IAM Proxy OIDC / SAML

https://wiki.idem.garr.it/wiki/Gruppo_di_Lavoro_IAM_Proxy_OIDC

Obiettivi del gruppo

- L'obiettivo primario del gruppo è rendere disponibile un authentication proxy che permetta alle applicazioni OIDC di collegarsi in modo trasparente alla federazione IDEM tramite SAML2.
- Il proxy deve essere semplice, funzionante all'avvio, con il minor numero possibile di configurazioni / personalizzazioni necessarie per entrare in funzione.
- La manutenzione dovrebbe essere il più semplice ed automatizzata possibile.

Analisi del lavoro

- Per raggiungere l'obiettivo principale si è scelto di creare un backend ed una discovery page IDEM per Satosa proxy;
- Satosa proxy è uno IAM Proxy puro in python, ossia offre unicamente i servizi di proxy e conversione autenticazione. Il vantaggio principale nell'utilizzo di questo prodotto è nella sua semplicità e replicabilità. L'applicazione non richiede database, può lavorare in userspace e le dipendenze sono gestibili tramite VENV;
- Per semplificare il lavoro ed aumentare l'appetibilità del risultato si propone di aggiungere il modulo al repository Satosa-Saml2Spid di Developers Italia in modo da offrire un'unica installazione che possa fare da proxy per l'autenticazione SPID, CIE, eIDAS e IDEM. Inoltre lavorare su un repository già attivo e mantenuto garantirebbe un mutuale aumento delle potenzialità del prodotto e della sostenibilità del progetto nel tempo;
- Per semplificare ulteriormente il lavoro di deploy verrà creata un'immagine docker del prodotto preconfigurato in modo da renderlo rapidamente operativo in caso di necessità.

IAM Proxy OIDC / SAML

Perché Satosa?

- Satosa proxy è uno IAM Proxy puro in python, ossia offre unicamente i servizi di proxy e conversione autenticazione. Il vantaggio principale nell'utilizzo di questo prodotto è nella sua semplicità e replicabilità. L'applicazione non richiede database, può lavorare in userspace e le dipendenze sono gestibili tramite VENV.

- Per semplificare il lavoro ed aumentare l'appetibilità del risultato si propone di aggiungere il modulo al repository Satosa-Saml2Spid di Developers Italia in modo da offrire un'unica installazione che possa fare da proxy per l'autenticazione SPID, CIE, eIDAS e IDEM. Inoltre lavorare su un repository già attivo e mantenuto garantirebbe un mutuale aumento delle potenzialità del prodotto e della sostenibilità del progetto nel tempo.

- Altre possibili soluzioni, tipo Keycloak, sono state valutate come non adatte allo scopo.

IAM Proxy OIDC / SAML

Perché Docker?

“*Per semplificare ulteriormente il lavoro di deploy verrà creata un’immagine docker del prodotto preconfigurato in modo da renderlo rapidamente operativo in caso di necessità.*”

A seguito di vari incontri in stile “Install Day” per l’installazione e la configurazione di Satosa.

Fatti anche per diffondere la conoscenza sul prodotto e sul nostro progetto.

Pur seguendo le precise indicazioni di installazione fornite nel README.md del repository si sono evidenziati alcuni problemi.

Problemi dovuti principalmente a:

- Differenti OS in cui veniva effettuata l’installazione;
- Versioni di Python (e pip) differenti;
- Conoscenze a livello sistemistico non equivalenti tra i diversi partecipanti.

Con Docker ed una composizione ci si deve solo preoccupare di valorizzare correttamente le ENV e di avere certificati validi.

IAM Proxy OIDC / SAML

Repository GitHUB Developers Italia

- https://github.com/italia/Satosa-Saml2Spid

Repository GitHUB IDEM GARR AAI Federation

- https://github.com/IDEM-GARR-AAI/Satosa-Saml2Spid

IAM Proxy OIDC / SAML

Dockerfile

Parte da una Alpine ufficiale (versione 3.13.5):

```
FROM alpine:3.13.5
```

Definisco le ENV che sono strettamente necessarie:

```
ENV BASEDIR="/satosa_proxy"
ENV COMMON_NAME="SPID example proxy"
ENV LOCALITY_NAME="Roma"
ENV ORGANIZATION_IDENTIFIER="PA:IT-c_h501"
ENV ORGANIZATION_NAME="SPID example proxy"
ENV SERIAL_NUMBER="1234567890"
ENV SPID_SECTOR="public"
ENV URI="https://spid.proxy.example.org"
ENV DAYS="7300"
ENV SATOSA_DISCO_SRV="https://localhost:9999/disco.html"
```

