iConnect 198625 Design Approach - Rework Authentication Scheme for API

Project Overview

Rework Authentication scheme for APIs to be more granular and support multiple certificates in 1 org. We have a few use cases where the client needs the ability support multiple authenticated identities into our API for a given instance. For example, you could have one authenticated identity have access to distributor's embedded API and another identity have access to Analytics API.

Authentication is certificate based and it is 1 certificate per organization. Today, because we only have 1 cert, we cannot limit one vendor from accessing the site without changing the cert for everyone. This is problematic when you can have multiple firms using the same API certificate and for whatever reason one of the firms needs to be prevented from accessing FL or from a particular service within FL.

In this project we are identifying in one place the list of certs that will be used for authentication within the system. This is a very similar layout to how we capture in one place 3rd Party authentication data. With each cert we provide a backup cert so they can self-service the renewal without involving us to coordinate the switch to the new cert. We will move the SSO cert info here to keep all cert definitions in one place. How the cert is used is slightly different in a SSO request but the need for a primary and a secondary is needed, and having a single place to view cert usage makes sense

Requirements / User Stories

Create a new table to support multiple certificates per supported services

Today in the Admin/Organization/Security, FL stores the IDP certificate, IDP backup certificate, and the web service certificate. There is only place to store 1 web service certificate and it is used by all services. This task will create a new table to store the supported services & add the services that are supported. The supported services would be available in a multi-select field. New supported services will need to go through the base team to be supported and added to the table.

We will need to have the ability to define the areas the certificate can access (SSO, web services, IDP, API, Salesforce, etc.).

Multiple services can still be supported under the same certificate but this allows for the flexibility to support different certificates per access point.

Supported Services should include the following:

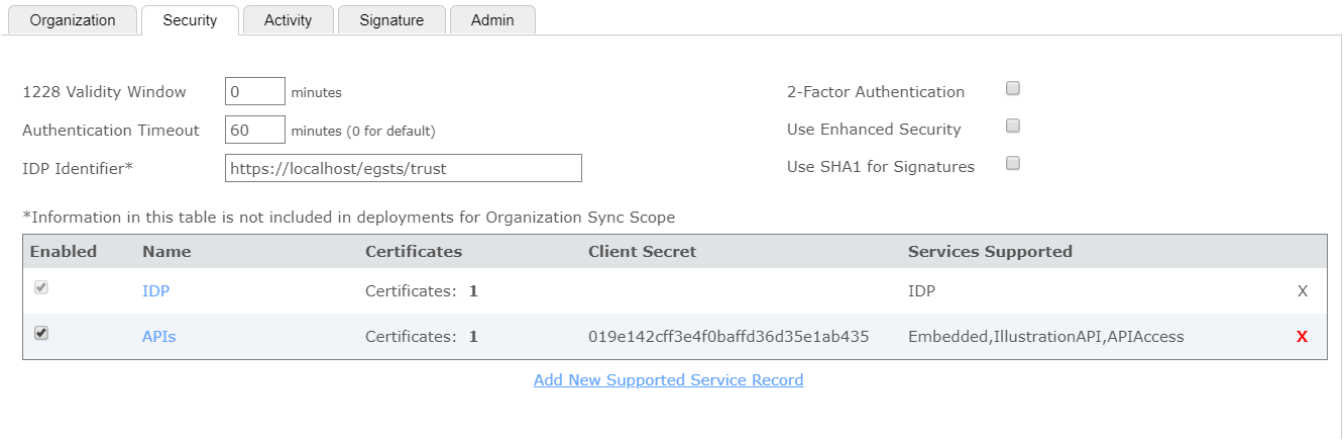
IDP

Embedded

Illustration API

API Access

The table will allow a naming/description (which will be editable text field), then a certificate link, and then tell FL what services that cert can access. (supported services table will be managed at Org level by IT)



