MFA & IDEM/REFEDS

Tutorial days CCR 29 novembre 2023

Enrico M.V. Fasanelli

Prologo

- Provo ad usare alcune tecniche descritte ieri da Monica De Simone
- Ovviamente la presentazione ieri era già pronta e quindi non è stata costruita attorno a quelle tecniche che non risultano quindi “integrate”
- Timing (a frequenza variabile)
  - Ho inserito alcuni “separatori” nelle slides tra un argomento e l’altro per prendere domande relative all’argomento appena trattato.
- Feedback (o, se volete, alarm-clock)
  - Codice menti.com

Agenda

- Autenticazione Multifattore
  - Due parole su Autenticazione e Fattori
  - Il software e l'architettura del sistema
  - La configurazione implementata
  - Gestione del token
  - Utilizzo del secondo fattore
- Profili IDEM/REFEDS e configurazione di SP SAML
  - I profili IDEM ed i corrispondenti profili REFEDS
  - Casi d'uso e configurazioni SP

menti.com 52 25 18 0

- https://www.menti.com/alf99rxr8kpq

Fattori di Autenticazione

Autenticazione: conosci; hai; sei

- La verifica del fatto che chi si presenta davanti ad un sistema informatico sia chi dice di essere si può effettuare attraverso:
  - qualcosa che si conosce (password)
  - qualcosa che si possiede (telefono, token, applicazione certificata)
  - qualcosa che si è (caratteristiche del corpo → biometria)
- Quando l'autenticazione richiede più di uno di questi metodi, si parla di Autenticazione a 2 fattori o 2FA (o a molti fattori: MFA)

Perché MFA/2FA?

- Le password ***dovrebbero*** essere mantenute come il segreto più prezioso, ma di fatto non tutti gli utenti prestano adeguata attenzione e cadono nelle trappole degli «estorsori di credenziali»
- Questo espone sia i dati personali del possessore della password, sia i sistemi a cui tale utente può accedere, esponendoli
  - all'utilizzo improprio (ad esempio mail SPAM)
  - **ad un disastro informatico** (ransomware con perdita di possesso dei dati)
- La richiesta di due fattori differenti (e non semplicemente due password) rende molto più difficile, se non impossibile, il lavoro degli estorsori di credenziali, salvaguardando sia i dati che i sistemi informatici.

Quale secondo fattore?

- Anche se l'accesso via caratteristiche biometriche è sempre più in voga su sistemi personali (Touch-ID/Face-ID) il suo dispiegamento nel contesto INFN sarebbe troppo oneroso (se non altro nel rapporto costi/benefici)
- L'unica strada veramente perseguibile è quella del «qualcosa che si possiede»
  - Telefono
  - Token
  - Applicazione certificata
  - …

Autenticazione: conosci; hai; sei

- La verifica del fatto che chi si presenta davanti ad un sistema informatico sia chi dice di essere si può effettuare attraverso:
  - qualcosa che si conosce (password)
  - qualcosa che si possiede (telefono, token, applicazione certificata)
  - qualcosa che si è (caratteristiche del corpo→biometria)
- Quando l'autenticazione richiede più di uno di questi metodi, si parla di Autenticazione a 2 fattori o 2FA (o a molti fattori: MFA)

Tutorial days CCR - 29 novembre 2023 Autenticazione Multifattore - Enrico M. V. Fasanelli 3

Token

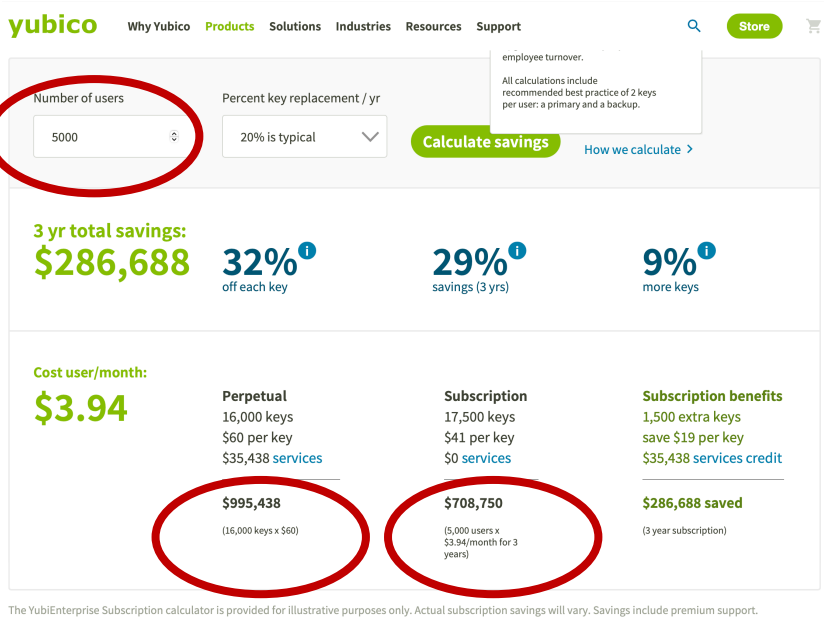
- Standardizzazione definita via RFC dalla *Initiative for Open AuTHentication* (OATH)
  - HOTP – An HMAC-Based OTP Algorithm (RFC 4226)
  - TOTP – Time-based One-time Password Algorithm (RFC 6238)
  - OCRA – OATH Challenge/Response Algorithms Specification (RFC 6287)
- Token hardware
  - Dimensioni tipiche di un portachiavi o di una smartcard che al loro interno contengono un piccolo apparato elettronico in grado di generare un codice univoco che dipende dall'apparato stesso oltre che dall'algoritmo.
- Token software
  - Implementazioni in SW delle funzionalità di un Token hardware

“Token” software

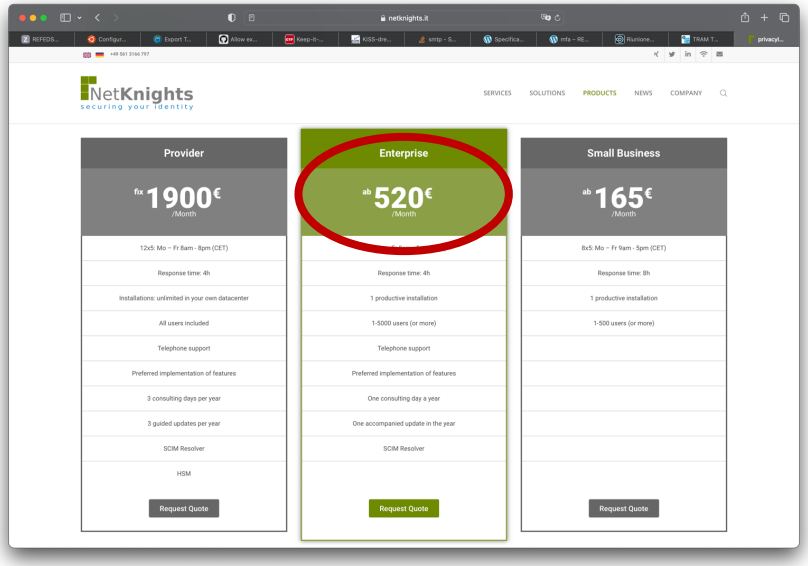
- Normalmente con “Token” si indica un oggetto; “qualcosa di fisico”
- Siccome l’oggetto implementa un algoritmo è naturale estendere questo nome ad un software e parlare di “Token Software” (tipicamente implementato in App per smartphone).
- Il “Token Software” fornisce le stesse funzionalità di un token hardware.
- Nella classificazione delle modalità di gestione dei fattori di autenticazione, si da un ulteriore salto logico, integrando in “Token Software” anche “processi” o “workflow” che permettono la gestione di un fattore di autenticazione
  - Ricezione di un codice usa-e-getta via e-mail o SMS
  - Stampa di una serie di codici usa-e-getta

Hardware o software?