Eseguo i comandi per aggiungere una timezone all’immagine:

```
RUN apk add --update --no-cache tzdata \
 && cp /usr/share/zoneinfo/Europe/Rome /etc/localtime \
 && echo "Europe/Rome" > /etc/timezone \
 && apk del tzdata
```

IAM Proxy OIDC / SAML

Dockerfile

Carico i file/directory che mi servono:

```
COPY example/ $BASEDIR/
COPY requirements.txt $BASEDIR/
COPY oids.conf $BASEDIR/pki/
COPY build_spid_certs.sh $BASEDIR/pki/
```

Eseguo le operazioni di installazione:

```
RUN apk add --update xmlsec libffi-dev libressl-dev python3 py3-pip python3-dev procps git openssl build-base gcc wget bash jq \
&& cd $BASEDIR/pki/ \
&& chmod 755 $BASEDIR/pki/build_spid_certs.sh \
&& $BASEDIR/pki/build_spid_certs.sh \
&& cd $BASEDIR/ \
&& pip3 install --upgrade pip \
&& pip3 install yq \
&& pip3 install -r requirements.txt --ignore-installed \
&& wget https://registry.spid.gov.it/metadata/idp/spid-entities-idps.xml -O metadata/idp/spid-entities-idps.xml \
&& adduser --disabled-password wert \
&& chown -R  wert . \
&& chmod +x run.sh
```

IAM Proxy OIDC / SAML

Dockerfile

Definisco USER e WORKDIR

USER wert

WORKDIR $BASEDIR/

Lancio il cuore del futuro container running

CMD bash run.sh

Perché lo chiamo il cuore del container running?

- Esegue la sostituzione di tutte le variabili nei file di configurazione;
- Lancia Satosa con uWSGI :
  - Se nel run o nell'esecuzione con docker-compose non è valorizzata la ENV "SATOSA_BY_DOCKER" viene lanciato solo Satosa (per default in uwsgi);
  - Altrimenti viene lanciato anche un uWSGI per servire le parti static del servizio. Ed entrambe in HTTPS;

https://github.com/IDEM-GARR-AAI/Satosa-Saml2Spid/blob/master/README.md

IAM Proxy OIDC / SAML

Dockerfile

Metadata (usati per fissare al suo interno dei valori che caratterizzano l’immagine e che possono essere poi letti facilmente):

```
# Metadata params
ARG BUILD_DATE
ARG VERSION
ARG VCS_URL="https://github.com/IDEM-GARR-AAI/Satosa-Saml2Spid.git"
ARG VCS_REF
ARG AUTHORS
ARG VENDOR

# Metadata : https://github.com/opencontainers/image-spec/blob/main/annotations.md
LABEL org.opencontainers.image.authors=$AUTHORS \
      org.opencontainers.image.vendor=$VENDOR \
      org.opencontainers.image.title="Satosa-Saml2Spid" \
      org.opencontainers.image.created=$BUILD_DATE \
      org.opencontainers.image.version=$VERSION \
      org.opencontainers.image.source=$VCS_URL \
      org.opencontainers.image.revision=$VCS_REF \
      org.opencontainers.image.description="Docker Image di Satosa-Saml2Spid."
```

Sono ancora da definire VERSION, AUTHORS e VENDOR .

IAM Proxy OIDC / SAML

Come fare la build

Per avere le label valorizzate in maniera corretta, oltre ad aggiungere quelle statiche nel Dockerfile occorre eseguire la build con un comando del tipo:

```
docker build --build-arg BUILD_DATE=`date -u +"%Y-%m-%dT%H:%M:%SZ"` --build-arg VCS_REF=`git rev-parse --short HEAD` -t scolagreco/satosa-saml2spid .
```

Comando: docker inspect scolagreco/satosa-saml2spid

```
...
        "Labels": {
            "org.opencontainers.image.authors": "",
            "org.opencontainers.image.created": "2022-08-02T10:56:12Z",
            "org.opencontainers.image.description": "Docker Image di Satosa-Saml2Spid.",
            "org.opencontainers.image.revision": "45fc252",
            "org.opencontainers.image.source": "https://github.com/IDEM-GARR-AAI/Satosa-Saml2Spid.git",
            "org.opencontainers.image.title": "Satosa-Saml2Spid",
            "org.opencontainers.image.vendor": "",
            "org.opencontainers.image.version": ""
        }
...
```

