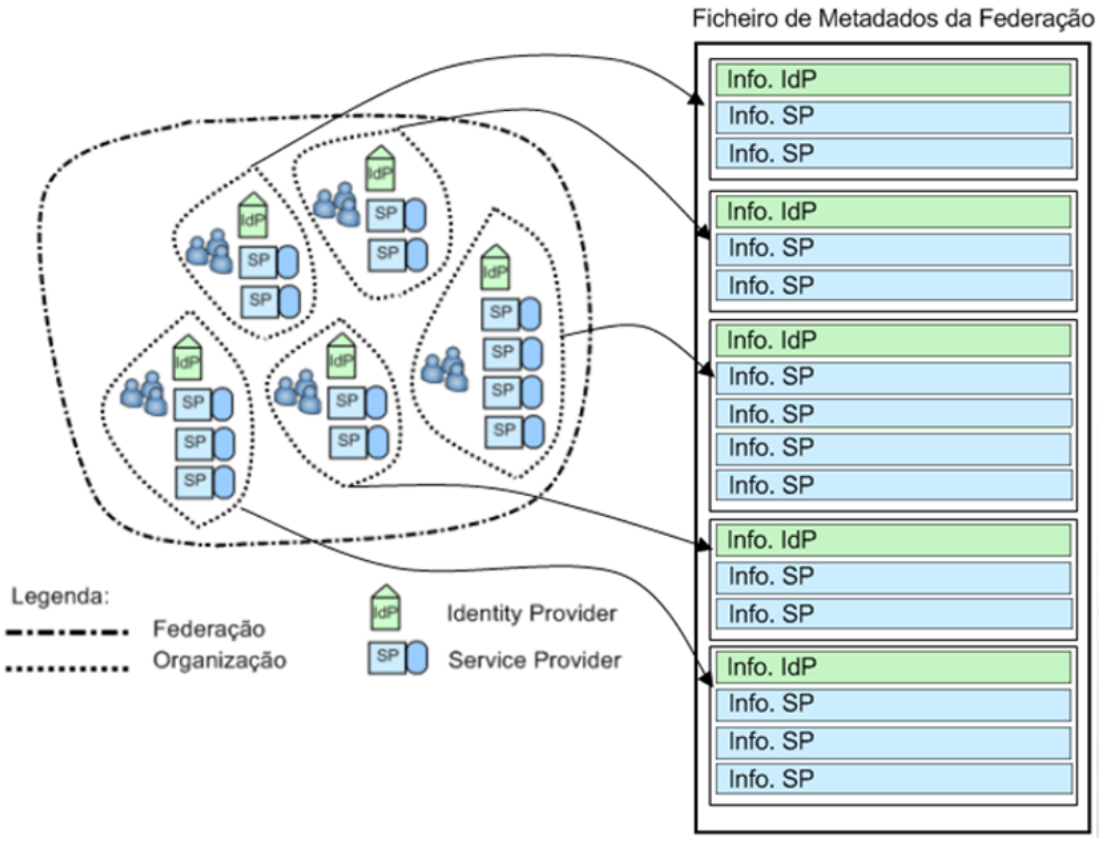
Metadados - O que são ?

Metadados da Federação

Os **metadados** de uma federação enumeram os intervenientes da federação considerados de confiança (fornecedores de identidade e serviço) e armazenam informação (ex.: entityID, chave pública do certificado) que permite estabelecer uma comunicação segura. Para iniciar o processo de comunicação entre o um fornecedor de identidade e o fornecedor de serviço é necessário utilizar os **metadados** para verificar a respectiva autenticidade.



A verificação é realizada através da comparação do nome (entityID) com os nomes existentes no respectivo ficheiro de metadados. Se o nome corresponde a uma entrada no ficheiro, é utilizado o respectivo certificado para decifrar a mensagem recebida. Identificado correctamente os intervenientes podem iniciar a comunicação para permitir o acesso ao serviço. Se não existe correspondência de nomes, não é possível estabelecer a comunicação e o acesso ao serviço.