Hardware



Software



Token software

- Oltre all'evidente "vantaggio" economico il token software presenta un atrettanto importante vantaggio operativo
  - Indipendenza dalla disponibilità di un singolo ogetto fisico
  - Vasta scelta di App per la gestione dei token e l'ottenimento dei codici di accesso






menti.com 52 25 18 0

- https://www.menti.com/alf99rxr8kpq

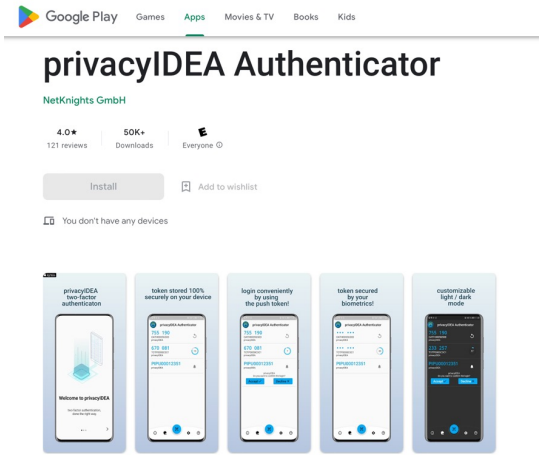
privacyIDEA Authentication System

privacyIDEA Authentication System (1)

- Sistema di Autenticazione modulare
- Inizialmente sviluppato per la gestione di autenticazione con OTP
- Gira su sitemi Linux
- OpenSource, rilasciato con licenza AGPLv3
- Supporta vari tipi di «tokens» (noi abbiamo deciso di usarne solo uno)
- Multi-REALM
- Tre layers:
  - API;
  - Libreria;
  - Database

privacyIDEA Authentication System (2)

- Web UI per amministrazione
- Autenticazione via API o Plug-in (disponibili per FreeRADIUS, SimpleSAMLphp, WordPress, DokuWiki, PAM, …)
- 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

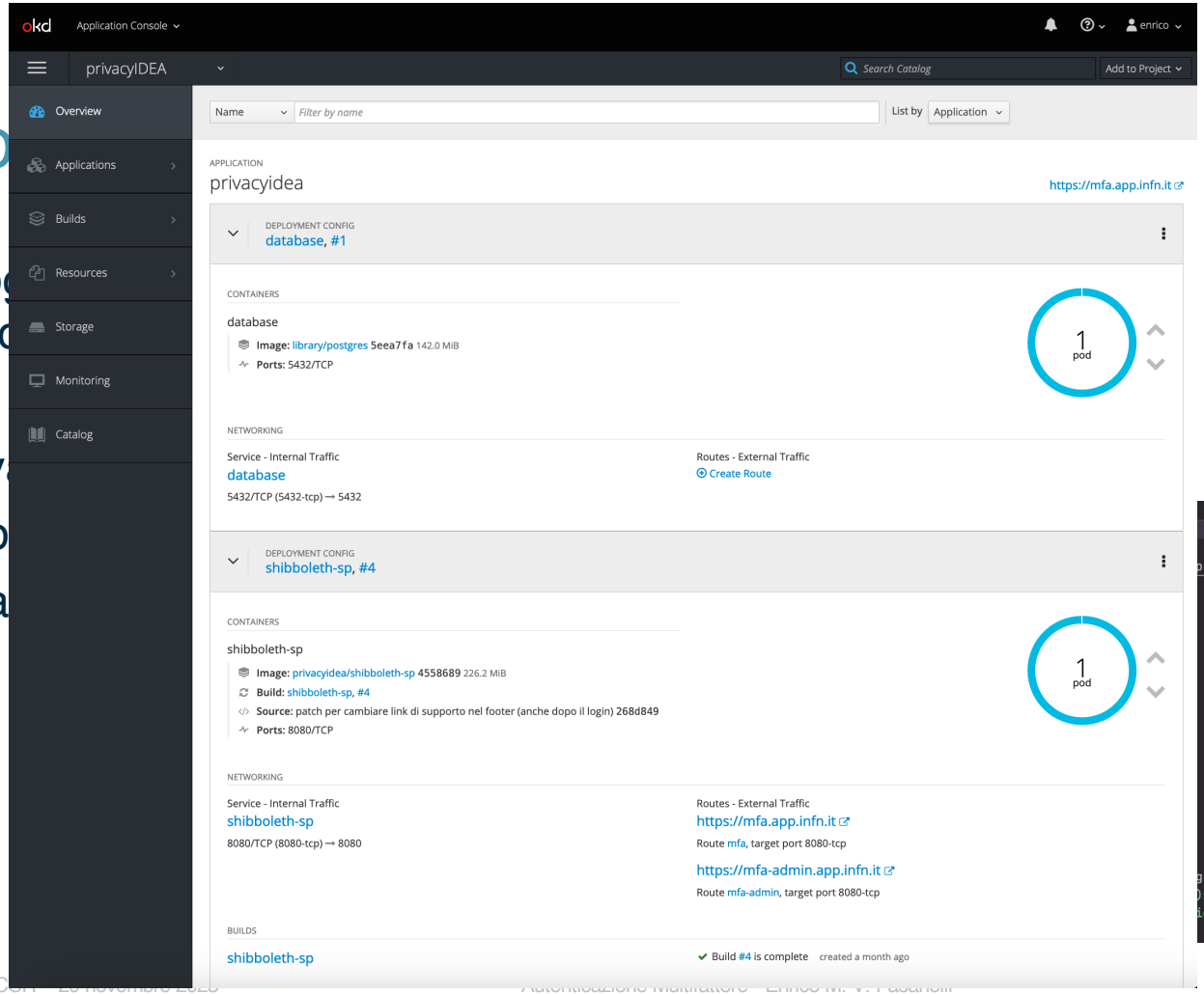
- Progetti nei cluster OKD (dev, pre e prod)
- DB postgresql
- privacyIDEA 3.8.1 Docker image
  - psycopg2 (PostgreSQL driver)
  - apache 2.4 con moduli shib e wsgi

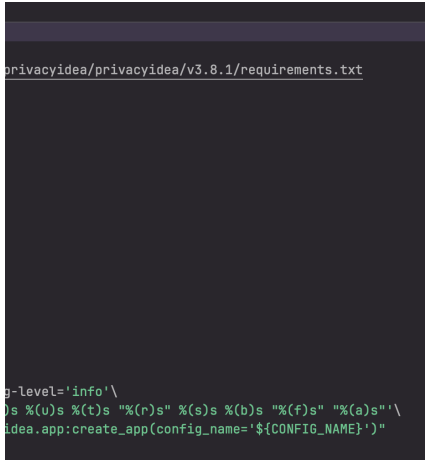
Dockerfile

```
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}')"

```

Il no

- Prog
  proc
- DB
- priv
  - p
  - a





Cosa proteggere con il secondo fatore

Due scenari

- Applicazioni e/o ruoli
  - Abilitare il secondo fattore solo per servizi e/o ruoli selezionati
    - Servizi di tipo amministrativo
    - Ruoli con privilegi da amministratore

- Autenticazione in sé (e quindi tutto quello che c'è dietro)
  - 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).

MFA in contesto IDEM/eduGAIN

- INFN-AAI gestisce un IdP registrato in IDEM (e quindi in eduGAIN)
- Il profilo MFA in eduGAIN è regolamentato 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.

MFA in contesto IDEM/eduGAIN

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

MFA in contesto IDEM/eduGAIN

- INFN-AAI gestisce un Id
- Il profilo MFA in eduGA
- Il 24 maggio 2023 l'asse 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.

Scelta «secondo» scenario

- Auto-enrollment del token TOTP via credenziali INFN-AAI
  - Registrazione dello stato di «mfa-enabled» in GODiVA
  - Notifica dell'avvenuto rilascio del token
  - Attivazione del MFA per tutti i servizi

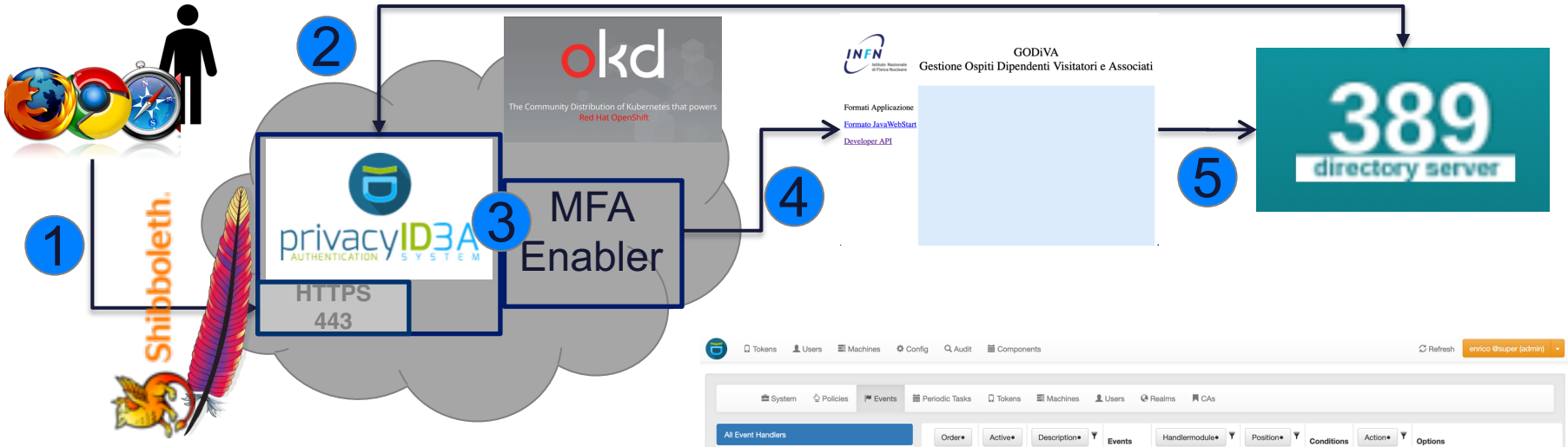
Scelta «secondo» scenario

- Auto-enrollment del token TOTP via credenziali INFN-AAI
  - Registrazione dello stato di «mfa-enabled» in GODiVA
  - Notifica dell'avvenuto rilascio del token
  - Attivazione del MFA per tutti i servizi

