Virtual Identity Provider

Definition

A single identity provider usually offers different profiles or service levels to diffeferent service provider. To be able to define this behavior, any Identity Provider can be split into many virtual identity providers. Those identity providers will be served by the same actual identity provider, but they will have different profile configurations.

Standard attributes

Identification

- **publicID**: unique name to identify the identity provider.
- **Name**: user friendly name to identify the identity provider.
- **Organization**: company name of the external IdP.
- **Contact**: email address of the external IdP.

Service configuration

- **Metadata**: the Metadata for an Identity Provider defines how this Identity Provider delivers its service:
  - Which security algorithms does it support.
  - The public portion of it's signing and encrypting keys.
  - The SAML protocols does it support.
  - The URL of each SAML protocol endpoint.
  - Contact information.

Leave it blank as Soffid IdP will fulfill it for you.

SAML Security

- **Public key**:
  - **Generate public/private key**:
    - **Delete public/private key**: allows you to delete the public/private key generated previously.
    - **Generate PKCS10**: generates a PKCS10 file (Certification request standard)

    - **Upload PKCS12 file**: allows you to upload a PKCS#12 file. That file must contain the private and public kesus and the server certificate as weel. Mind that PKCS#12 file use to be protected by a PIN.
- **Certificate chain**: text certificate chain created with one of the previous options.

Authentication

- **Authentication methods**: matrix to define the authentication methods that will be required to successfully authenticate the user. Each row indicates the first authentication method, and each column indicates the second factor to use.
- **Adaptive authentication**: that option allows you to add additional authentication matrix which will be run when the condition defined was comply.
    - **Description**: rule description to identify it.
    - **Condition**: script to enable that rule. The result of the rule must be true or false.

      There are some available vars to create the condition. You can visit the Condition for Adaptive authentication page for more information and some examples.
    - **Matrix**: to define the authentication methods that will be required to successfully authenticate the user. Each row indicates the first authentication method, and each column indicates the second factor to use.

Advances authentication

- **Allow user to recover password**: if it is checked (selected value is Yes), and the password recovery addon is installed, the user will be allowed to execute the password recovery mechanism.
- **Allow user to self-register**: if it is checked (selected value is Yes), the user will be allowed to register itself. This option sends an email to the user to verify the email address is correct, and then lets the user to enter a new password.
- **Registet identities identified by external IdPs**: allows Soffid IdP to automatically register a new identity when a user authenticates with a third-party IdP, and this identity does not exist yet in Soffid database. Furthermore, at the third party IdP configuration page, one can tune how this identity is going to be created.

Profiles

A profile is a protocol implemented by the Identity Provider. There are some accepted protocols, those allows a custom config dependent on the selected profile

- OpenIDProfile
- SAML1ArtifactResolutionProfile
- SAML1AttributeQueryProfile
- SAML2ArtifactResolutionProfile
- SAML2AttributeQueryProfile
- SAML2ECPProfile

- SAML2SSOProfile

> You can visit the Profiles chapter for more information about each one.

Service Providers

It will be necessary to bind any service provider to the virtual identity provider. When no such bind exists for a service provider, the actual identity provider profile configuration applies.

Revision #14
Created 8 September 2021 09:43:19
Updated 20 June 2022 10:36:39