2FA

INFN
CCR - AAI

Loano 26 maggio 2023

Enrico M.V. Fasanelli

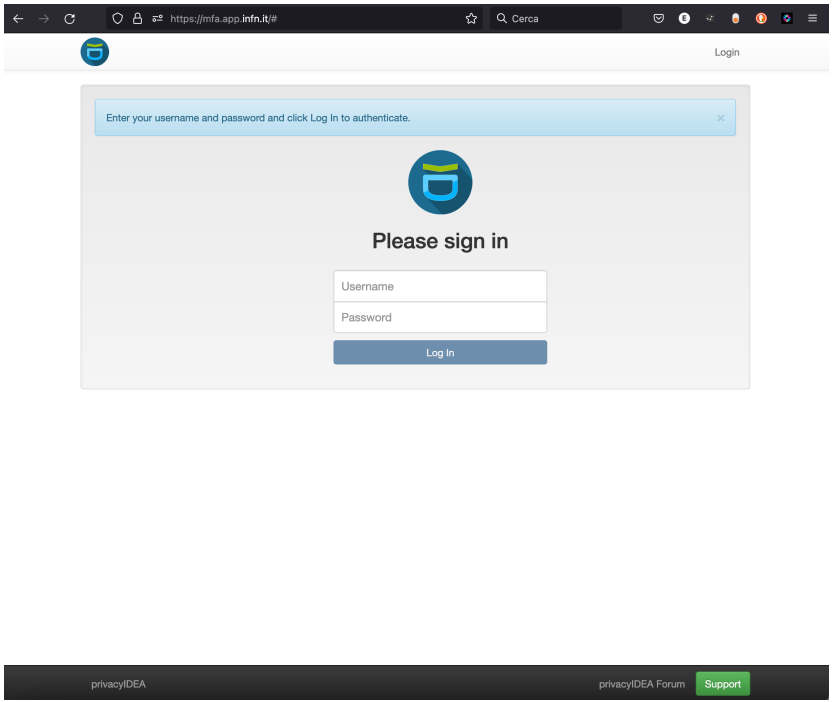
2FA.zip

Versione breve

(aggiornamento dalla CCR di Marzo 2023)