IAM Proxy OIDC / SAML

compose-Satosa-Saml2Spid

docker-compose.yml
.env
init-mongo.sh
Mongodata
nginx
oidc_op_frontend.yaml
run.sh
satosa

.env

```
MONGO_DBUSER=satosa
MONGO_DBPASSWORD=thatpassword
HOSTNAME=localhost
```

```
.
├── docker-compose.yml
├── init-mongo.sh
├── mongodata
│   ├── ...
│   └── ...
├── nginx
│   ├── 403.html
│   ├── 404.html
│   ├── 50x.html
│   ├── certs
│   │   ├── proxy_local.key
│   │   └── proxy_local.pem
│   ├── nginx.conf_proxy_http
│   ├── nginx.conf_uwsgi_pass
│   └── satosa_static
│       ├── disco.html
│       ├── eidas
│       │   ├── css
│       │   │   ├── ...
│       │   │   └── ...
│       │   └── img
│       │       ├── ...
│       │       └── ...
│       ├── error_page.html
│       └── spid
│           ├── ...
│           └── ...
├── oidc_op_frontend.yaml
├── run.sh
└── satosa
    ├── certs
    ├── conf
    └── logs

18 directories, 109 files
```

IAM Proxy OIDC / SAML

docker-compose.yml

I service sono:

- satosa-mongo;
- satosa-mongo-express;
- satosa-saml2spid;
- satosa-nginx

satosa-mongo:

```
image: mongo
container_name: satosa-mongo
restart: always
environment:
  MONGO_INITDB_DATABASE: oidcop
  MONGO_INITDB_ROOT_USERNAME: "${MONGO_DBUSER}"
  MONGO_INITDB_ROOT_PASSWORD: "${MONGO_DBPASSWORD}"
volumes:
  - mongodata:/data/db
  - /usr/share/zoneinfo/Europe/Rome:/etc/localtime:ro
  - ./init-mongo.sh:/docker-entrypoint-initdb.d/init-mongo.sh
ports:
  - '27017-27019:27017-27019'
```

satosa-mongo-express:

```
image: mongo-express
container_name: satosa-mongo-express
restart: always
ports:
  - 8082:8081
environment:
  ME_CONFIG_BASICAUTH_USERNAME: satosauser
  ME_CONFIG_BASICAUTH_PASSWORD: satosapw
  ME_CONFIG_MONGODB_ADMINUSERNAME: "${MONGO_DBUSER}"
  ME_CONFIG_MONGODB_ADMINPASSWORD: "${MONGO_DBPASSWORD}"
  ME_CONFIG_MONGODB_URL: mongodb://${MONGO_DBUSER}:${MONGO_DBPASSWORD}@satosa-mongo:27017/
```

IAM Proxy OIDC / SAML

init-mongo.sh

```
#!/usr/bin/env bash

mongosh -- "$MONGO_INITDB_DATABASE"<<EOF

var rootUser = '$MONGO_INITDB_ROOT_USERNAME';
var rootPassword = '$MONGO_INITDB_ROOT_PASSWORD';
var admin = db.getSiblingDB('admin');
admin.auth(rootUser, rootPassword);
var user = '$MONGO_INITDB_ROOT_USERNAME';
var passwd = '$MONGO_INITDB_ROOT_PASSWORD';

db.createUser(
  {
    user: user,
    pwd:  passwd,
    roles: [
        { role: "readWrite" , db: '$MONGO_INITDB_DATABASE'}
    ]
  }
)

// make client_id unique
db.client.createIndex( { "client_id": 1 }, { unique: true } )
db.client.createIndex( { "registration_access_token": 1 }, { unique: true } )

// make access_token and sid unique
db.session.createIndex( { "sid": 1 }, { unique: true } )

// create expired session deletion
db.session.createIndex(
  { expires_at: 1 },
  { expireAfterSeconds: 0, partialFilterExpression: { count: { \$gt: 2 } } }
);

....

EOF
```

