

# Relazione del CTS

Andrea Ranaldi - ISPRA

Assemblea IDEM

08/03/2024



# Cosa abbiamo fatto

- *Profili di Garanzia*
- *Nuovo Regolamento*
- *Formazione*
- *Sviluppo*



# Senza profili

- Un'unica qualità di identità
- Un'unica qualità di autenticazione
- Un profilo di adesione generico



# Profili di garanzia

- *Separate identità e autenticazione*
- *Compatibilità con REFEDS Assurance Framework (RAF) v2.0*
- *Basato su NIST 800-63B*
- *Compatibilità con i profili SPID / eIDAS*
- *Pensati per il futuro*



# Con i profili

## Identità

- Deve essere definito un processo di identificazione
- La qualità dell'identità varia in base alle verifiche eseguite
- È necessario dichiarare il tempo di aggiornamento dei dati



# Con i profili

## Autenticazione

- Deve essere definito il processo di consegna e rinnovo dei fattori di autenticazione
- Vengono definiti i requisiti minimi di ogni fattore di autenticazione
- Può essere richiesto un secondo fattore



# Con i profili

## Autorizzazione

- I livelli di qualità di identificazione ed autenticazione definiscono il profilo rilasciato
- Il profilo viene rilasciato per singolo utente
- Il Service Provider può richiedere un profilo minimo per autorizzare l'accesso



# Nuovo regolamento

- Nessuna attività obbligatoria
- Definiti i controlli necessari
- Definiti i processi che gli aderenti devono aver definito
- Definita la procedura di adesione
- Definito la procedura di rinnovo



∞ La sicurezza diventa un processo continuo ∞

# Formazione

Seminario	Iscritti
<i>OIDC federation analisi protocollo</i>	239
<i>OIDC federation procedura di Onboarding</i>	193
<i>Identity Assurance</i>	189
<i>OIDC federation Prova su strada</i>	136
MFA	302
<i>Configurazione avanzata Identity Provider</i>	205
<i>IDP resiliente</i>	205
<i>Laboratorio MFA con Privacy Idea</i>	
<i>Laboratorio Proxy OIDC - SAML2</i>	