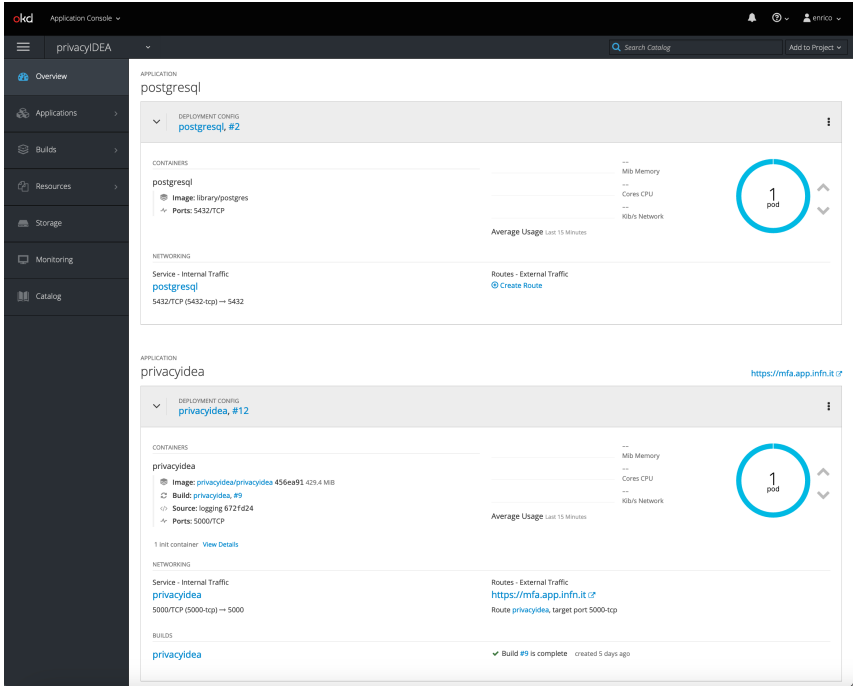
Habemus MFA

- https://mfa.app.infn.it/



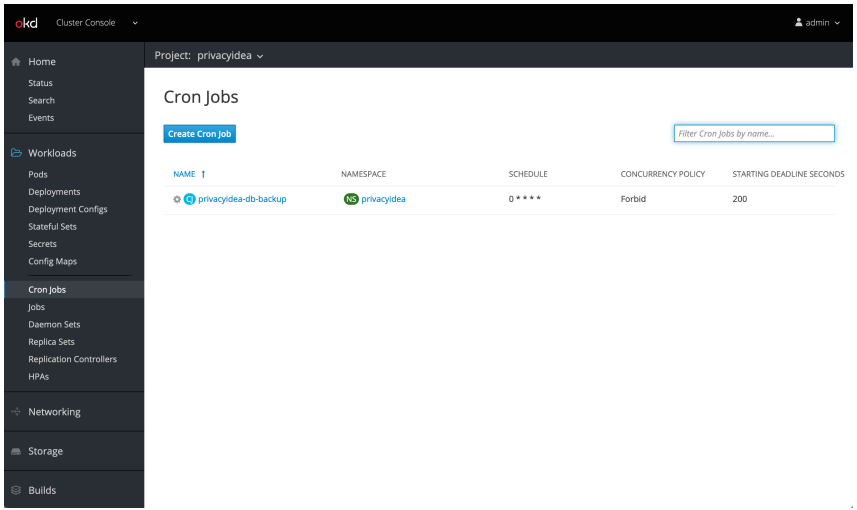
Habemus MFA

- https://mfa.app.infn.it/
- Cluster OKD di produzione



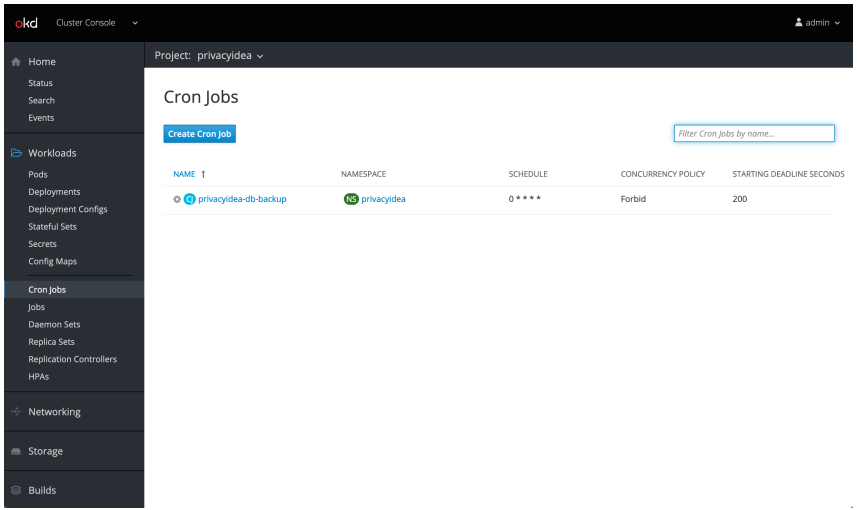
Habemus MFA

- https://mfa.app.infn.it/
- Cluster OKD di produzione
- Backup ogni ora



Habemus MFA

- https://mfa.app.infn.it/
- Cluster OKD di produzione
- Backup ogni ora
- Definita e verificata procedura di restore
  - da zero (build e deploy)
  - da backup



Token abilitati

- TOTP
  - SHA1/lunghezza 6 (compatibilità con Google Authenticator)
- PPR (paper)
  - 100 token HOTP in un PDF da stampare
- Registration token
  - Token iniziale per accesso alla console self-service per l'enrollment di un TOTP e/o PPR
- Password
  - Token da utilizzare nel caso di «lost-token»

The End

Grazie

Domande?

2FA.unzip

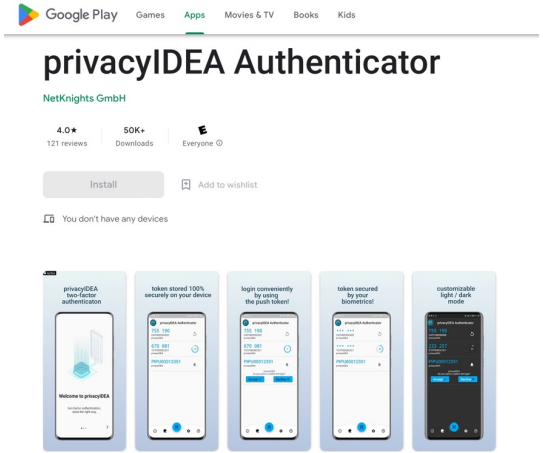
Qualche dettaglio in più

PrivacyIDEA Authentication (1)

- Applicazione scritta in Python (Open Source, AGPLv3)
- Supporta vari tipi di «tokens»
- Tre layers:
  - API;
  - Libreria;
  - Database
- Web UI per amministrazione
- Autenticazione via API o Plug-in (disponibili per FreeRADIUS, SimpleSAMLphp, WordPress, DokuWiki, PAM, …)
- Multi-REALM

PrivacyIDEA Authentication (2)

- Multiple user-backend (LDAP, SQL, SCIM, HTTP, File)
  - Custom user-backend via moduli python
- Dispiegabile in modalità HA (DB singolo o clustered-DB)
- Free app (IOS & Android)
- Enterprise support