IAM Proxy OIDC / SAML

```
satosa-saml2spid:
  image: scolagreco/satosa-saml2spid
  container_name: satosa-saml2spid
  depends_on:
    - satosa-mongo
  environment:
    - SATOSA_BY_DOCKER=1
    - SATOSA_BASE=https://$HOSTNAME
    # - SATOSA_CONTACT_PERSON_EMAIL_ADDRESS=support.example@organization.org
    # - SATOSA_CONTACT_PERSON_FISCALCODE=01234567890
    # - SATOSA_CONTACT_PERSON_GIVEN_NAME=Name
    # - SATOSA_CONTACT_PERSON_TELEPHONE_NUMBER=06123456789
    - SATOSA_DISCO_SRV=https://$HOSTNAME/static/disco.html
    # - SATOSA_ENCRYPTION_KEY=
    - MONGODB_PASSWORD=${MONGO_DBPASSWORD}
    - MONGODB_USERNAME=${MONGO_DBUSER}
    # - SATOSA_ORGANIZATION_DISPLAY_NAME_EN=Resource provided by Example Organization
    # - SATOSA_ORGANIZATION_DISPLAY_NAME_IT=Resource provided by Example Organization
    # - SATOSA_ORGANIZATION_NAME_EN=Resource provided by Example Organization
    # - SATOSA_ORGANIZATION_NAME_IT=Resource provided by Example Organization
    # - SATOSA_ORGANIZATION_URL_EN=https://example_organization.org
    # - SATOSA_ORGANIZATION_URL_IT=https://example_organization.org
    # - SATOSA_PRIVATE_KEYS=
    # - SATOSA_PUBLIC_KEY=
    # - SATOSA_SALT=
    # - SATOSA_STATE_ENCRYPTION_KEY
```

IAM Proxy OIDC / SAML

```
    # - SATOSA_UI_DESCRIPTION_EN=Resource description
    # - SATOSA_UI_DESCRIPTION_IT=Resource description
    # - SATOSA_UI_DISPLAY_NAME_EN=Resource Display Name
    # - SATOSA_UI_DISPLAY_NAME_IT=Resource Display Name
    # - SATOSA_UI_INFORMATION_URL_EN=https://example_organization.org/information_url_en
    # - SATOSA_UI_INFORMATION_URL_IT=https://example_organization.org/information_url_en
    # - SATOSA_UI_LOGO_HEIGHT=60
    # - SATOSA_UI_LOGO_URL=https://example_organization.org/logo.png
    # - SATOSA_UI_LOGO_WIDTH=80
    # - SATOSA_UI_PRIVACY_URL_EN=https://example_organization.org/privacy_en
    # - SATOSA_UI_PRIVACY_URL_IT=https://example_organization.org/privacy_en
    - SATOSA_UNKNOW_ERROR_REDIRECT_PAGE=https://$HOSTNAME/static/error_page.html
    # - SATOSA_USER_ID_HASH_SALT
  expose:
    - 10000
    - 9999
  ports:
    - "10000:10000"
    - "9999:9999"
  volumes:
      - /usr/share/zoneinfo/Europe/Rome:/etc/localtime:ro
      - ./run.sh:/satosa_proxy/run.sh
#       - satosa_base_static:/satosa_proxy/static/:ro    # Togliere il commento a questo volume se nel container satosa-nginx si vuole utilizzare la directory interna con i file statici.
```

IAM Proxy OIDC / SAML

```
  satosa-nginx:
    image: nginx:alpine
    container_name: satosa-nginx
    depends_on:
      - satosa-saml2spid
    ports:
      - "80:80"
      - "443:443"
    volumes:
      - ./nginx/nginx.conf_uwsgi_pass:/etc/nginx/nginx.conf:ro
      - ./nginx/50x.html:/usr/share/nginx/html/50x.html:ro
      - ./nginx/404.html:/usr/share/nginx/html/404.html:ro
      - ./nginx/403.html:/usr/share/nginx/html/403.html:ro
      - ./nginx/certs/:/etc/nginx/certs/:ro
      - satosa_static:/var/www/html/:ro        # Monta la directory static locale, esterna ai container, può essere customizzata.
#     - satosa_base_static:/var/www/html/:ro    # Monta la directory static del volume interno al container satosa-saml2spid.
```

IAM Proxy OIDC / SAML

L’uso più semplice

git clone git@github.com:IDEM-GARR-AAI/Satosa-Saml2Spid.git

cd Satosa-Saml2Spid/compose-Satosa-Saml2Spid/

Anche senza modificare nulla.
Quindi **NON** valorizzando nessuna variabile nei seguenti file:

- .env
- docker-compose.yml

E **NON** sostituendo i certificati forniti.

