

# RCTSaai Metadata



The federation metadata file is available in the following url:

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

If you need the metadata 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 metadata 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](mailto: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.rctsaii.pt/rr/signedmetadata/federation/rctsaii/metadata.xml" backingFilePath="/etc/shibboleth/rctsaii/RCTSaii_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(
        'rctsaii' => array(
            'cron' => array('hourly'),
            'sources' => array(
                array( 'src' => 'https://registry.rctsaii.pt/rr/signedmetadata/federation
/rctsaii/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/rctsaii/',
            'outputFormat' => 'flatfile',
        ),
    ),
);
```