Il nostro deploy

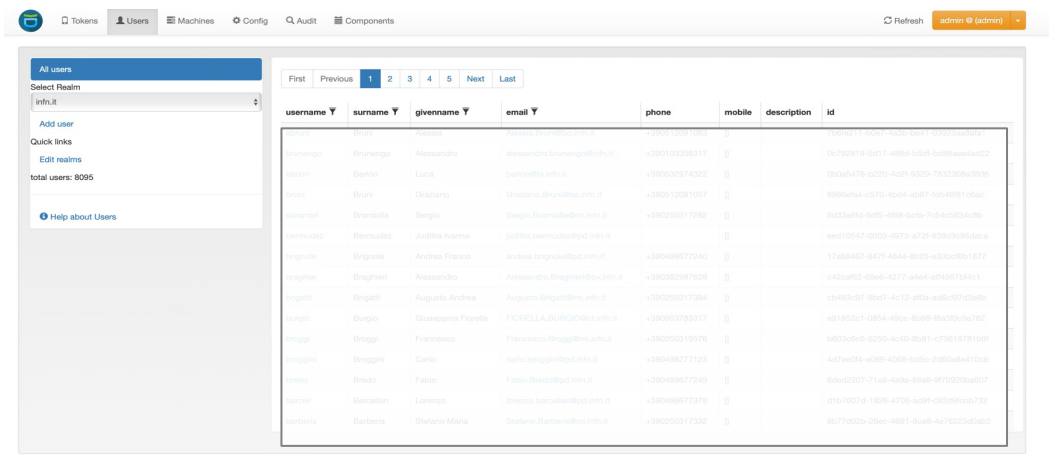
- Progetti nei cluster OKD (dev, pre e prod)
- DB postgresql
- privacyIDEA 3.8.1 Docker image basata su python:3.8
  - psycopg2
  - gunicorn

Dockerfile

```
FROM python:3.8

RUN pip install -r https://raw.githubusercontent.com/privacyidea/privacyidea/v3.8.1/requirements.txt
RUN pip install privacyidea==3.8.1

RUN mkdir privacyidea
WORKDIR privacyidea

RUN pip install psycopg2
RUN pip install gunicorn==20.1.0

COPY ./pi.cfg /etc/privacyidea/pi.cfg
COPY ./logging.yml /etc/privacyidea/logging.yml

EXPOSE 5000
VOLUME [ "/log" ]

ENV CONFIG_NAME="production"

CMD gunicorn --access-logfile='-' --log-file='-' --log-level='info'\
 --access-logformat '%({x-forwarded-for}i)s %(h)s %(l)s %(u)s %(t)s "%(r)s" %(s)s %(b)s "%(f)s" "%(a)s"'\
 --forwarded-allow-ips='*' -b '0.0.0.0:5000' "privacyidea.app:create_app(config_name='${CONFIG_NAME}')"

```

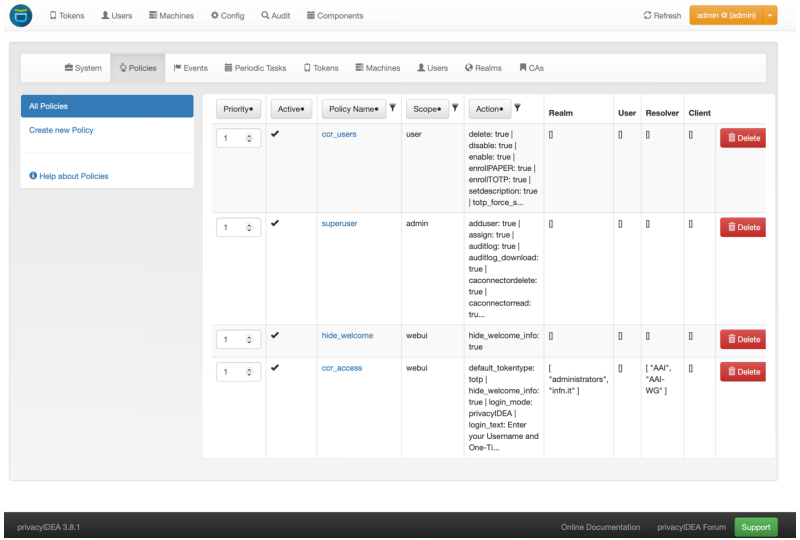
La nostra configurazione

- Userstore LDAP (dipendenti, associati ed ospiti)
  - (uid=*)(eduPersonAffiliation=member)



La nostra configurazione

- Userstore LDAP (dipendenti, associati ed ospiti)
  - (uid=*)(eduPersonAffiliation=member)
- Policy
  - Gli administrators possono emettere
    - registration token
    - password (lost-token scenario)
  - Users self-enroll token (TOTP e PPR) via WebUI
  - WebUI access via privacyIDEA (OTP)



Comma 22?

- INFN-AAI gestisce un IdP registrato in IDEM (e quindi in eduGAIN)

Comma 22?