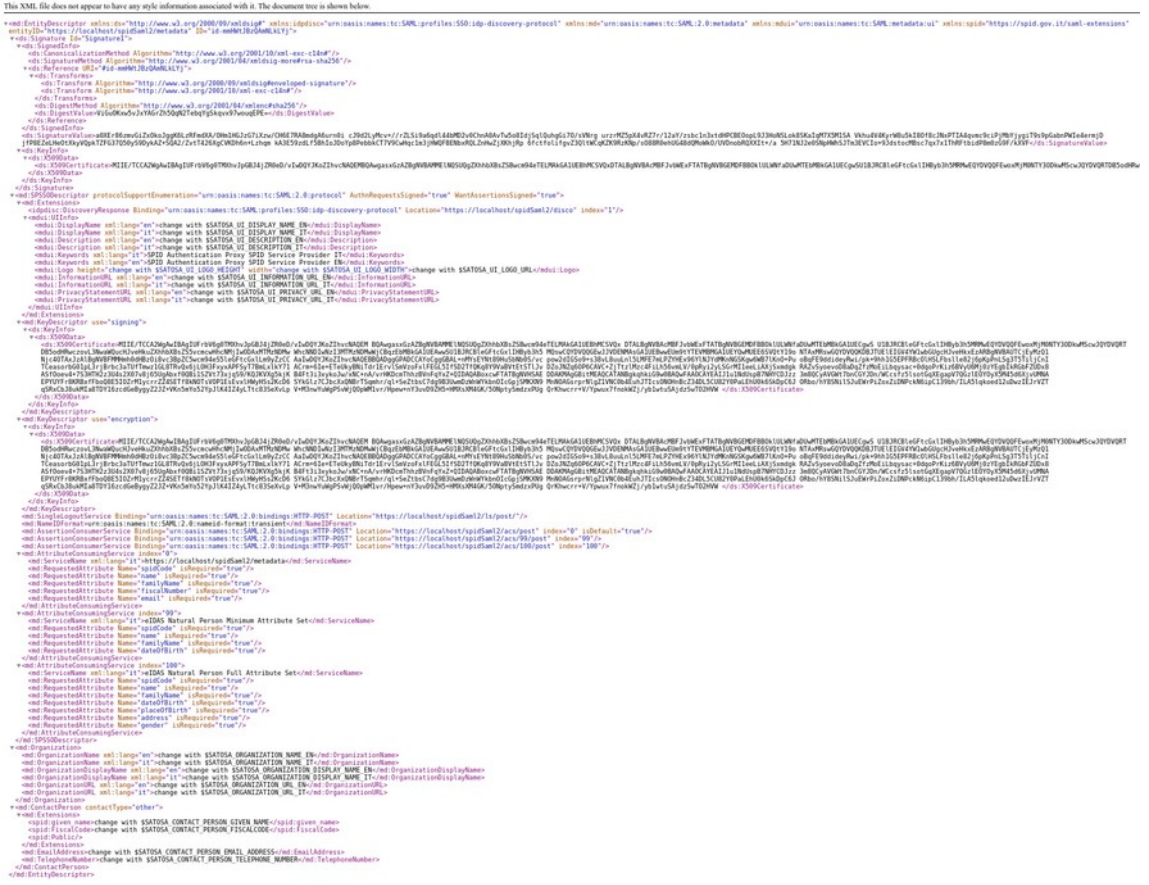
Si può far partire la composizione:

docker-compose pull; docker-compose down -v; docker-compose up -d; docker-compose logs -f

```
...
satosa-saml2spid       | [2022-10-27 16:21:04] [INFO ]: Running SATOSA version 8.0.0 [satosa.proxy_server.make_app:195]
satosa-saml2spid       | [2022-10-27 16:21:04] [INFO ]: Loading backend modules... [satosa.base.__init__:42]
satosa-saml2spid       | [2022-10-27 16:21:06] [INFO ]: Setup backends: ['Saml2', 'spidSaml2'] [satosa.plugin_loader.load_backends:49]
satosa-saml2spid       | [2022-10-27 16:21:06] [INFO ]: Loading frontend modules... [satosa.base.__init__:45]
satosa-saml2spid       | claims_interface not seems to be a valid configuration parameter
satosa-saml2spid       | [2022-10-27 16:21:06] [INFO ]: Setup frontends: ['Saml2IDP', 'OIDC'] [satosa.plugin_loader.load_frontends:70]
satosa-saml2spid       | [2022-10-27 16:21:06] [INFO ]: Loading micro services... [satosa.base.__init__:51]
satosa-saml2spid       | [2022-10-27 16:21:06] [INFO ]: Loaded request micro services: ['IdpHinting', 'DiscoToTargetIssuer', 'DecideBackendByTargetIssuer']
[satosa.plugin_loader.load_request_microservices:260]
satosa-saml2spid       | [2022-10-27 16:21:06] [INFO ]: Loaded response micro services:[] [satosa.plugin_loader.load_response_microservices:281]
satosa-saml2spid       | WSGI app 0 (mountpoint='') ready in 4 seconds on interpreter 0x560e8ad02680 pid: 19 (default app)
satosa-saml2spid       | *** uWSGI is running in multiple interpreter mode ***
satosa-saml2spid       | spawned uWSGI worker 1 (pid: 19, cores: 2)
satosa-saml2spid       | spawned uWSGI worker 2 (pid: 21, cores: 2)
satosa-saml2spid       | spawned uWSGI worker 3 (pid: 23, cores: 2)
satosa-saml2spid       | spawned uWSGI worker 4 (pid: 25, cores: 2)
```

