SSO SAML prerequisites

Document version	**V01**		
Date(s)	Creation of the document	30-05-2022	Clément Cazeaux IT Engineer
	Document Review		
Document status	**UPDATED**		
Confidentiality	**C1**		

Table of contents

Objective

The purpose of this document is to define the prerequisites for setting up an SSO protocol between SKINsoft and its customers.

Protocol

The recommended protocol is saml-v2.

Terms used

IdP: IDentity Provider: the interface with which the SP communicates to authenticate the user. In principle, it is based on a directory of users and is managed by the customer.

SP: Service Provider: the application offering services to authenticated clients. In this case, TRYPHON.

Correspondence between AD and S-Museum

The element used to map an SSO user in the directory to a SKINsoft user in its database is :

Entity	Link
Customer	NameID (email or UPN)
SKINsoft	User.username

SKINsoft configuration requirements

The login.sso-domains text field is used to add new authorised domains, as with frontend.domains. The domains (with https://) of the IdPs must be entered here. Several domains can be added.

The *login.saml-providers* key is used to configure the various IdPs. An IdP is configured using the following sub-fields:

1. registration-id: a simple name used as an access point for the IdP in the TRYPHON API
2. provider-name: the name displayed in the Frontend when the authentication method is selected
3. idp-metadata: URL to the IDP metadata file. Ideally, this should be a local file, but HTTP is also supported.
4. private-key (optional): if you want to sign messages from the TRYPHON Service Provider, enter the local private key file here

5. certificate (optional): if you want to sign messages from the TRYPHON Service Provider, enter the local public certificate file here
6. entityId (optional) : To be specified if used.
7. assertionConsumerServiceLocation (optional) : To be specified if used.

Example of a SKINsoft configuration file:

```
login:
 sso-domains: https://stubidp.sustainsys.com, https://example.com
 saml-providers:
  # IdP de test, sans mots de passe
  - registration-id: sustainsys
    provider-name: SustainSys
    idp-metadata: https://stubidp.sustainsys.com/Metadata
  # IdP avec metadonnees et certificats locaux
  - registration-id: example2
    provider-name: Secured IdP
    idp-metadata: file:///home/skin/sso/metadata.xml
    private-key: file:///home/skin/sso/privateKey.key
    certificate: file:///home/skin/sso/certificate.crt
```

Access account for SKINsoft

There are two possible solutions:

- either accounts are created in the IDP directory and SKINsoft does not have login/password access.

- either SKINsoft can be accessed by login/password only for administration accounts and there is no need to create accounts in the IDP.

SKINsoft uses the script generate_saml_cert.sh :

1. Its own private key stored on the SKINsoft server
2. Certificate request (and/or self-signed certificate)
3. Metadata file with certificate

The SP metadata file generated by SKINsoft is optional; it enables the IDP team to better configure the server, but generally the IDP metadata file is sufficient.