- INFN-AAI gestisce un IdP registrato in IDEM (e quindi in eduGAIN)
- Il profilo MFA in eduGAIN è regolati da REFEDS-MFA

3. Syntax

In a SAML assertion, compliance is communicated by asserting the AuthnContextClassRef:

https://refeds.org/profile/mfa

4. Criteria

By asserting the URI shown above, an Identity Provider claims that:

- The authentication of the user's current session used a combination of at least two of the four distinct types of factors defined in ITU-T X.1254: Entity authentication assurance framework, section 3.1.3, authentication factor (something you know, something you have, something you are, something you do) [4].
- The factors used are independent, in that access to one factor does not by itself grant access to other factors.
- The combination of the factors mitigates single-factor only risks related to non-real-time attacks such as phishing, offline cracking, online guessing and theft of a (single) factor.

Comma 22?

- INFN-AAI gestisce un IdP registrato in IDEM (e quindi in eduGAIN)
- Il profilo MFA in eduGAIN è regolati da REFEDS-MFA
- L'altro ieri (24 maggio 2023) l'assemblea dei membri di IDEM ha approvato il documento «Profili di garanzia delle identità digitali della Federazione IDEM»

Comma 22?

- INFN-AAI gestisce un Id
- Il profilo MFA in eduGA
- L'altro ieri (24 maggio 2 documento «Profili di ga

4.5.2. Autenticazione a più fattori

1. L'autenticazione a più fattori DEVE essere effettuata con uno dei seguenti mezzi:
    - una combinazione di due o più fattori che rispondano agli stessi requisiti indicati per l'autenticazione a singolo fattore (vedi 4.5.1).
    - un dispositivo "Multi-Factor" hardware o software così come definito in [NIST 800-63B].
2. I fattori di autenticazione utilizzati per l'autenticazione combinata DEVONO essere di tipo diverso.
3. I fattori di autenticazione utilizzati per l'autenticazione combinata DEVONO essere indipendenti.
4. Un ulteriore fattore di autenticazione PUÒ essere attivato tramite un fattore esistente, in tal caso DEVE essere sempre prevista la notifica dell'attivazione sui canali di contatto dell'utente, inoltre DEVONO essere adottate misure per limitare il rischio di compromissione, quali l'invio di un messaggio di attivazione secondo le specifiche indicate al punto 2 del paragrafo 4.5.1 o tramite un processo supervisionato. In ogni caso, l'ulteriore fattore NON DEVE essere accessibile utilizzando l'esistente e DEVE mantenere l'indipendenza di tutte le altre operazioni di gestione come l'eliminazione, la modifica, il reset.
5. Le specifiche di autenticazione del REFEDS MFA Profile [REFEDS-MFA] sono pienamente compatibili con le specifiche qui indicate.

Due scenari

- Abilitare il secondo fattore solo per servizi e/o ruoli selezionati
  - Servizi di tipo amministrativo
  - Ruoli con privilegi da amministratore
- Questo rende impraticabile ottenere il secondo fattore via autenticazione INFN-AAI →Registration token → overhead amministrativo

Due scenari

- Abilitare il secondo fattore solo per servizi e/o ruoli selezionati
  - Servizi di tipo amministrativo
  - Ruoli con privilegi da amministratore
- Questo rende impraticabile ottenere il secondo fattore via autenticazione INFN-AAI →Registration token → overhead amministrativo

- Imporre l'utilizzo del secondo fattore per l'accesso a tutti i servizi web (una volta per ogni autenticazione → una volta al giorno, grazie al SSO).
- Necessario scrivere un plug-in per la registrazione in GODiVA dello stato dell'enrollment

Primo scenario (quello del comma22)

- Qualcuno (help-desk, servizio XYZ) genera un Registration Token e lo consegna in qualche modo all'utente.
- L'utente utilizza il Registration Token per accedere alla WebUI attraverso la quale può effettuare l'enrollment di un Token che utilizzerà quando gli sarà richiesto dal servizio configurato per autenticazione con doppio fattore.

- Con:
  - Overhead per help-desk/servizioXYZ
  - Che me ne faccio di un token che non mi verrà richiesto (quasi) mai?
- Pro:
  - Siamo (quasi) pronti per la produzione

Secondo scenario

- L'utente accede con le credenziali INFN-AAI alla WebUI ed effettua l'enrollment di un Token
- Una volta attivato il Token, il secondo fattore sarà richiesto per qualunque accesso Web protetto da autenticazione INFN-AAI (SAML o OIDC)

- Pro:
  - Nessun overhead per help-desk/servizioXYZ
  - Utilizzo subito il mio secondo fattore
- Con:
  - NON siamo ancora pronti per la produzione

