the information associated with your certificate is correct, and complete any required fields.

* DNS Name

?

Additional DNS Names

Enter one or more DNS names separated with a "," as a delimiter.

* Common name

Department

Multiple Certificates Allowed

* Email

Note: Email address is case-sensitive. It must exactly match the email address configured in your email client.

* First Name

* Last Name

* Phone

Comments

?

☒ Paste CSR ☐ Upload CSR

* Paste CSR below: ?

If you have any questions, contact JFSC Registry API Team

RegistryAPI@jerseyfsc.org

* Required Information

Continue

Once the certificate application is approved by the Commission, you will receive an email from the PKI service to the email address provided. The email will contain the content of the following:

- Client Signing Certificate
- Registry API Root CA certificate

The following is the Client Signing Certificate including its issuing chain:

-----BEGIN CERTIFICATE-----

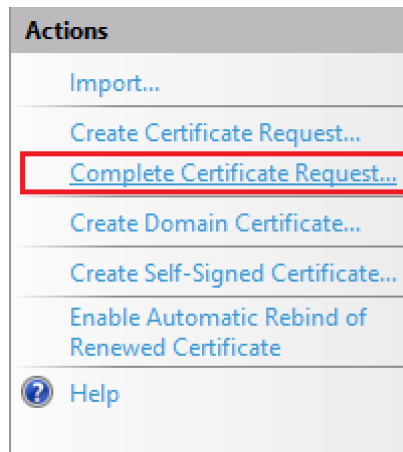
MIAGCSqGS1b3DQEHAqCAMIACAQExADALBgkqhkiG9w0BBwGggDCCBo0wggV1oAMC

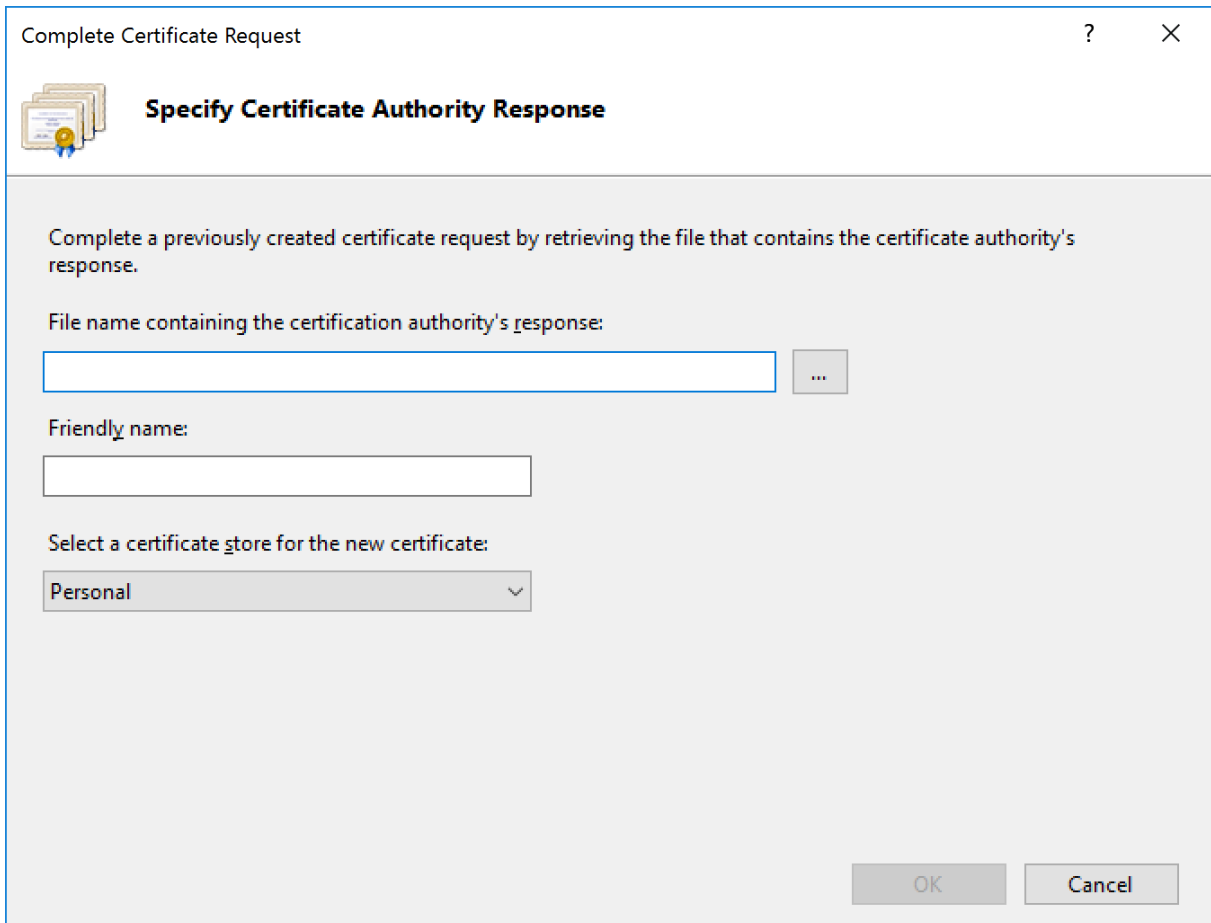
```
AQICECphUpOQgkDrsoU4zgBkUVgWDQYJKoZlHvcNAQELBQAwYjELMAkGA1UEBhMC
VVMxHTAbBgNVBAoTFFN5bWFudGVjIENvcnBvcnF0aW9uMTQwMgYDVQQDEytTeW1h
bnRIYyBNYW5hZ2VkiFBLSSBPbmtpbmUgVGVzdCBEcml2ZSBSb290MB4XDTE3MDQx
ODAwMDAwMFoXDTE3MDUxODIzNTk1OVowezEhMB8GA1UEAwwYRVJTTCBTaWduaW5n .....
```