Ficheiro de Metadados da Federação

Cada federação tem o seu ficheiro de metadados que partilha com todos os intervenientes (fornecedores de serviço e fornecedores de identidade).

Metadados RCTSaai

The federation metadata file is available in the following url:

https://registry.rctsaai.pt/rr/signedmetadata/federation/rctsaai/metadata.xml

If you need the metada regarding only Identity Providers, the file is available in the following url:

https://registry.rctsaai.pt/rr/metadata/federation/rctsaai/IDP/metadata.xml (Unsigned metadata)

If you need the metada regarding only Service Providers, the file is available in the following url:

https://registry.rctsaai.pt/rr/metadata/federation/rctsaai/SP/metadata.xml (Unsigned metadata)

Metadata file digitally signed

The federation metadata file is digitally signed. To obtain the certificate **metadatasigner.pem**, referenced in the configurations below, you must make the request via email to RCTSaai team (rctsaai@fccn.pt).

Metadata Configuration - Shibboleth

Upload Certificate

The metadatasigner.pem certificate used to validate the federation metadata should be placed in the following location: /opt/shibboleth-idp/credentials/

relying-party.xml

```
1. Add new block with the new link:


 <metadata:MetadataProvider id="URLMD" xsi:type="metadata:FileBackedHTTPMetadataProvider" xmlns="urn:mace:
shibboleth:2.0:metadata"
                        metadataURL="https://registry.rctsaai.pt/rr/signedmetadata/federation/rctsaai
/metadata.xml"
                        backingFile="/opt/shibboleth-idp/metadata/RCTSaai_metadata.xml"
                        minRefreshDelay="PT5M"
                        maxRefreshDelay="PT1H"
                        refreshDelayFactor="0.75" >


                 <metadata:MetadataFilter xsi:type="SignatureValidation" xmlns="urn:mace:shibboleth:2.0:
metadata" trustEngineRef="shibboleth.RR-RCTSaaiMetadataTrustEngine"  requireSignedMetadata="true" />

</metadata:MetadataProvider>



2. Add after block </ security: Credential> the reference to metadatasigner.pem certificate:

 <security:TrustEngine id="shibboleth.RR-RCTSaaiMetadataTrustEngine" xsi:type="security:
StaticExplicitKeySignature">
         <security:Credential  id="RCTSaaiFederationCredentials" xsi:type="security:X509Filesystem">
                         <security:Certificate>/opt/shibboleth-idp/credentials/metadatasigner.pem</security:
Certificate>
                 </security:Credential>
</security:TrustEngine>
```

Upload Certificate

The metadatasigner.pem certificate used to validate the federation metadata should be placed in the following location: /etc/shibboleth/

shibboleth2.xml

```
<MetadataProvider type="XML" uri="https://registry.rctsaai.pt/rr/signedmetadata/federation/rctsaai/metadata.
xml" backingFilePath="/etc/shibboleth/rctsaai/RCTSaai_metadata.xml"  reloadInterval="60">

        <MetadataFilter type="Signature" certificate="metadatasigner.pem"/>

</MetadataProvider>
```

Metadata Configuration - SimpleSAMLphp

Upload Certificate

The metadatasigner.pem certificate used to validate the federation metadata should be placed in the following location: /var/simplesaml/cert/

config-metarefresh.php

```
 <?php
   $config = array(
        'sets' => array(
               'rctsaai' => array(
                       'cron' => array('hourly'),
                       'sources' => array(
                              array( 'src' => 'https://registry.rctsaai.pt/rr/signedmetadata/federation
/rctsaai/metadata.xml',
                                     'certFingerprint' => '0b3b547d116b92d5f3008a3b4058e7a762f21d9d',
                                      'certificate'              => 'metadatasigner.pem', ),
                                      ),
                                      'maxCache' => 60*60*24*4, // Maximum 4 days cache time.
                                      'maxDuration' => 60*60*24*10, // Maximum 10 days duration on
ValidUntil.
                                      'outputDir' => 'metadata/rctsaai/',
                                      'outputFormat' => 'flatfile',
                              ),
       )
);
```