Primo scenario: ToDo

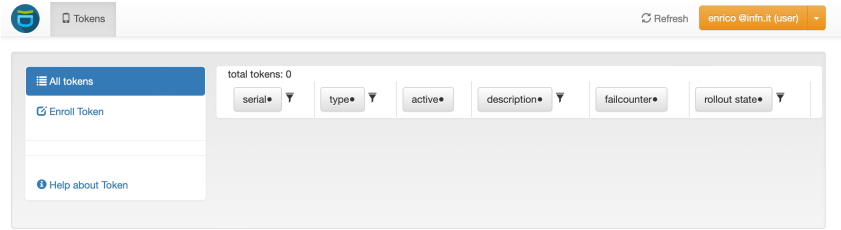
- Includere il plug-in privacyIDEA nell'IdP di produzione (test di funzionalità già effettuati)
- Definire la lista dei SP (ed eventualmente dei ruoli) da proteggere con 2FA.

Secondo scenario: ToDo

- Proteggere l'accesso alla WebUI con autenticazione INFN-AAI (SAML o OIDC)
- Registrare in GODiVA lo stato di «2fa-enabled» (via trigger interni a privacyIDEA)

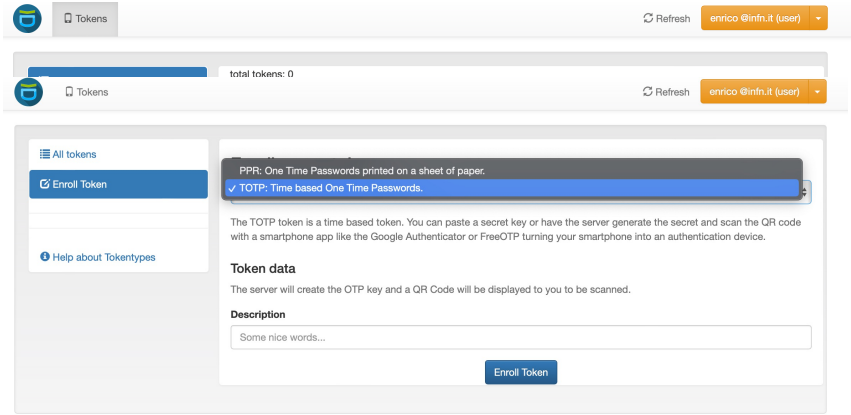
Acquisizione del token

- L’utente effettua il login



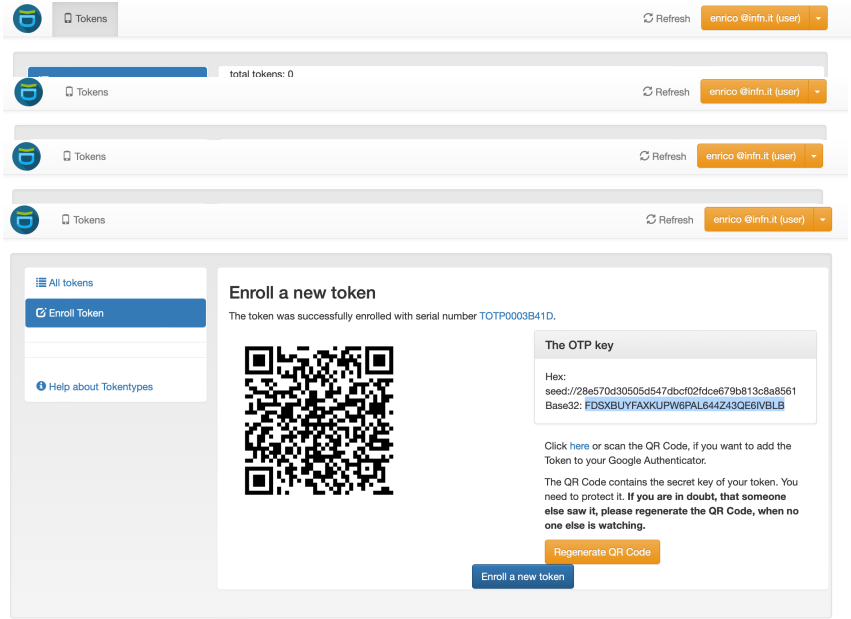
Acquisizione del token

- L’utente effettua il login
- Enroll token
  - Sceglie TOTP o PPR



Acquisizione del token

- L'utente effettua il login
- Enroll token
  - Sceglie TOTP o PPR
  - Inserisce una descrizione
- Acquisisce il seed via QR-code o HEX
- Memorizzare il seed in una applicazione (privacyIDEA, Google Authenticator, Bitwarden,…)



Conclusioni

- Saremmo pronti per accendere il secondo fattore nel primo scenario, ma a mio parere sarebbe meglio optare per il secondo scenario.
- In ogni caso rimangono fuori i servizi web che si autenticano via LDAP (baltig, Alfresco, …). Siamo in attesa di una quotazione da parte di NetKnights per il supporto enterprise
- Tutto quanto sopra si applica ad autenticazione ed autorizzazione per i servizi nazionali collegati al INFN-AAI.
- In linea di principio è possibile «federare» server privacyIDEA di realm differenti per concentrare l'autenticazione anche per servizi di sede, ma non abbiamo effettuato prove.