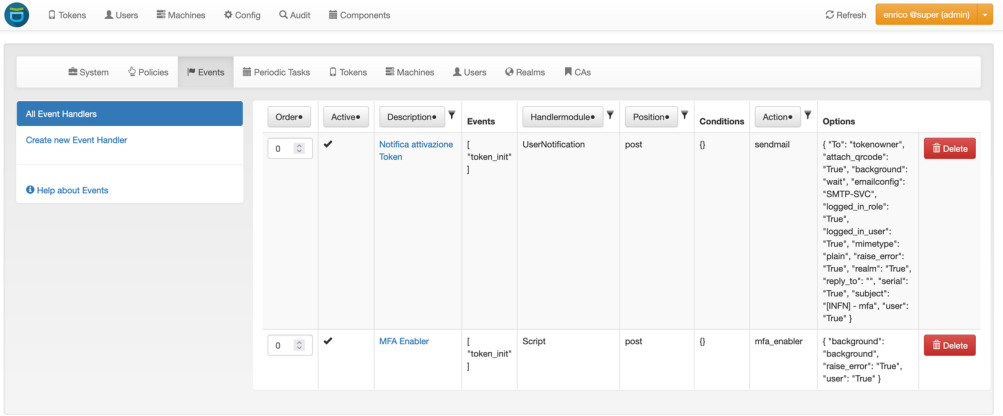
MFA Enabler

- Python script «home made» inserito nel container di privacyIDEA che interagisce on le API di GODiVA (definito apposito «dettaglio» e relativo automatismo di sincronia verso LDAP)
- Notifica dell'avvenuto enrollment di un token via automatismi di privacyIDEA
- MFA richiesta per tutti i servizi web protetti dall'IdP, via modulo privacyIDEA per simpleSAMLphp

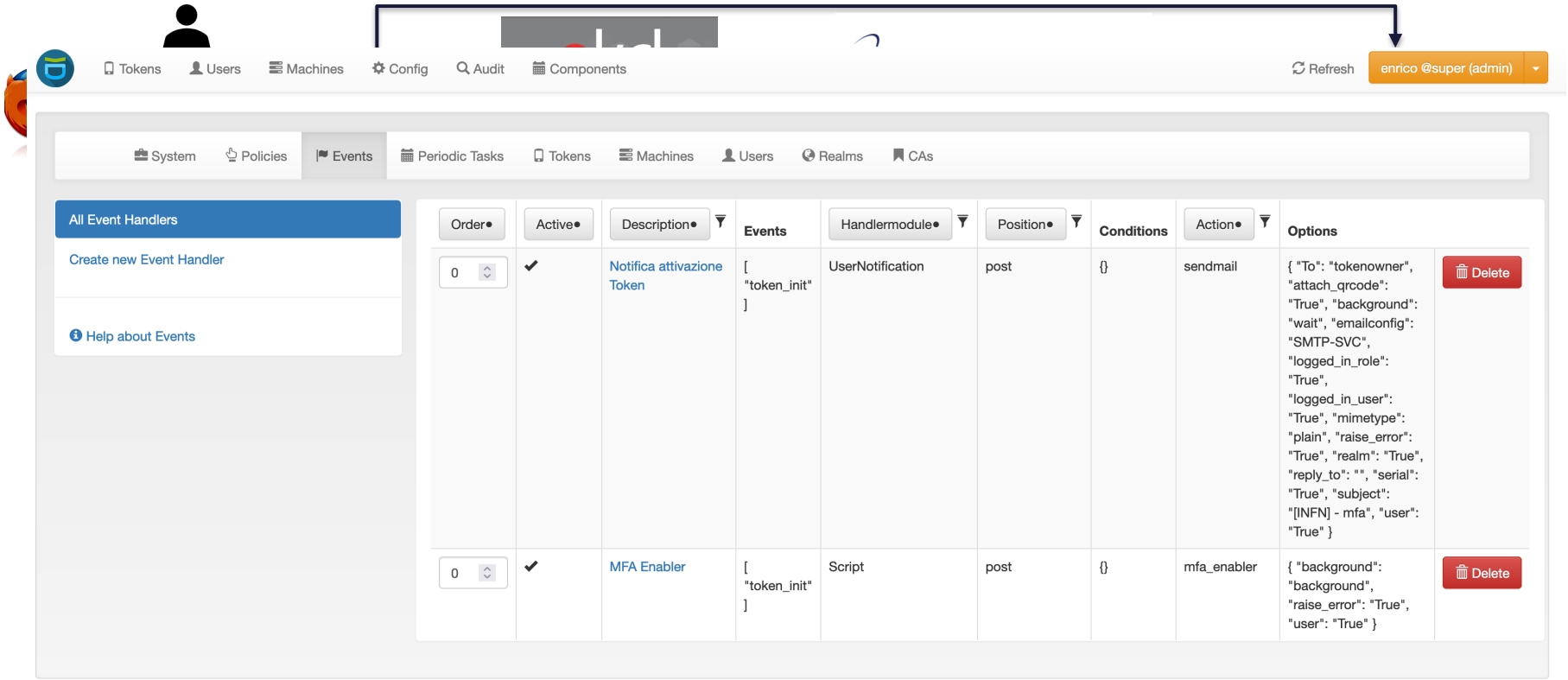
Architettura privacyIDEA + MFA-enabler



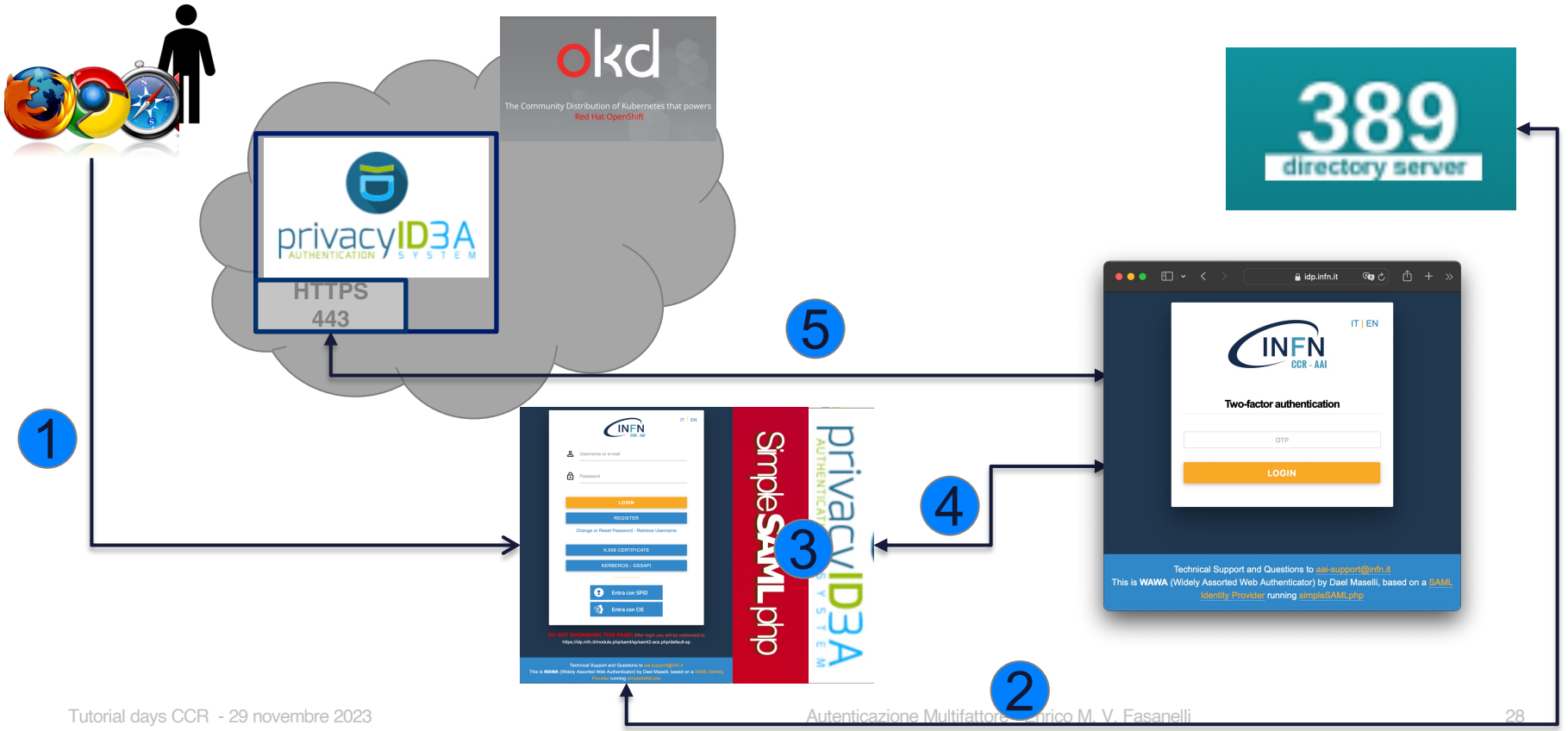
https://mfa.app.infn.it/



Architettura privacyIDEA + MFA-enabler



Architettura login con MFA



Architettura login con MFA

```
/**…
'excludeEntityIDs' => array(
    '/https:\/\/vault.infn.it\/shibboleth\/',
    '/https:\/\/vault-security.infn.it\/shibboleth\/',
    '/https:\/\/(.*).infn.it\/(.*)/',
),

/**…
'includeAttributes' => array(
    '/https:\/\/(.*).infn.it\/(.*)/' => array(
        'schacUserStatus' => array(
            '/urn:schac:userStatus:it:infn.it:mfa:enabled/',
        )
    )
)
```