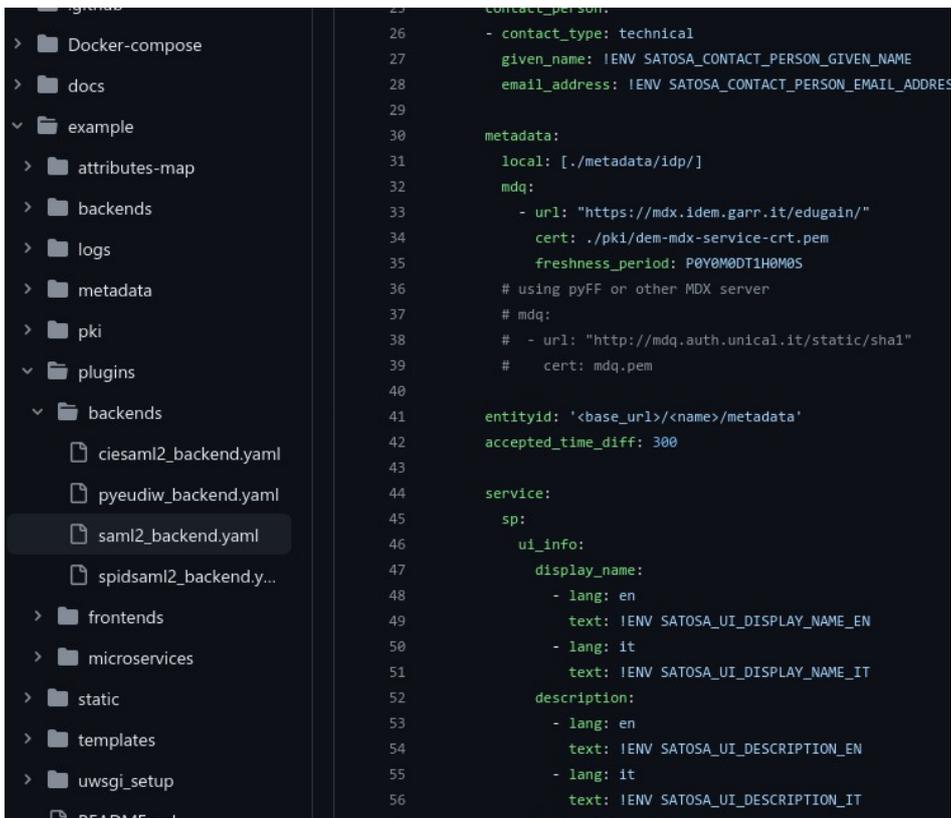
# Sviluppo

## Shibboleth:

- Membri dell Shibboleth Consortium grazie a GARR

## Satosa-Saml2Spid:

- Sviluppato attivamente dal CTS e da vari enti membri



The image shows a file explorer on the left and a code editor on the right. The file explorer displays a directory structure with folders like 'Docker-compose', 'docs', 'example', 'attributes-map', 'backends', 'logs', 'metadata', 'pki', 'plugins', 'backends', 'frontends', 'microservices', 'static', 'templates', and 'uwsgi\_setup'. The code editor shows a configuration file with the following content:

```
25 contact_person:
26   - contact_type: technical
27     given_name: IENV_SATOSA_CONTACT_PERSON_GIVEN_NAME
28     email_address: IENV_SATOSA_CONTACT_PERSON_EMAIL_ADDRESS
29
30 metadata:
31   local: [./metadata/idp/]
32   mdq:
33     - url: "https://mdx.idem.garr.it/edugain/"
34       cert: ./pki/dem-mdx-service-crt.pem
35       freshness_period: P0Y0M0DT1H0M0S
36     # using pyFF or other MDX server
37     # mdq:
38     #   - url: "http://mdq.auth.unical.it/static/sha1"
39     #     cert: mdq.pem
40
41   entityid: '<base_url>/<name>/metadata'
42   accepted_time_diff: 300
43
44 service:
45   sp:
46     ui_info:
47       display_name:
48         - lang: en
49           text: IENV_SATOSA_UI_DISPLAY_NAME_EN
50         - lang: it
51           text: IENV_SATOSA_UI_DISPLAY_NAME_IT
52       description:
53         - lang: en
54           text: IENV_SATOSA_UI_DESCRIPTION_EN
55         - lang: it
56           text: IENV_SATOSA_UI_DESCRIPTION_IT
```

# Ed ora? Proposte per il nuovo CTS!



- **Formazione**
- **Nuovi gruppi**
- **Comunità!**

# Formazione

- Aggiornamento Shibboleth (verso la versione 5)
- Profili di garanzia
  - Livelli di garanzia
  - SFA
  - MFA
  - Configurazione dei profili con Shibboleth
  - Configurazione dei profili con SimpleSAMLPHP
- Approfondimenti verso le nuove tecnologie
  - OIDC Federation
  - Digital Wallet



Trasformare i corsi in guide

# Gruppi di lavoro

- Gruppi di lavoro misti RTD, DPO e tecnici per la creazione di procedure esempio per l'adesione ai profili di garanzia
  - Processi di identificazione
  - Processi di consegna e rinnovo fattori
  - Analisi dei rischi e conservazione di log e credenziali
- Analisi dei possibili sviluppi futuri della federazione
  - Integrazione con i nuovi protocolli
    - OpenID Connect
    - OIDC Federation
    - Digital wallet
  - Identità digitale unica