IAM Proxy OIDC / SAML

https://localhost/spidSaml2/metadata



IAM Proxy OIDC / SAML

https://localhost/Saml2IDP/metadata

This XML file does not appear to have any style information associated with it. The document tree is shown below.


```
<md:EntityDescriptor xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:mdui="urn:oasis:names:tc:SAML:metadata:ui" entityID="https://localhost/Saml2IDP/metadata">
 <md:IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" WantAuthnRequestsSigned="false">
  <md:Extensions>
   <mdui:UIInfo>
    <mdui:DisplayName xml:lang="en">change with $SATOSA_UI_DISPLAY_NAME_EN</mdui:DisplayName>
    <mdui:DisplayName xml:lang="it">change with $SATOSA_UI_DISPLAY_NAME_IT</mdui:DisplayName>
    <mdui:Description xml:lang="en">change with $SATOSA_UI_DESCRIPTION_EN</mdui:Description>
    <mdui:Description xml:lang="it">change with $SATOSA_UI_DESCRIPTION_IT</mdui:Description>
    <mdui:Logo height="change with $SATOSA_UI_LOGO_HEIGHT" width="change with $SATOSA_UI_LOGO_WIDTH">change with $SATOSA_UI_LOGO_URL</mdui:Logo>
    <mdui:InformationURL xml:lang="en">change with $SATOSA_UI_INFORMATION_URL_EN</mdui:InformationURL>
    <mdui:InformationURL xml:lang="it">change with $SATOSA_UI_INFORMATION_URL_IT</mdui:InformationURL>
    <mdui:PrivacyStatementURL xml:lang="en">change with $SATOSA_UI_PRIVACY_URL_EN</mdui:PrivacyStatementURL>
    <mdui:PrivacyStatementURL xml:lang="it">change with $SATOSA_UI_PRIVACY_URL_IT</mdui:PrivacyStatementURL>
   </mdui:UIInfo>
  </md:Extensions>
  <md:KeyDescriptor use="signing">
   <ds:KeyInfo>
    <ds:X509Data>
     <ds:X509Certificate>MIIE/TCCA2WgAwIBAgIUFrbV6g0TMXhvJpGBJ4jZR0eD/vIwDQYJKoZIhvcNAQEM BQAwgasxGzAZBgNVBAMMElNQSUQgZXhhbXBsZSBwcm94eTELMAkGA1UEBhMCSVQx DTALBgNVBAcMBFJvbWExFTATBgNVBGEMDFBBOklULWNfaDUwMTEbMBkGA1UECgwS U1BJRCBleGFtcGxlIHByb3h5MRMwEQYDVQQFEwoxMjM0NTY3ODkwMScwJQYDVQRT
     DB5odHRwczovL3NwaWQucHJveHkuZXhhbXBsZS5vcmcwHhcNMjIwODAxMTMzNDMw WhcNNDIwNzI3MTMzNDMwWjCBqzEbMBkGA1UEAwwSU1BJRCBleGFtcGxlIHByb3h5 MQswCQYDVQQGEwJJVDENMAsGA1UEBwwEUm9tYTEVMBMGA1UEYQwMUEE6SVQtY19o NTAxMRswGQYDVQQKDBJTUElEIGV4YW1wbGUgcHJveHkxEzARBgNVBAUTCjEyMzQ1