Acceptance Criteria

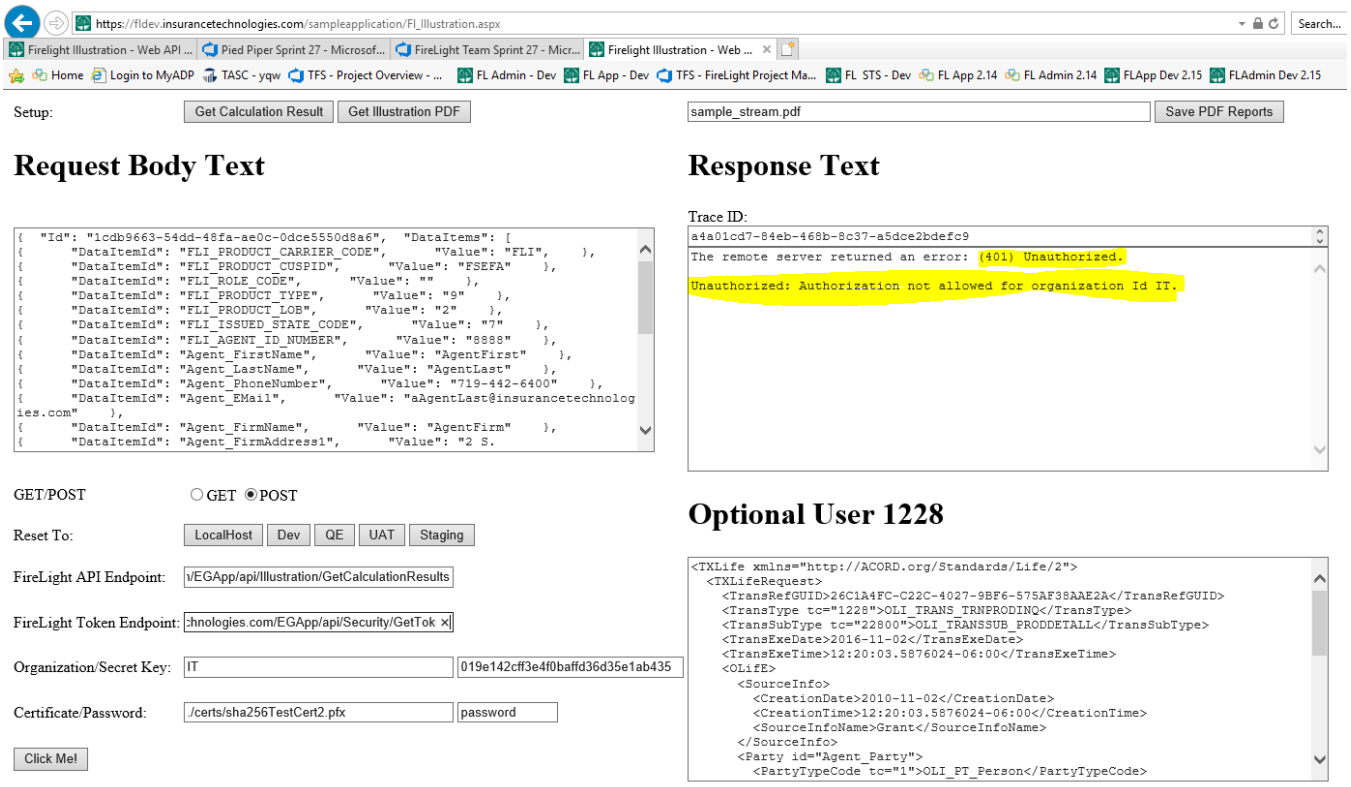
- Verify that the table in the Organizations tab is showing multiple certificates for the supported services.
- The supported services are available in a multi-select field.
- Have the base team add a new supported service (embedded) and ensure it is available in the supported services drop-down.
- The table will have areas to define the description, load the certificate and/or backup cert, and define the supported service.

Set EGAuth to give certain claims-based tokens based on certificate given

When we get a set of credentials for a client in our EGAuth system, we need to give out tokens that have claims restricted to the 'Services Supported' based on cert used in the credentials (match it up to the configuration of the cert table). Testing for this will require a dev, who will need to inspect the token via the debugger or something in order to verify the claim on the token.

Test screen - the expected result

Without illustration certificate configurated for the org IT ('Web API' only at this moment, and I will add illustration back on after my testing) the illustration service call won't be authorized.