1

2

Pilota MFA

INFN
CCR - AAI

Acquisizione ed utilizzo del token

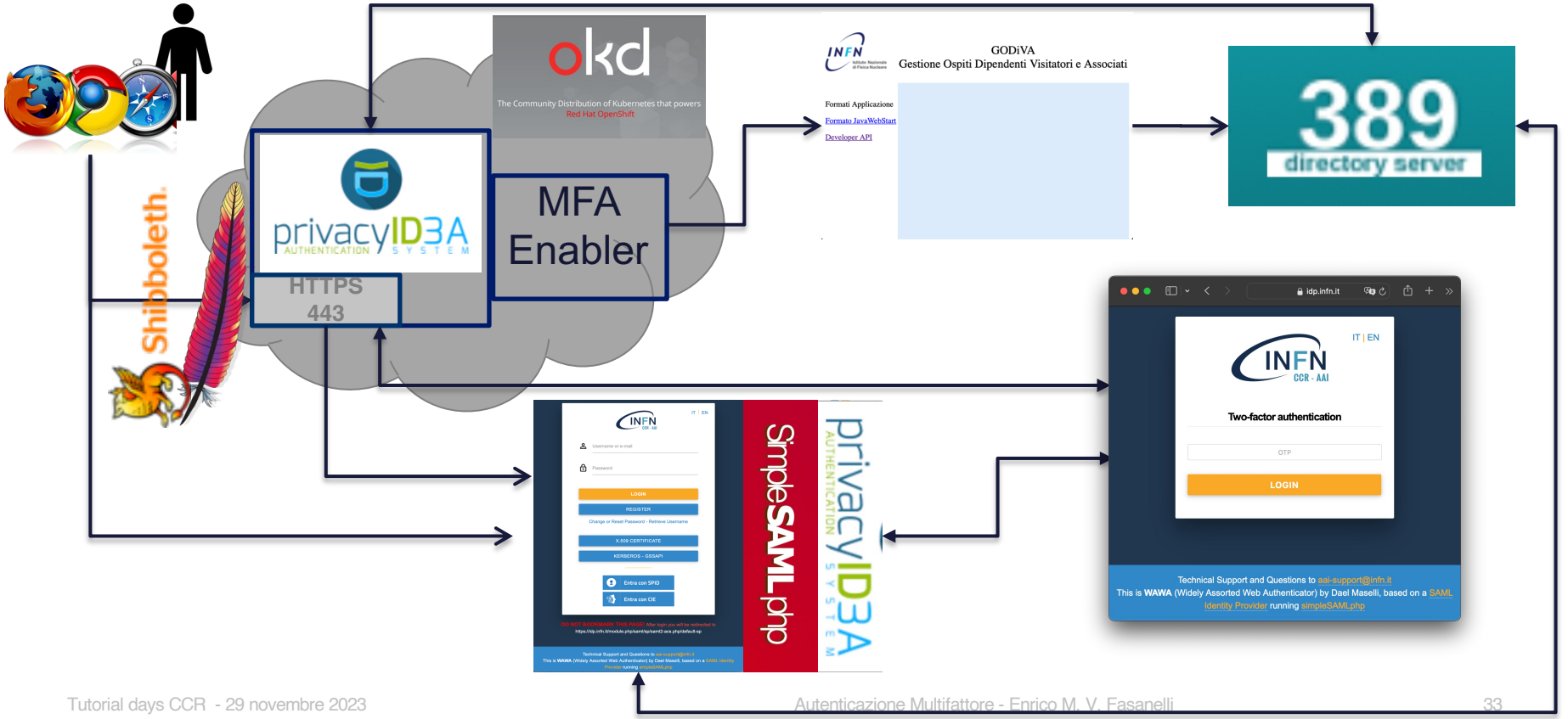
menti.com 52 25 18 0

- https://www.menti.com/alf99rxr8kpq

Pilota MFA

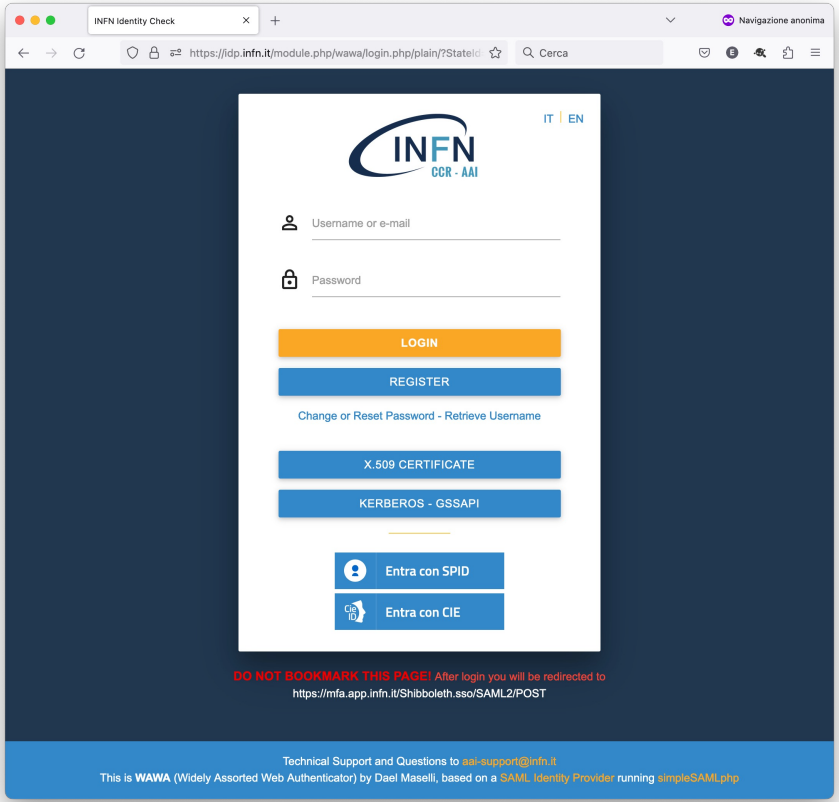
- Dallo scorso 31 ottobre è partita una fase pilota per l'utilizzo del secondo fattore di autenticazione
- Invito inviato ai componenti dei servizi calcolo e reti, ma il pilota è aperto a tutti
- Lo scopo è di verificare sia l'infrastruttura che le policy definite
  - Secondo fattore richiesto per l'accesso a qualunque servizio con la sola esclusione di https://vault.infn.it/
  - Auto-enrollment via autenticazione INFN-AAI
  - Gestione tokens via INFN-AAI+MFA
- Feedback/Richieste di supporto via e-mail ad aai-support@infn.it