The End

Grazie

Domande?

2FA

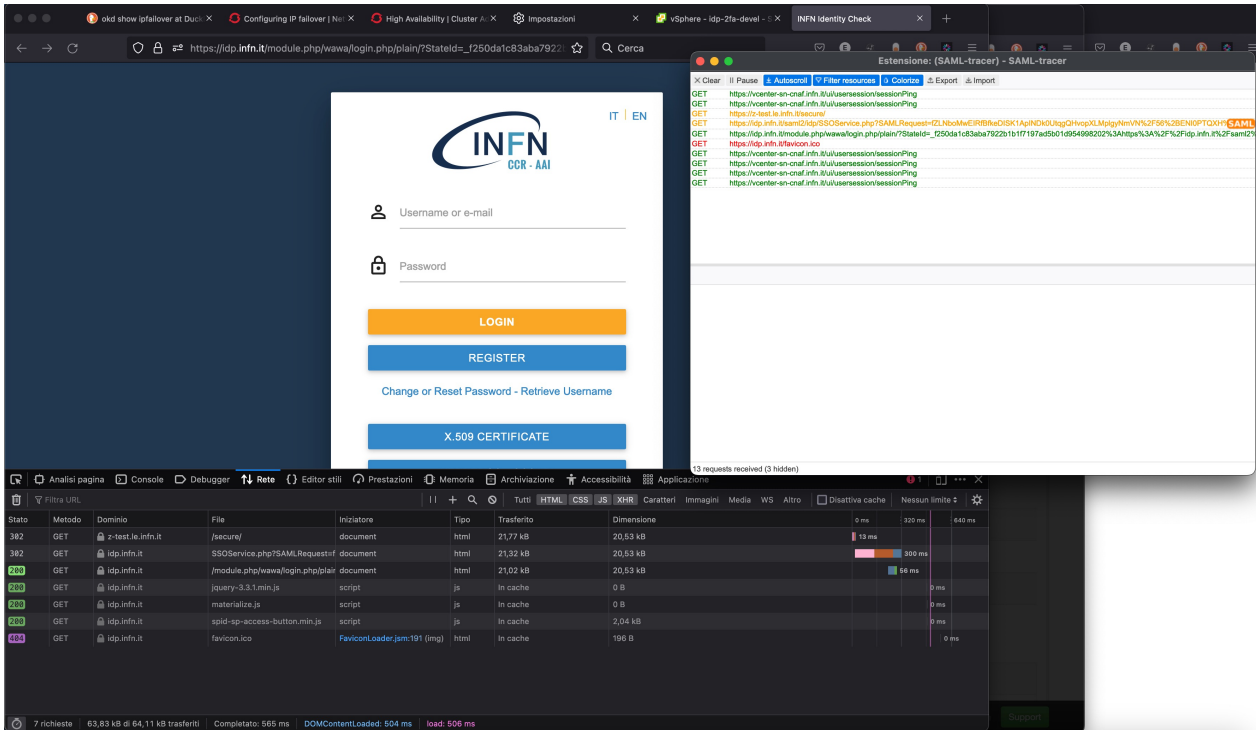
INFN
CCR - AAI

Backup slides

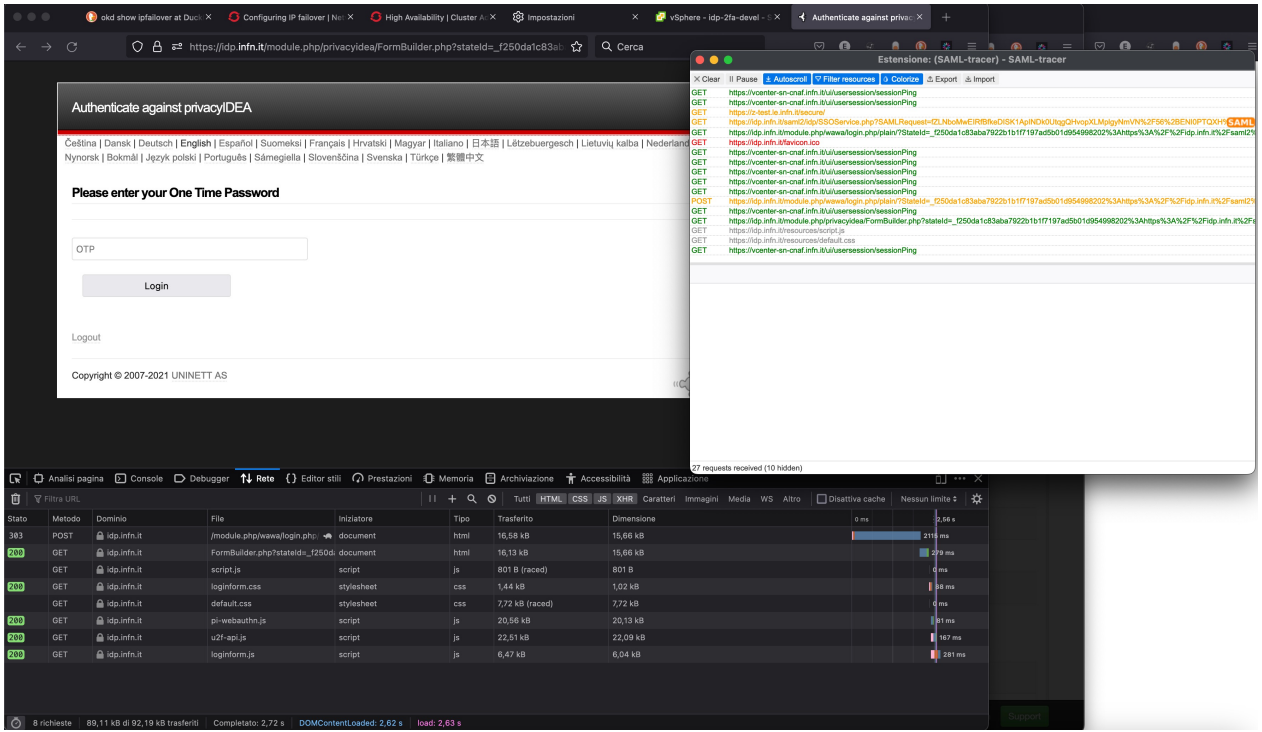
Test PrivacyIDEA & SSP

- Server su https://aai-pi-devel.infn.it/
- IdP di sviluppo in https://idp-dev-2fa.infn.it/
- SP su VM in VirtualBox (presto in https://aai-48-222.infn.it/)
- /etc/hosts riconfigurato per
  - ldp.infn.it → idp-pi-devel.infn.it
  - z-test.le.infn.it -> VM VirtualBox