     Njc4OTAxJzAlBgNVBFMMHmh0dHBzOi8vc3BpZC5wcm94eS5leGFtcGxlLm9yZzCC AaIwDQYJKoZIhvcNAQEBBQADggGPADCCAYoCggGBAL+nMYsEYNt89HuSbNb0S/vc pow2dIGSo9+s38vL8uuLnl5LMFE7mLPZYHEx96YlNJYdMKnNGSKgw6WB7lKnO+Pu oBqFE9ddideyRwi/pk+9hh1G5EPFRBcOlHSLFbslle82j6pKpPnLSg3T5TiljCnI
     TCeasorbG01pL3rjBrbc3aTUfTmwz1GL8TRvQx6jLOH3FxyxAPFSyT7BmLxlkY71 ACrm+6Ie+ETeUkyBNiTdr1ErvlSmVzoFxlFEGL5IfSD2TfQKq8Y9VaBVtEtSTlJv DZoJNZq6OP6CAVC+ZjTtzlMzc4FiLh56vmLV/0pRyi2yLSGrMI1eeLiAXjSxmdgk RAZvSyoevoD8aDqZfzMoEiLbqysac+0dqoPrKiz6BVyU6Mj0zYEgbIkRGbFZUDx8
     ASfOoev4+7S3HTH2z3U4s2X07v8j65UgAbxf0QBil5ZVt73xjqS9/KQJKVXg5kjK B4Ft3i3xykoJw/xNC+nA/vrHKDcmThhzBVnFqYxZ+QIDAQABoxcwFTATBgNVHSAE DDAKMAgGBitMEAQCATANBgkqhkiG9w0BAQwFAAOCAYEAIJ1u1NdUspB7NHYCDJzz 3m8QCyAVGWt7bnCGYJDn/WCcsfz5lsotGqXEgapV7QGzlEOYOyX5M45d6XjvUMNA
     EPYUYFr8KRBxfFboQ8E5IOZrM1ycrrZZ4SETf8kNOTsVOP1EsEvxlHWyHSs2KcD6 SYkGlz7CJbcXxQNBrTSqmhr/ql+SeZtbsC7dg9B3UwmDzWnWYkbnOIcGpjSMKXN9 MnNOAGsrprNlgZ1VNC0b4EuhJTIcs0NOHnBcZ34DL5CU82Y0PaLEhU0k6SkDpC6J ORbo/hY8SNilSJuEWrPiZoxZiDNPckN6ipC139bh/ILA5lqkoed12uDwzIEJrVZT
     qSRxCbJ8ukMIa8TDY16zcdGeBygyZ2JZ+VKn5mYo52YpJlK4IZ4yLTtc83SeXvLp V+M3nwYuWgPSvWjQOpWM1vr/Hpew+nY3uvD9ZH5+HMXsXM4GK/50NptySmdzxPUg QrKhwcrr+V/Ypwux7fnokWZj/yblwtuSAjdzSwTO2HVW </ds:X509Certificate>
    </ds:X509Data>
   </ds:KeyInfo>
  </md:KeyDescriptor>
  <md:KeyDescriptor use="encryption">
   <ds:KeyInfo>
    <ds:X509Data>
     <ds:X509Certificate>MIIE/TCCA2WgAwIBAgIUFrbV6g0TMXhvJpGBJ4jZR0eD/vIwDQYJKoZIhvcNAQEM BQAwgasxGzAZBgNVBAMMElNQSUQgZXhhbXBsZSBwcm94eTELMAkGA1UEBhMCSVQx DTALBgNVBAcMBFJvbWExFTATBgNVBGEMDFBBOklULWNfaDUwMTEbMBkGA1UECgwS U1BJRCBleGFtcGxlIHByb3h5MRMwEQYDVQQFEwoxMjM0NTY3ODkwMScwJQYDVQRT
     DB5odHRwczovL3NwaWQucHJveHkuZXhhbXBsZS5vcmcwHhcNMjIwODAxMTMzNDMw WhcNNDIwNzI3MTMzNDMwWjCBqzEbMBkGA1UEAwwSU1BJRCBleGFtcGxlIHByb3h5 MQswCQYDVQQGEwJJVDENMAsGA1UEBwwEUm9tYTEVMBMGA1UEYQwMUEE6SVQtY19o NTAxMRswGQYDVQQKDBJTUElEIGV4YW1wbGUgcHJveHkxEzARBgNVBAUTCjEyMzQ1
     Njc4OTAxJzAlBgNVBFMMHmh0dHBzOi8vc3BpZC5wcm94eS5leGFtcGxlLm9yZzCC AaIwDQYJKoZIhvcNAQEBBQADggGPADCCAYoCggGBAL+nMYsEYNt89HuSbNb0S/vc pow2dIGSo9+s38vL8uuLnl5LMFE7mLPZYHEx96YlNJYdMKnNGSKgw6WB7lKnO+Pu oBqFE9ddideyRwi/pk+9hh1G5EPFRBcOlHSLFbslle82j6pKpPnLSg3T5TiljCnI
     TCeasorbG01pL3rjBrbc3aTUfTmwz1GL8TRvQx6jLOH3FxyxAPFSyT7BmLxlkY71 ACrm+6Ie+ETeUkyBNiTdr1ErvlSmVzoFxlFEGL5IfSD2TfQKq8Y9VaBVtEtSTlJv DZoJNZq6OP6CAVC+ZjTtzlMzc4FiLh56vmLV/0pRyi2yLSGrMI1eeLiAXjSxmdgk RAZvSyoevoD8aDqZfzMoEiLbqysac+0dqoPrKiz6BVyU6Mj0zYEgbIkRGbFZUDx8