Acquisizione e gestione di tokens



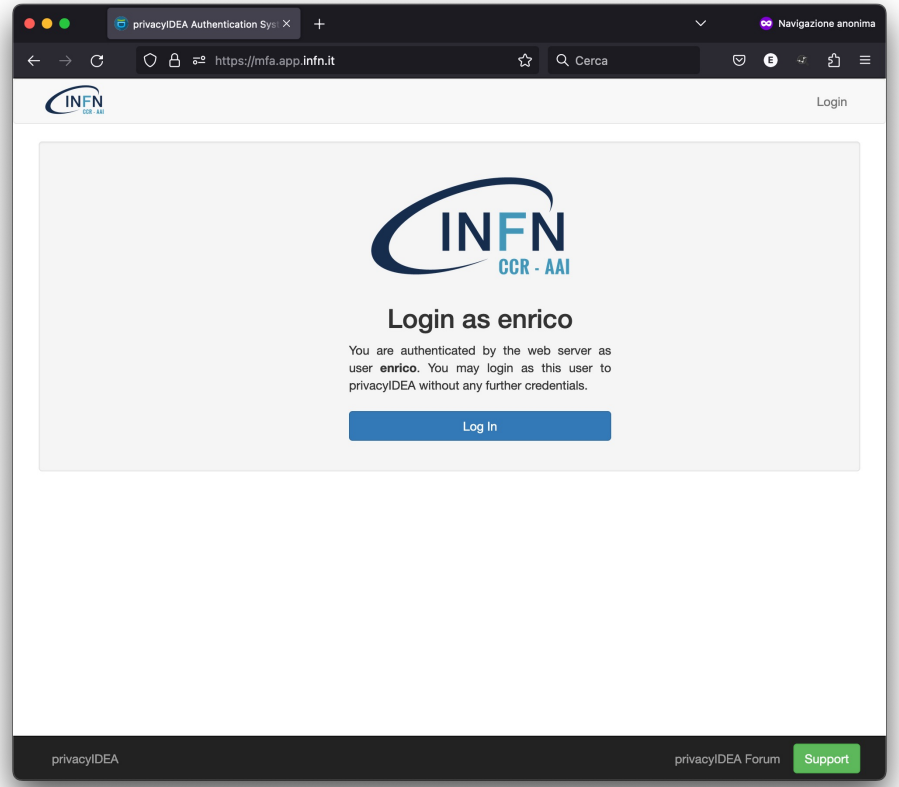
Acquisizione del token

- Si accede alla URL https://mfa.app.infn.it/



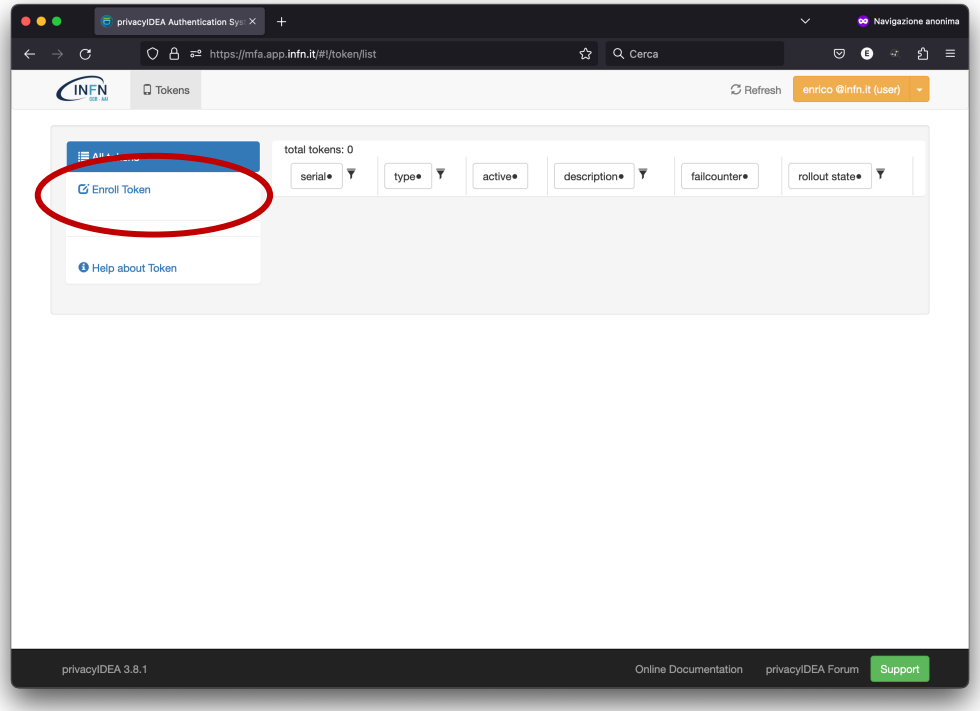
Acquisizione del token

- Si accede alla URL https://mfa.app.infn.it/
- Si entra nel sistema MFA



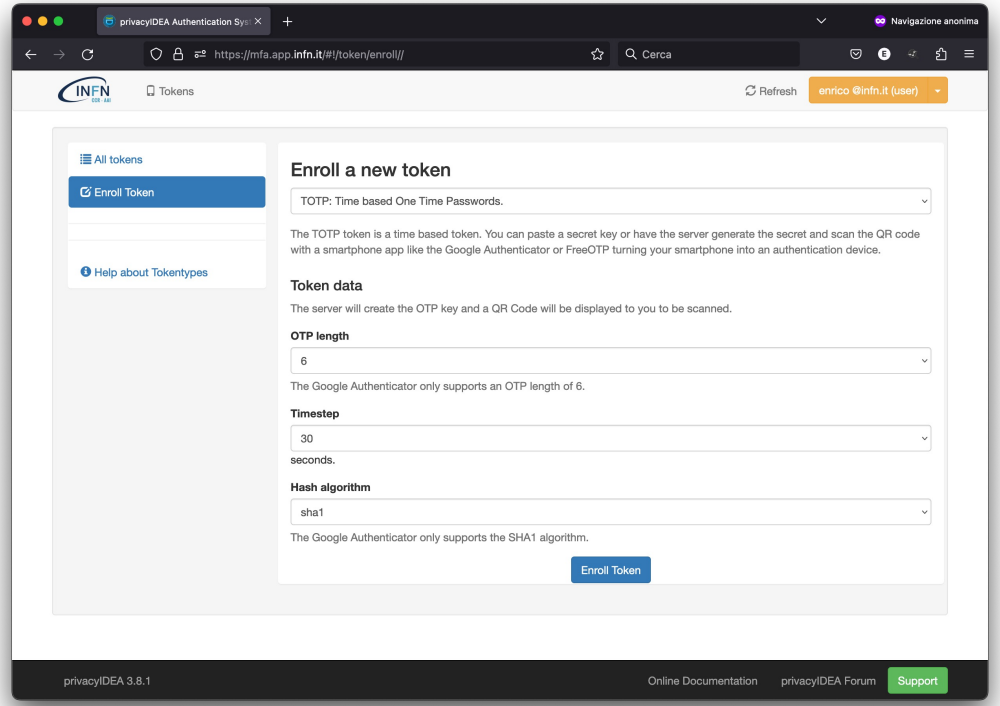
Acquisizione del token

- Si accede alla URL https://mfa.app.infn.it/
- Si entra nel sistema MFA
- Gestione Token



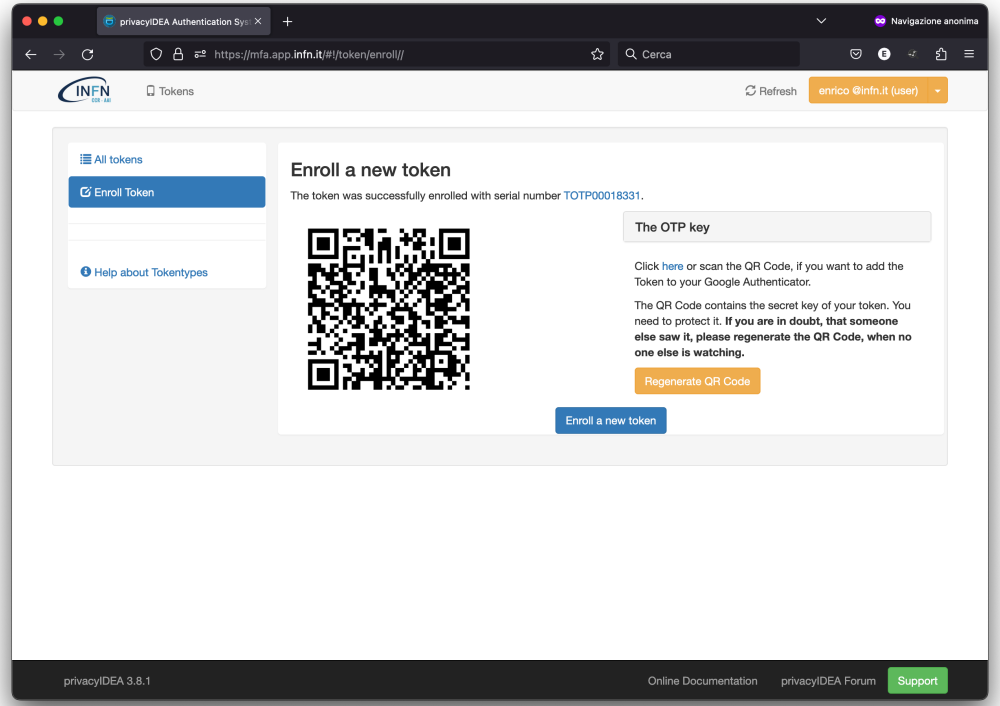
Acquisizione del token

- Si accede alla URL https://mfa.app.infn.it/
- Si entra nel sistema MFA
- Gestione Token
- Enroll token



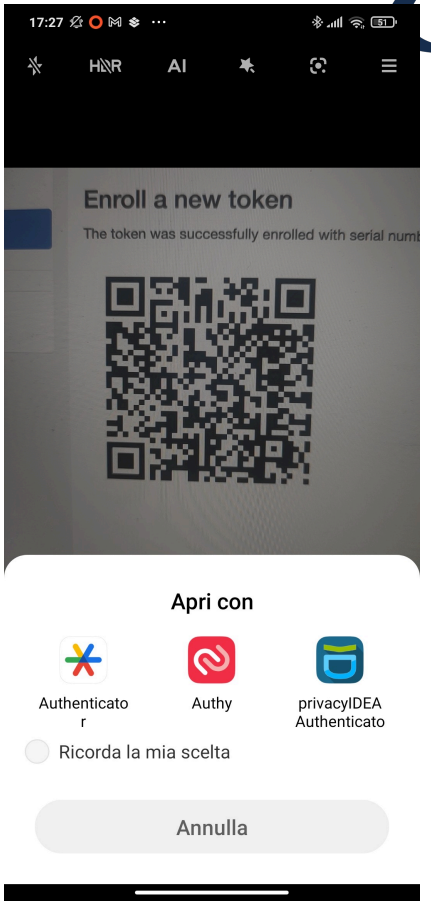
Acquisizione del token

- Si accede alla URL https://mfa.app.infn.it/
- Si entra nel sistema MFA
- Gestione Token
- Enroll token
- QR code