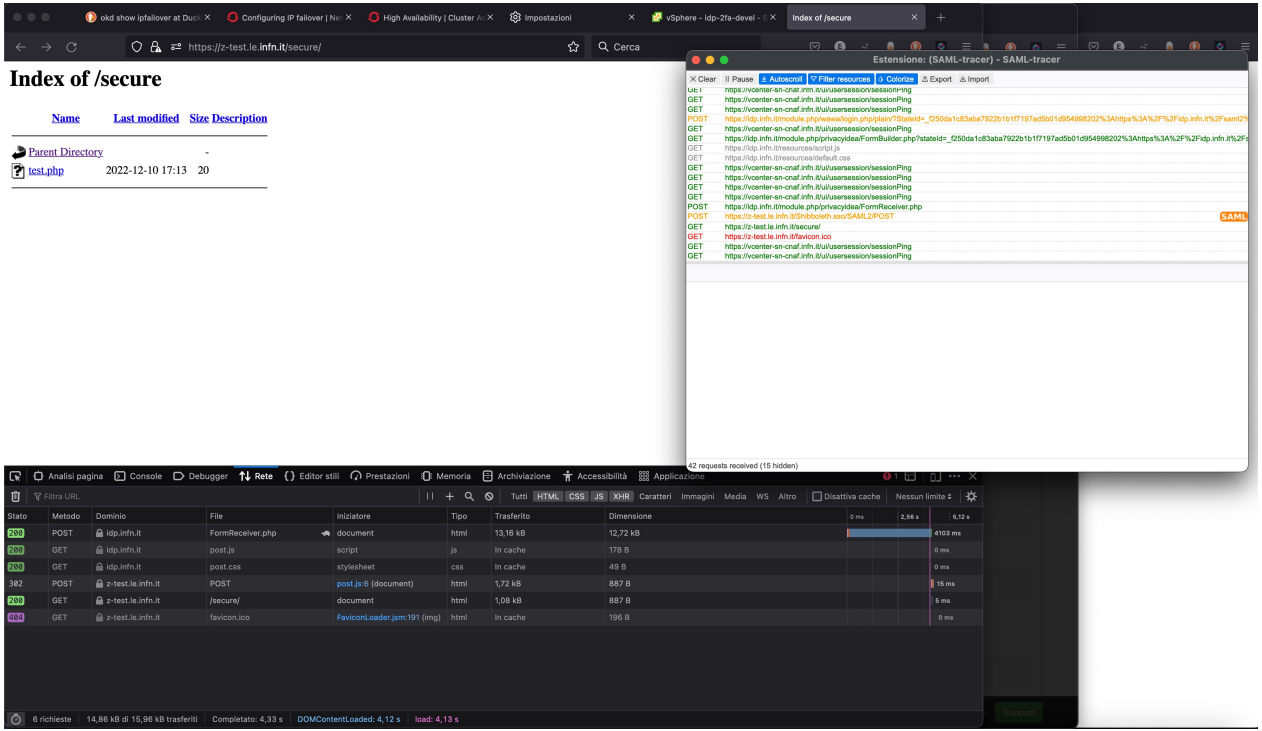
https://z-test.le.infn.it/secure –> IdP



Login → 2FA request page



OTP → access granted



SAML authproc PrivacyideaAuthProc

```
  'authproc' =>
  array (
    75 =>
    array (
      'class' => 'core:GenerateCF',
      'attrname' => 'codiceFiscale',
    ),
    20 => array(
       'class'             => 'privacyidea:PrivacyideaAuthProc',
        /**
         * Enter the URL to your privacyIDEA instance.
         * Required.
         */
        'privacyideaServerURL' => 'https://aai-pi-devel.infn.it',

        /**
         * Enter the realm, where your users are stored.
         * Optional.
         */
       'realm'             => 'infn.it',
       'uidKey'            => 'uid',
       'sslverifyhost'     => true,
       'sslverifypeer'     => true,
       'serviceAccount'    => 'service',
/**     'servicePass'       => 'service',
*/      'serviceRealm'      => 'service',
        /**
         * Set doSendPassword to 'true' to send a request to validate/check with the username
         * and an empty pass prior to the login.
         * This can be used to trigger challenges depending on the configuration in privacyIDEA
         * and requires no service account. If 'doTriggerChallenge' is enabled, this setting has no effect.
         * The value has to be a string.
         * Optional.
         */
        'doSendPassword' => 'false',
        /**
         * Set custom hints for the OTP and password fields
         */
        'otpFieldHint' => 'Insert your PIN and OTP (no other char)',
        'passFieldHint' => 'Password',
    ),
```

Role-based 2FA request

```
        /**
         * Per value in excludeEntityIDs, you may specify another set of regular expressions to match the
         * attributes in the SAML request. If there is a match in any attribute value, this filter will
         * set the state variable to true and thereby enable privacyIDEA where it would be normally disabled
         * due to the matching entityID. This may be used to enable 2FA at this entityID only for privileged
         * accounts.
         * The key in includeAttributes must be identical to a value in excludeEntityIDs to have an effect!
         *
         * Optional.