     ASfOoev4+7S3HTH2z3U4s2X07v8j65UgAbxf0QBil5ZVt73xjqS9/KQJKVXg5kjK B4Ft3i3xykoJw/xNC+nA/vrHKDcmThhzBVnFqYxZ+QIDAQABoxcwFTATBgNVHSAE DDAKMAgGBitMEAQCATANBgkqhkiG9w0BAQwFAAOCAYEAIJ1u1NdUspB7NHYCDJzz 3m8QCyAVGWt7bnCGYJDn/WCcsfz5lsotGqXEgapV7QGzlEOYOyX5M45d6XjvUMNA
     EPYUYFr8KRBxfFboQ8E5IOZrM1ycrrZZ4SETf8kNOTsVOP1EsEvxlHWyHSs2KcD6 SYkGlz7CJbcXxQNBrTSqmhr/ql+SeZtbsC7dg9B3UwmDzWnWYkbnOIcGpjSMKXN9 MnNOAGsrprNlgZ1VNC0b4EuhJTIcs0NOHnBcZ34DL5CU82Y0PaLEhU0k6SkDpC6J ORbo/hY8SNilSJuEWrPiZoxZiDNPckN6ipC139bh/ILA5lqkoed12uDwzIEJrVZT
     qSRxCbJ8ukMIa8TDY16zcdGeBygyZ2JZ+VKn5mYo52YpJlK4IZ4yLTtc83SeXvLp V+M3nwYuWgPSvWjQOpWM1vr/Hpew+nY3uvD9ZH5+HMXsXM4GK/50NptySmdzxPUg QrKhwcrr+V/Ypwux7fnokWZj/yblwtuSAjdzSwTO2HVW </ds:X509Certificate>
    </ds:X509Data>
   </ds:KeyInfo>
  </md:KeyDescriptor>
  <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>
  <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://localhost/Saml2/sso/post"/>
  <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://localhost/spidSaml2/sso/post"/>
  <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://localhost/Saml2/sso/redirect"/>
  <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://localhost/spidSaml2/sso/redirect"/>
 </md:IDPSSODescriptor>
 <md:Organization>
   <md:OrganizationName xml:lang="en">change with $SATOSA_ORGANIZATION_NAME_EN</md:OrganizationName>
   <md:OrganizationName xml:lang="it">change with $SATOSA_ORGANIZATION_NAME_IT</md:OrganizationName>
   <md:OrganizationDisplayName xml:lang="en">change with $SATOSA_ORGANIZATION_DISPLAY_NAME_EN</md:OrganizationDisplayName>
   <md:OrganizationDisplayName xml:lang="it">change with $SAOSA_ORGANIZATION_DISPLAY_NAME_IT</md:OrganizationDisplayName>
   <md:OrganizationURL xml:lang="en">change with $SATOSA_ORGANIZATION_URL_EN</md:OrganizationURL>
   <md:OrganizationURL xml:lang="it">change with $SATOSA_ORGANIZATION_URL_IT</md:OrganizationURL>
 </md:Organization>
 <md:ContactPerson contactType="technical">
   <md:GivenName>change with $SATOSA_CONTACT_PERSON_GIVEN_NAME</md:GivenName>
   <md:EmailAddress>change with $SATOSA_CONTACT_PERSON_EMAIL_ADDRESS</md:EmailAddress>
 </md:ContactPerson>
</md:EntityDescriptor>
```