Acceptance Criteria

- Set up a cert table entry containing a cert for a Services Supported value of 'Web API' only
- Send in a request to the token service using the above cert
- Verify that the token has the claim necessary

Move existing service certificates to reside under the new certificate table

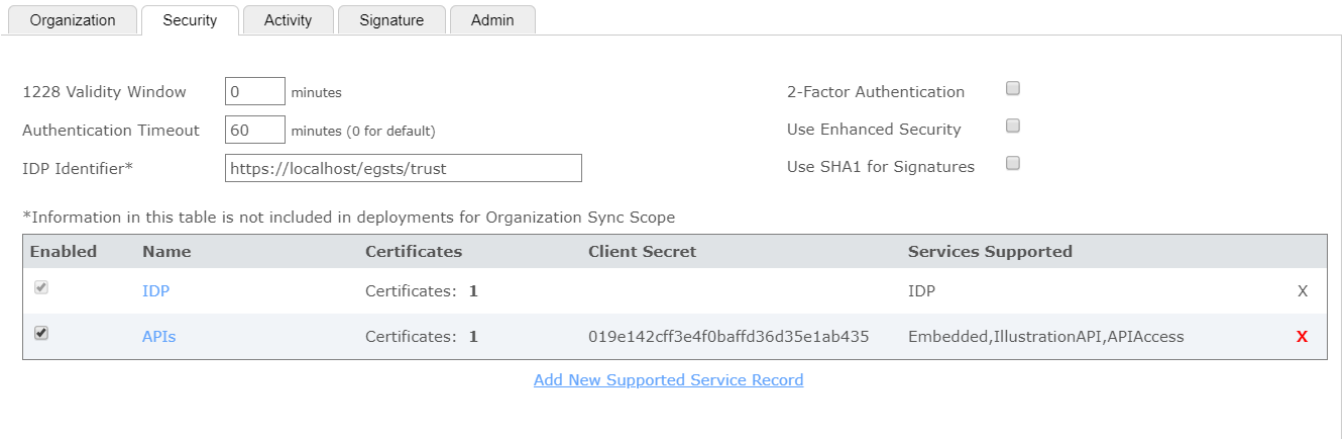
Client will already have certificates in the org table for services like IDP, CRM certs and embedded. These will need to be moved to the new table that will contain all of the services supported and their certificates.

Please note that the IDP is not editable.

Acceptance Criteria

- Verify that table is populated with Primary and secondary existing certificates
- The other services like Web API will be associated with the CRM functions. Embedded will have its own service and the certificates will now reside under this location.

- Note what was originally posted for the certificates, and verify they are showing in the new table
- Verify all current services (including SSO) are showing in the table
- Note what was in the certificates before the addition to the table
- The services for SSO will reside under IDP and are not editable.



Change SSO Logic to use new IDP Cert Location (in new table)

Acceptance Criteria

- SSO certs work with new database table location

Set Web API to only work with tokens that have relevant claims

Make sure Web API only works with tokens that have 'Web API' claims in them. This will need a dev to test.

Acceptance Criteria

- Tokens that only have Web API claims must only work with Web API.
- Tokens that do not have Web API claims must not work with Web API.

Set Embedded to only work with tokens that have relevant claims

Make sure Embedded API only works with tokens that have 'Embedded' claims in them.

Acceptance Criteria

- Tokens that only have Embedded claims must only work with Embedded.
- Tokens that do not have Embedded claims must not work with Embedded

Add List Profile to drive Security visibility

Add in the ability to limit the supported services based on licensing per organization. In order to achieve this, we will need to add in a list profile to control this feature. The services will be enabled or disabled based on client license, but will be visible.

Default will be IDP visible and selected, others will need to be added.

Acceptance Criteria

- Vendor rights login will show all supported services and be editable
- IDP will be defaulted as the only service selected for client environments
- All supported services will be either enabled or disabled based on license of clients.
- Add profile list into DB table ListProfile to enable the service in Supported Services Configuration view -
- <ArrayOfSupportedServices xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
- <SupportedServices>IllustrationAPI</SupportedServices>
- <SupportedServices>IDP</SupportedServices>
- <SupportedServices>Embedded</SupportedServices>
- </ArrayOfSupportedServices>

Move Web Service Token Secret to Supported Service level

Need to move the Web Service Token Secret from the organization level to the supported service level

Acceptance Criteria