         */
        'includeAttributes' => array(
            '/http(s)\/\/conditional-no2fa-provider.de\/(.*)/' => array(
                'memberOf' => array(
                    '/cn=2fa-required([-_])regexmatch(.*),cn=groups,(.*)/',
                    'cn=2fa-required-exactmatch,ou=section,dc=privacyidea,dc=org'
                ),
                'myAttribute' => array(
                    '/(.*)2fa-required/', '2fa-required',
                )
            )
```

Test SSH

- RL7 (CentOS7) con pam_krb5+LDAP, python 2.7
- RL8/9 (Alma Linux) con sssd krb5+LDAP multi-domain (roma1+bologna)
  - ~~Funziona~~ anche con python 3 (anche se non è certificato dal produttore)
    - Non corretta interazione con pam_sssd/direttive pam

```
~]# grep ^auth /etc/pam.d/sshd
auth        required      pam_sepermit.so
auth        substack      password-auth
auth        sufficient    pam_python.so \
  /usr/lib/python2.7/site-packages/privacyidea_pam-2.11dev0-py2.7.egg/privacyidea_pam.py \
  cacerts=/etc/pki/ca-trust/extracted/pem/tls-ca-bundle.pem \
  url=https://aai-pi-devel.infn.it debug realm=infn.it prompt=Insert_OTP
auth        include       postlogin

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication yes
```

SSH login

```
o → ssh enrico@aai-ws0-devel.infn.it
(enrico@aai-ws0-devel.infn.it) Password:
(enrico@aai-ws0-devel.infn.it) Insert_OTP:
X11 forwarding request failed on channel 0
Last login: Tue Mar 21 10:21:05 2023 from dxcnaf3.infn.it
Could not chdir to home directory /afs/infn.it/user/e/enrico: No such file or directory
/usr/bin/id: cannot find name for group ID 30010
[enrico@aai-ws0-devel /]$
```

Conclusioni su privacyIDEA & plugins

- Lo strumento offre tutte le funzionalità che ci servono ora e si è dimostrato sinora stabile, robusto ed attivamente sviluppato
  - Siamo partiti a Dicembre con la 3.7 ora è alla versione 3.8.1
  - In fase di rilascio la versione del plug-in SAML per SSP1.19
- È necessario un po' di lavoro aggiuntivo per
  - Configurare a modo i vari plugin;
  - Verificare la loro interazione on altri sistemi (vedi sssd);
  - Disegnare una pagina web decente per la richiesta del secondo fattore;
  - Configurare il servizio in produzione;
  - Test di scalabilità e resilienza;