Metadados eduGAIN

Os metados da Federação eduGAIN estão disponível no seguinte url:

https://rctsaai-rr.fccn.pt/rr/signedmetadata/federation/RURVR0FJTg~~/metadata.xml

Metadata Assinada

O ficheiro de metadados da federação encontra-se assinado digitalmente. Para obter o certificado ***metadatasigner.pem***, referenciado nas configurações abaixo, deve realizar o pedido via email à equipa RCTSaai (rctsaai@fccn.pt).

Configurar Metadados - Shibboleth

Descarregar Certificado

O certificado metadatasigner.pem utilizado para validar a metadata da federação deve ser colocado na seguinte localização:

/opt/shibboleth-idp/credentials/

relying-party.xml

```
1. Adicionar novo bloco com o novo link e referencia ao url:

  <metadata:MetadataProvider id="URLMD2" xsi:type="metadata:FileBackedHTTPMetadataProvider" xmlns="urn:mace:
shibboleth:2.0:metadata"
                        metadataURL="https://rctsaai-rr.fccn.pt/rr/signedmetadata/federation/RURVR0FJTg~~
/metadata.xml"
                        backingFile="/opt/shibboleth-idp/metadata/edugain_metadata.xml"
                        minRefreshDelay="PT5M"
                        maxRefreshDelay="PT1H"
                        refreshDelayFactor="0.75" >


                        <metadata:MetadataFilter xsi:type="SignatureValidation" xmlns="urn:mace:shibboleth:
2.0:metadata" trustEngineRef="shibboleth.RR-RCTSaaiMetadataTrustEngine" requireSignedMetadata="true" />


        </metadata:MetadataProvider>



2. Adicionar após o bloco </security:Credential> a referencia ao certificado metadatasigner.pem

 <security:TrustEngine id="shibboleth.RR-RCTSaaiMetadataTrustEngine" xsi:type="security:
StaticExplicitKeySignature">
         <security:Credential  id="RCTSaaiFederationCredentials" xsi:type="security:X509Filesystem">
                         <security:Certificate>/opt/shibboleth-idp/credentials/metadatasigner.pem</security:
Certificate>
                </security:Credential>
</security:TrustEngine>
```

Descarregar Certificado

O certificado metadatasigner.pem utilizado para validar a metadata da federação deve ser colocado na seguinte localização:

/etc/shibboleth/

relying-party.xml

```
<MetadataProvider type="XML" uri="https://rctsaai-rr.fccn.pt/rr/signedmetadata/federation/RURVR0FJTg~~
/metadata.xml" backingFilePath="/etc/shibboleth/rctsaai/edugain_metadata.xml"  reloadInterval="60">

         <MetadataFilter type="Signature" certificate="metadatasigner.pem"/>

</MetadataProvider>
```

Configurar Metadados - SimpleSAMLphp

Descarregar Certificado

O certificado metadatasigner.pem utilizado para validar a metadata da federação deve ser colocado na seguinte localização:

/var/simplesaml/cert/

config-metarefresh.php

```
 <?php
   $config = array(
        'sets' => array(
                'edugain' => array(
                        'cron' => array('hourly'),
                        'sources' => array(
                                array( 'src' => 'https://rctsaai-rr.fccn.pt/rr/signedmetadata/federation
/RURVR0FJTg~~/metadata.xml',
                                       'certFingerprint' => '0b3b547d116b92d5f3008a3b4058e7a762f21d9d',
                                        'certificate'              => 'metadatasigner.pem', ),
                                        ),
                                        'maxCache' => 60*60*24*4, // Maximum 4 days cache time.
                                        'maxDuration' => 60*60*24*10, // Maximum 10 days duration on
ValidUntil.
                                        'outputDir' => 'metadata/edugain/',
                                        'outputFormat' => 'flatfile',
                                ),
        )
);
```