-----END CERTIFICATE-----

The entire content of this certificate should be saved into a text file and saved with a .p7b extension type.

If the CSR was created using IIS, then you should open the “Server Certificates” module and click on the “Complete Certificate Request” option.

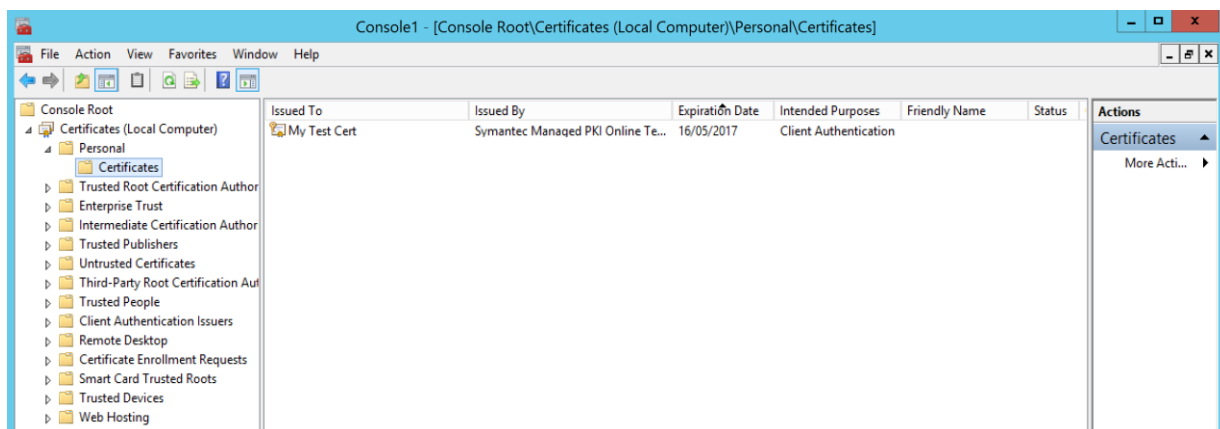




The dialog box is titled "Complete Certificate Request" and contains a sub-header "Specify Certificate Authority Response" with a certificate icon. The main text reads: "Complete a previously created certificate request by retrieving the file that contains the certificate authority's response." Below this are three input fields: "File name containing the certification authority's response:" with a text box and a browse button (...), "Friendly name:" with a text box, and "Select a certificate store for the new certificate:" with a dropdown menu currently showing "Personal". At the bottom right are "OK" and "Cancel" buttons.

Provide the p7b file (as created from the email) in the first field of this screen.

A friendly name should be provided for the certificate. This should be noted as it will be required to retrieve the certificate when connecting to the API.



3.5 Integration Testing

Once the test certificates and Client Registry API key are installed and development is complete, the applicant is required to notify the JFSC API Administrator on registryAPI@jerseyfsc.org and a suitable testing schedule will be agreed.

The applicant will be provided with a number of test cases to validate the message format and data mappings of their submissions.

If testing is found to be unsuccessful the applicant will be advised, and a retest will be scheduled.

If testing is successful, the applicant will receive a confirmation email from the JFSC Administrator that the test cases were successful. The email will contain a new link to register for a Production Client Signing Certificate on the Digicert RA Portal and it is installed on Production servers as per the same process defined in section 3.2.

The applicant is now ready for production level submissions.

If you require any further assistance in completing any of the above steps, please contact a JFSC API team member at registryAPI@jerseyfsc.org



4 API Service Calls

4.1 Request Limits

The Registry API will apply a restriction to the rate of accepted submissions. This rate has yet to be determined and will be published at a later date. Attempts to increase the concurrency of the submission calls will be ignored by the API.

4.2 Response Rates

The proposed service level agreement for the service calls are set-out in the following table.

Service Name	Maximum Time	% Response Rate
All synchronous service calls	5 seconds	95%