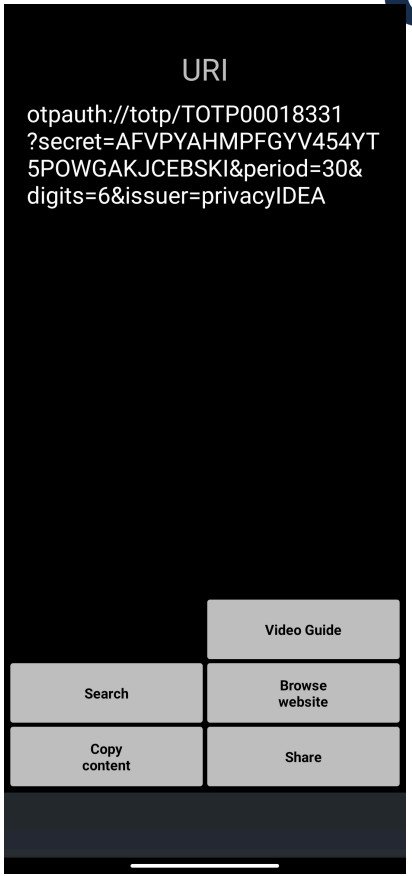
Acquisizione del token

- Si accede alla URL https://mfa.app.infn.it/
- Si entra nel sistema MFA
- Gestione Token
- Enroll token
- QR code nello smartphone



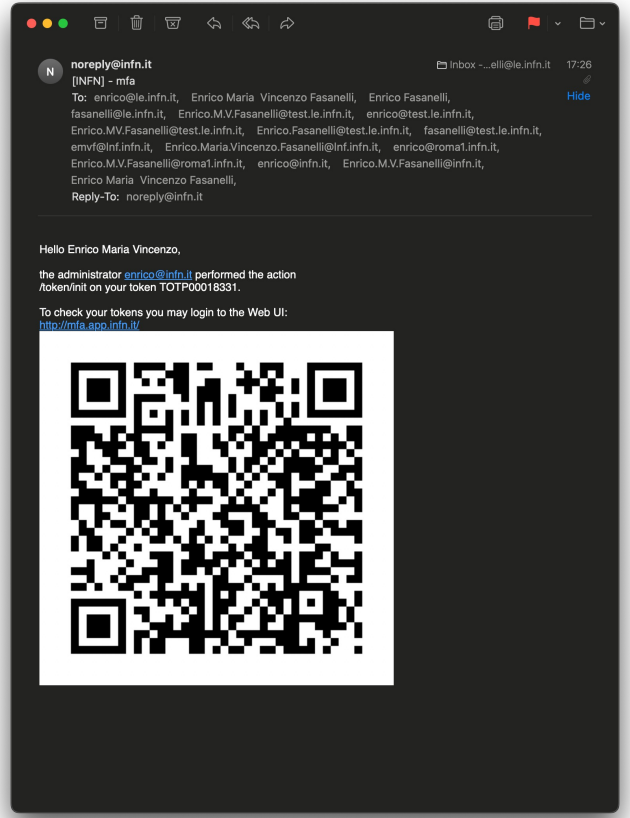
QRcode e segreto

- Un qualunque QRcode Reader visualizza le caratteristiche del token ed in particolare il **secret** in formato base32 e le caratteristiche dell'OTP
- Esporre il QRcode equivale ad esporre il **sistema per il calcolo dell'OTP** e compromettere quindi il secondo fattore



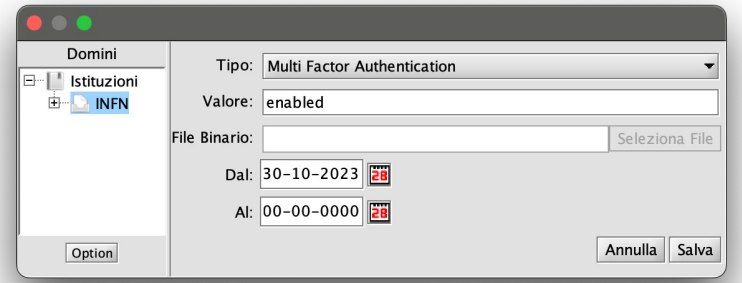
Notifiche

- Il processo di acquisizione del token invia un mail a tutti gli indirizzi contenuti in mailAlternateAddress
- Il QRcode non viene più inviato (molti usano indirizzi e-mail tipo gmail e comunque non è garantita la cancellazione del mail)



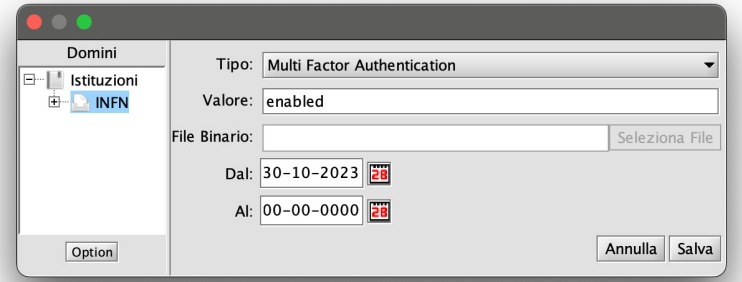
MFA enabled

- L’emissione del token comporta la registrazione in GODiVA del valore «enabled» nell’attributo «Multi Factor Authentication»



MFA enabled

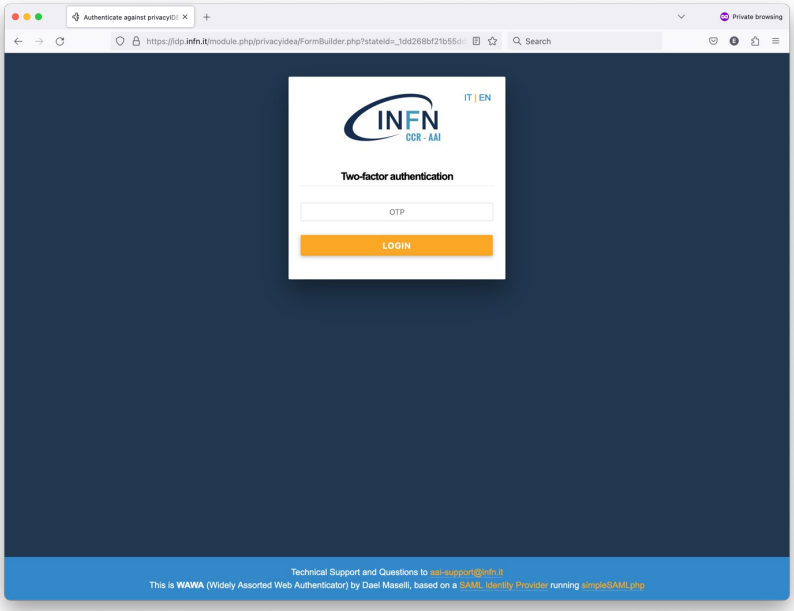
- L’emissione del token comporta la registrazione in GODiVA del valore «enabled» nell’attributo «Multi Factor Authentication»
- In corrispondenza, in LDAP compare un nuovo valore dell’attributo schacUserStatus




```
 2023-10-31 08:53:16    kirjava in ~
○ → searchds -b ou=people,dc=infn,dc=it  "cn=enrico*fasanelli"
schacUserStatus: urn:schac:userStatus:it:infn.it:mfa:enabled
```

Utilizzo del token

- L’accesso a qualunque SP INFN richiede il secondo fattore a chi ce l’ha (query LDAP su schacUserStatus)
- SSO è abilitato e quindi lo chiede solo 1 volta per ogni sessione (la durata della sessione dell’IdP è 8 ore)

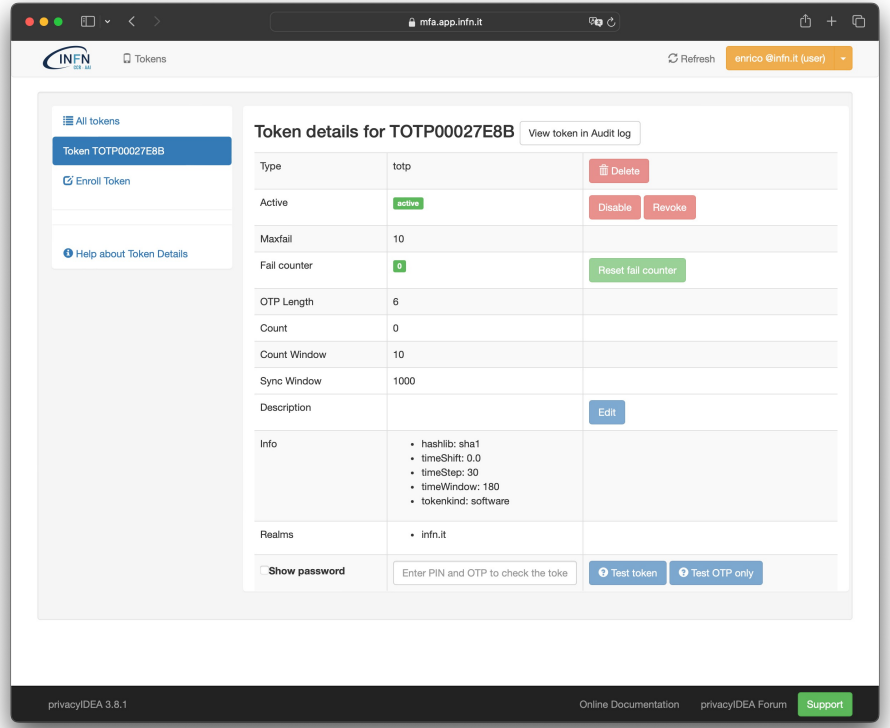


SSO

- Il protocollo SAML prevede che il Service Provider possa ignorare il SSO e richiedere la ri-autenticazione
- Ci sono alcuni SP (in area DSI) che utilizzano questa funzionalità e richiedono ogni volta la ri-autenticazione
  - Libro Firma https://librofirma.dsi.infn.it/
  - Portale DSI https://portale.dsi.infn.it/
- Libro Firma sarà presto sostituito con il nuovo (per il quale sarà possibile evitare questo comportamento)
- Stiamo lavorando con la DSI per valutare il da farsi per il loro Portale