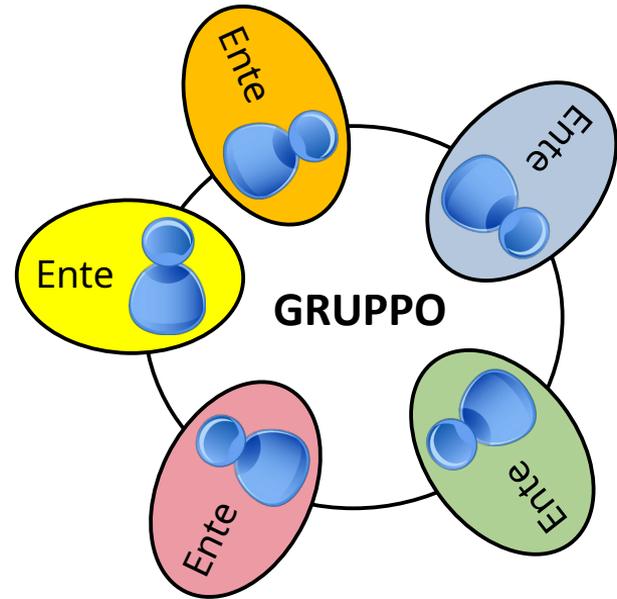
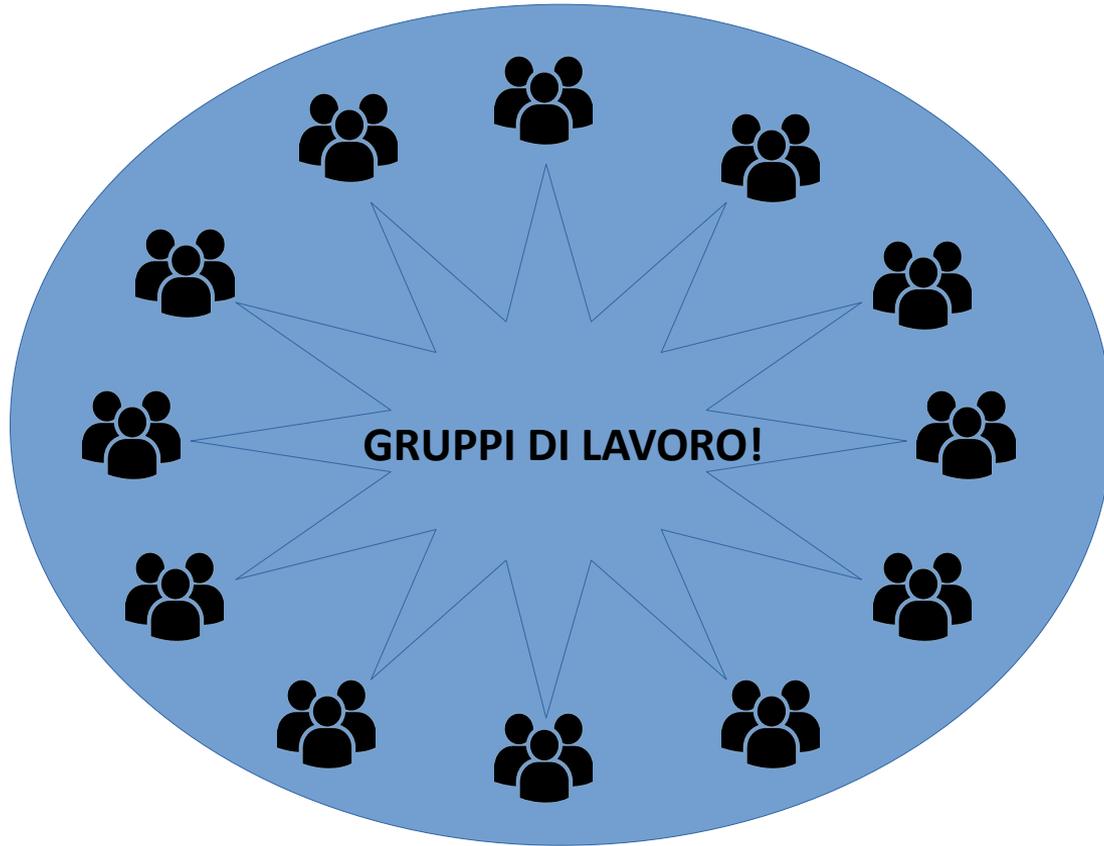


# Ripartire dalla Comunità!

- Coinvolgere RTD (responsabili della transizione digitale) e RDP/DPO (responsabili della protezione dei dati personali) nelle problematiche di identità digitale, autenticazione ed autorizzazione
- Definire un sistema per far certificare da IDEM la partecipazione ai gruppi di lavoro
- IDEM Day in presenza
- Eventi IDEM per il pubblico



# Ricordate come lavoriamo?



# Ora tocca a voi



- Domande
- Commenti
- Idee