Gestione dei Token

- Con le attuali policy, l'unica cosa che l'utente può fare è acquisire nuovi token
- Tutte le altre operazioni su un token NON sono abilitate per ridurre il numero di «errori»



INFN Vault

vaultwarden/Bitwarden

Pillole formative SSNN

- Il prossimo 7 dicembre è prevista la sessione delle pillole formative dei SSN in cui si parlerà di password manager e del relativo servizio https://vault.infn.it/
- Senza voler rubare la scena, sono necessarie un paio di anticipazioni
- Il sistema si basa su **vault**warden che è una implementazione in linguaggio Rust delle API di un server Bitwarden

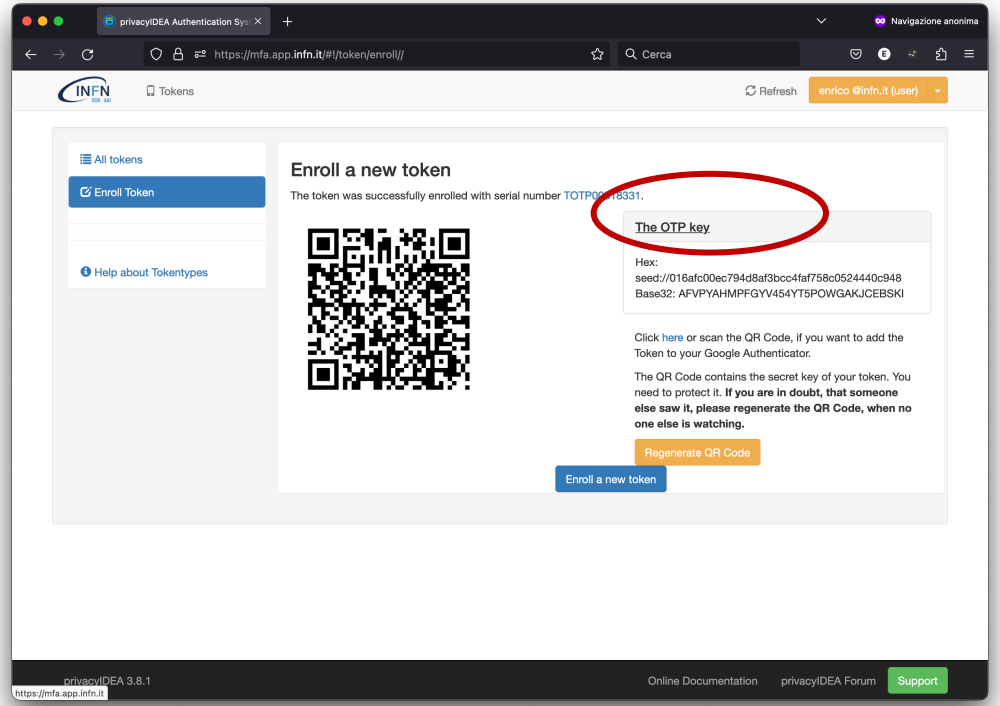
Vault INFN/Bitwarden

- L’accesso avviene in 2 passi
  - INFN-AAI inoltra a vault.infn.it l’indirizzo e-mail
  - vault.infn.it chiede una master-password con cui cifrerà il DB che rimane quindi personale

- Se si dimentica la master-password, non c’è modo di recuperare quanto cifrato in Vault INFN
- La master-password DEVE essere differente da tutte le vostre altre password e deve essere una vera lunga passphrase
- È possibile agganciare un qualunque client Bitwarden (sia App per vari sistemi operativi che estensioni per I vari browser) al Vault INFN

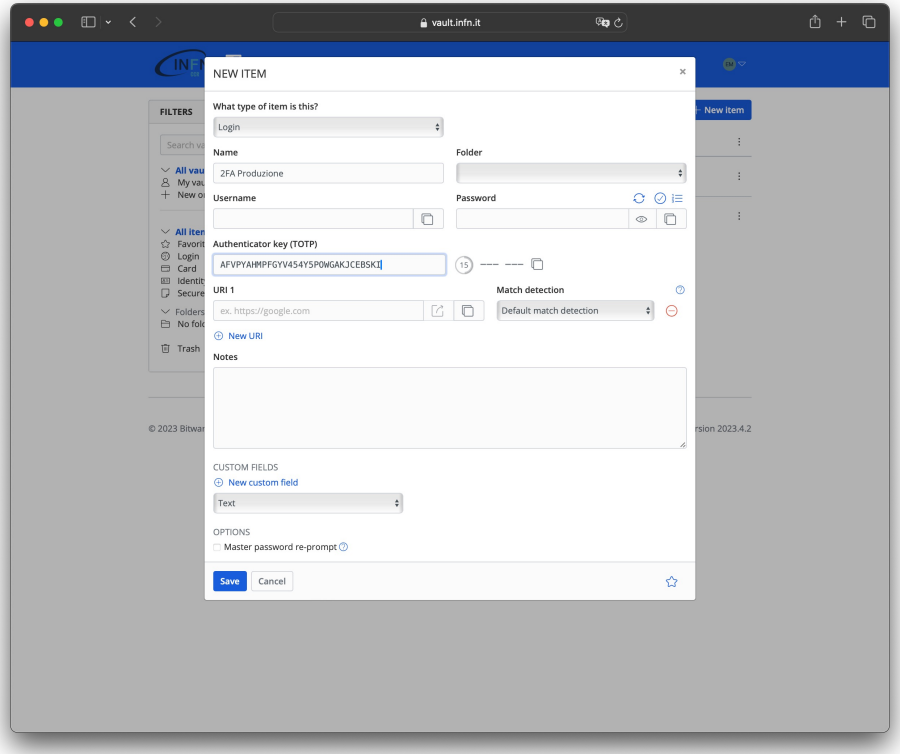
Acquisizione del token

- Si accede alla URL https://mfa.app.infn.it/
- Si entra nel sistema MFA
- Gestione Token
- Enroll token
- QR code nello smartphone
- OTP Key per vault.infn.it o altro autenticatore



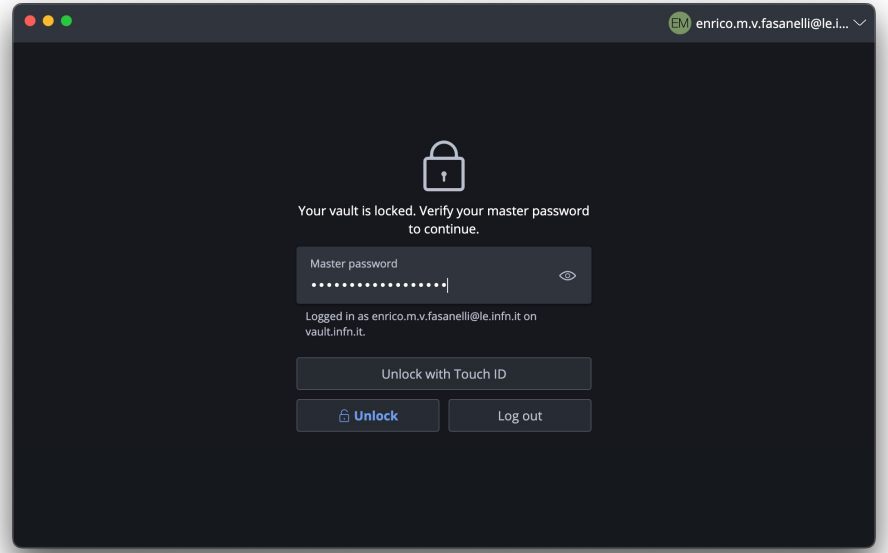
Vault INFN/Bitwarden

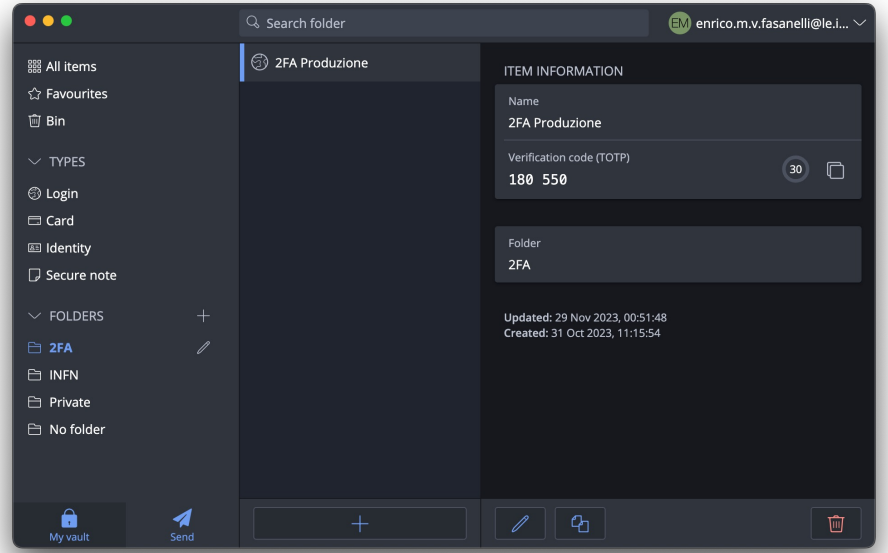
- La chiave in formato base32 può essere memorizzata in vault.infn.it (o nelle app Bitwarden collegate) per poter avere accesso all'OTP in mancanza di altro autenticatore



Utilizzo di Vault INFN per TOTP

- Una volta inserito il codice base32 nel TOTP generator di Vault INFN, qualunque client Bitwarden collegato a vault.infn.it potrà essere usato come generatore TOTP





menti.com 52 25 18 0

- https://www.menti.com/alf99rxr8kpq

Profili di garanzia delle Identità Digitali della Federazione IDEM

Identità Digitali: LoA, IDEM-Px, REFEDS

- Da alcuni anni INFN-AAI ha definito, analogamente a quanto fatto da SPiD e per compatibilità con esso, i livelli di confidenza delle Identità Digitali (di fatto solo LoA1 e LoA2)
- Questi livelli sono compatibili sia con quelli definiti da IDEM che con quelli codificati da REFEDS per eduGAIN
- REFEDS ha definito profili di garanzia specializzandoli sia rispetto alle Identità Digitali (Identity Assurance Levels) che rispetto agli Attributi (Attribute Assurance Level) che rispetto gestione degli identificativi, oltre ad un profilo specifico per la robustezza dell'autenticazione (Autentication Assurance Level)
- IDEM ha definito 4 livelli per i profili di garanzia delle identità digitali, adottando I profili REFEDS per Attributi e robustezza dell'Autenticazione

Identity Provider, ma non solo

- Tutto questo definire profili, livelli e contesti di fatto è un lavoro che spetta all'Identity Provider, in funzione dei dati relativi all'identità ed ai meccanismi di autenticazione.
- I Service Provider, però possono richiedere all'IdP l'attivazione di un definito contesto di autenticazione
  - Ad esempio, un SP può richiedere che l'autenticazione avvenga con secondo fattore o che l'identità digitale abbia determinate caratteristiche e rifiutare l'accesso la risposta dell'IdP non soddisfa la richiesta.
- Quindi l'IdP, oltre a popolare correttamente gli attributi relativi all'Identità Digitale, deve saper rispondere opportunamente alle eventuali richieste effettuate dagli SP

REFEDS Assurance Framework (RAF)

- Gli IdP in federazione eduGAIN (tutti quelli che non hanno espicitamente richiesto di non partecipare) possono utilizzare il contesto di garanzia di REFEDS assegnando opportuni valori all'attributo eduPersonAssurance
- Questi valori hanno una «radice» comune definita da

  $PREFIX$=https://refeds.org/assurance
- Il RAF definisce l'assegnazione dei valori nelle tra categorie
  - Identifier uniqueness
  - Identity proofing and credential issuance, renewal and replacement
  - Attribute quality and freshness

RAF: Identifier uniqueness

Value	Description
$PREFIX$/ID/unique	The identifier MUST have the following four properties: (Unique-1) The user identifier represents a single natural person (Unique-2) The CSP can contact the person to whom the identifier is issued (Unique-3) The user identifier is never re-assigned (Unique-4) The user identifier is eduPersonUniqueId [eduPerson], SAML 2.0 persistent name identifier [OASIS SAML], subject-id or pairwise-id [OASIS SIA] or OpenID Connect sub (type: public or pairwise)

Value	Description
$PREFIX$/ID/eppn-unique-no-reassign	eduPersonPrincipalName value has the Unique-1, Unique-2 and Unique-3 properties.
$PREFIX$/ID/eppn-unique-reassign-1y	eduPersonPrincipalName value has the Unique-1 and Unique-2 property but may be re-assigned after a hiatus period of 1 year or longer.

RAF: Identity proofing

Value	Description
$PREFIX$/IAP/low	Example: self-asserted identity together with verified e-mail address, following sections sections 5.1.2-5.1.2.9 and section 5.1.3 of [Kantara SAC].
$PREFIX$/IAP/medium	Example: the person has sent a copy of their government issued photo-ID to the CSP and the CSP has had a remote live video conversation with them, as defined by [IGTF].
$PREFIX$/IAP/high	Example: the person has presented an identity document that is checked to be genuine and represent the claimed identity and steps have been taken to minimise the risk of a lost, stolen, suspended, revoked or expired document, following sections 2.1.2, 2.2.2 and 2.2.4 of eIDAS assurance level substantial [eIDAS LoA].

RAF: Attribute quality and freshness

Value	Description
$PREFIX$/ATP/ePA-1m	eduPersonAffiliation, eduPersonScopedAffiliation and eduPersonPrimaryAffiliation attributes (if populated and released to the RP) reflect user's departure within 31 days time
$PREFIX$/ATP/ePA-1d	eduPersonAffiliation, and eduPersonScopedAffiliation and eduPersonPrimaryAffiliation attributes (if populated and released to the RP) reflect user's departure within one days time

Cappuccino ed Espresso

- Le varie componenti sono state raccolte in due “collezioni” (con questi nomi esotici) per rendere più agevole il lavoro di IdP e SP
- Cappuccino è un profilo ragionevole per casi d’uso a basso livello di rischio
- Espresso è il profilo da usare nei casi che richiedono una vera verifica dell’identità digitale

Value	Cappuccino	Espresso
$PREFIX$	X	X
$PREFIX$/ID/unique	X	X
$PREFIX$/ID/eppn-unique-no-reassign		
$PREFIX$/ID/eppn-unique-reassign-1y		
$PREFIX$/IAP/low	X	X
$PREFIX$/IAP/medium	X	X
$PREFIX$/IAP/high		X
$PREFIX$/IAP/local-enterprise		
$PREFIX$/ATP/ePA-1m	X (*)	X (*)
$PREFIX$/ATP/ePA-1d		

Da IDEM-P0 ad IDEM-P3 (1)

- IDEM-P0 (corrisponde al LoA1 INFN o RAF IAP/low)
  - Auto-asserzione dell'identità con verifica del contatto
- IDEM-P1 (corrispondente al LoA2 INFN o RAF IAP/medium)
  - Verifica DE VISU dell'identità via confronto con documento di identità riconosciuto dallo Stato italiano e **apparentemente valido**

Da IDEM-P0 ad IDEM-P3 (2)

- IDEM-P2 (corrispondente a identità SPiD o RAF IAP/high o livello eIDAS Significativo)
  - Verifica DE VISU via confronto con documento di identità riconosciuto dallo Stato italiano e **che sia stato verificato per stabilirne l'autenticità oppure, secondo una fonte autorevole, esiste ed è collegato ad una persona reale.**
- IDEM-P3 (corrispondente ad identità CIE o livello eIDAS Elevato)
  - La verifica dell'identità digitale deve avvenire attraverso il riconoscimento effettuato da un pubblico ufficiale appositamente addestrato che verifica le corrispondenze biometriche della persona.

Profili IDEM: casi d'uso

- Un account autoregistrato con conferma via mail e autenticazione ad un fattore.
  - **eduPersonAssurance: https://idem.garr.it/af/IDEM-P0**
- Un account verificato tramite documento d'identità apparentemente autentico e autenticazione ad un fattore.
  - **eduPersonAssurance: https://idem.garr.it/af/IDEM-P0**
  - **eduPersonAssurance: https://idem.garr.it/af/IDEM-P1**
- Un account verificato tramite documento d'identità confermato e autenticazione a più fattori.
  - **eduPersonAssurance: https://idem.garr.it/af/IDEM-P0**
  - **eduPersonAssurance: https://idem.garr.it/af/IDEM-P1**
  - **eduPersonAssurance: https://idem.garr.it/af/IDEM-P2**

Le richieste dei SP

- Per essere conforme ai profili IDEM e REFEDS, un SP deve richiedere l'attributo eduPersonAssurance attraverso i medadati con la direttiva

  <RequestedAttribute FriendlyName="eduPersonAssurance"
  Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.11"
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
  isRequired="true"/>

- E nella richesta di autenticazione deve definite il tipo di autenticazione atttraverso la direttiva AuthnContextClassRef ed in particolare, se richiesto il singolo fattore

  AuthnContextClassRef: https://refeds.org/profile/sfa

- Mentre se è richiesto il doppio fattore

  AuthnContextClassRef: https://refeds.org/profile/mfa

The End

Grazie

Domande?