Nunzio Napolitano – CTS Marco Malavolti - GARR

Metadati

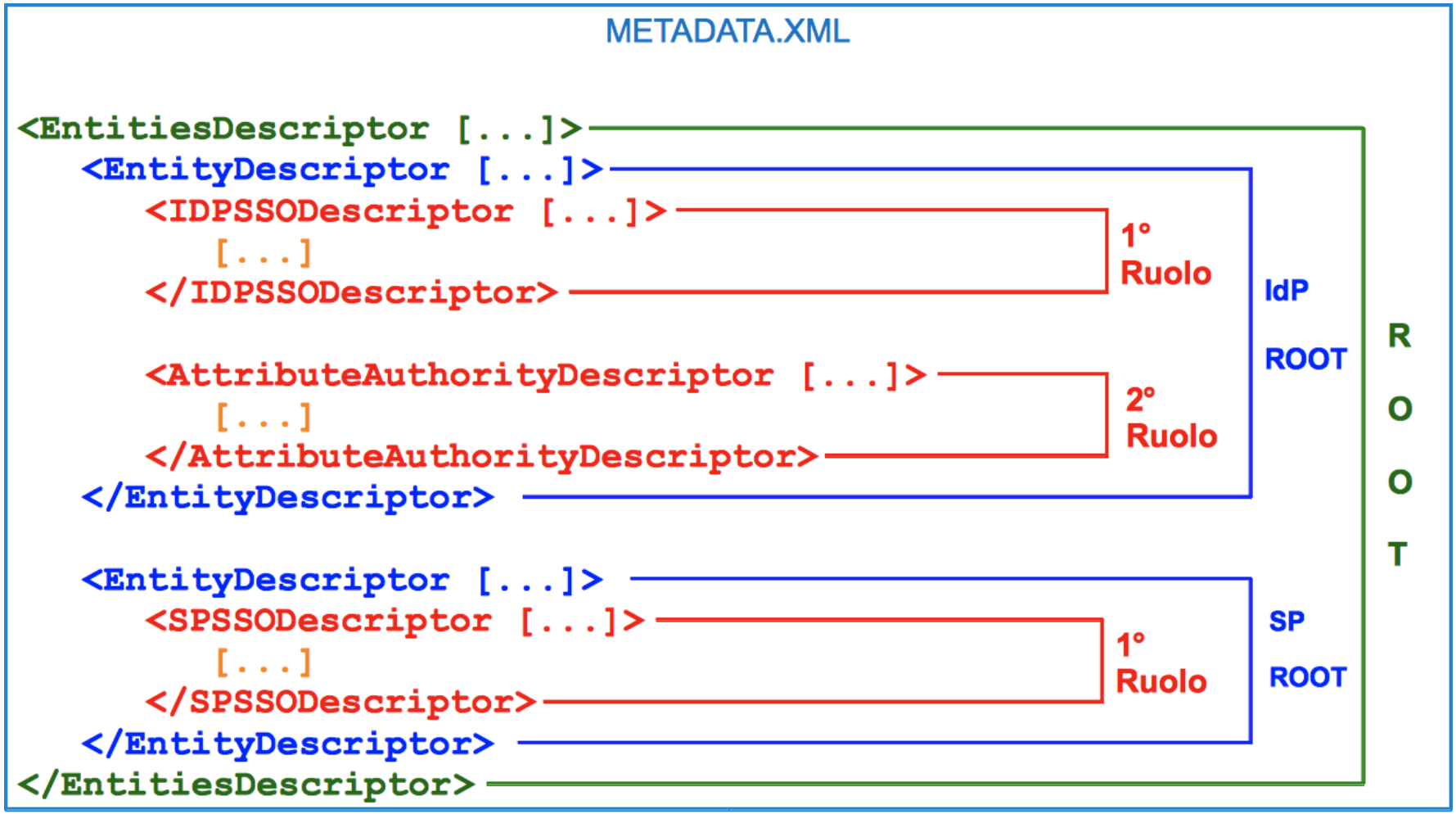
- Cosa sono
  - I Metadati sono particolari file XML che rappresentano le entità, descrivendone le caratteristiche essenziali:
    - Certificato usato per firmare e cifrare
    - Protocolli e profili supportati
    - Descrizione degli intenti
    - Informazioni aggiuntive es. riferimenti del supporto , nome organizzazione etc..
- Cosa Servono

  - Identificano e Rappresentano un entita' SAML: Risorsa (SP) o Servizio di Autenticazione (IdP)
  - Permettono di stabilire una comunicazione sicura con le altre entità

Metadati - estensioni

- I metadati, nella loro forma predefinita, descrivono esaustivamente le entità, permettendo loro di comunicare. Estendendoli è possibile agevolare l'interazione con l'utente sfruttando nuove e più dettagliate informazione proprie delle entità.
- Estensioni
  - Extensions for Login and Discovery User Interface
  - Extensions for Registration and Publication Information
  - Extension for Entity Attributes
- Profili
  - Metadata Interoperability Profile
  - Data Protection Code of Conduct
  - Edugain Metadata Profile
  - IDEM Metadada Profile

Metadati - esempio



Metadati – oneri ed onori

- I metadati di una federazione descrivono la federazione stessa.
  - Le singole EntityID identificano UNIVOCAMENTE un'entità (IdP o SP)
  - Elemento fondamentale per la fiducia reciproca
  - Rispecchiano la dimensione della federazione
- La gestione dei metadati comporta i seguenti «oneri»:
  - Editing di un file XML (*servizio- utenti*)
  - Carico di lavoro da parte del servizio
  - Interfederazioni: collezione e gestione di diversi set di metadati da parte della federazione
  - Trigger manuale delle modifiche
  - Gestire una grossa quantità di dati
    - IDEM – 9923 linee , Descriptor : 130 entities, 47 IdP, 83 SP
    - Edugain – 2984 linee , Descriptor : 90 entities, 48 IdP, 42 SP

I software – sono veramente utili?

- Collezione automatica dei metadati da parte della Federazione
  - Errore umano nello scambio informazioni
  - Aggiornamento automatico dei dati
  - Verifiche di consistenza (https://aai.pionier.net.pl/Metadata/)
- Gestione e visualizzazione delle informazioni mantenute nei metadati in una modalità user-friendly
  - Interfacce grafiche
  - Funzionalità Import/export
- Distribuzione dei dati della Federazione
  - Pubblicazione dei metadati
  - Pubblicazione dei metadati aggregati (interfederazione)
  - Elenco delle risorse disponibili (http://beta.terena-met.yaco.es/met/federation/idem/)

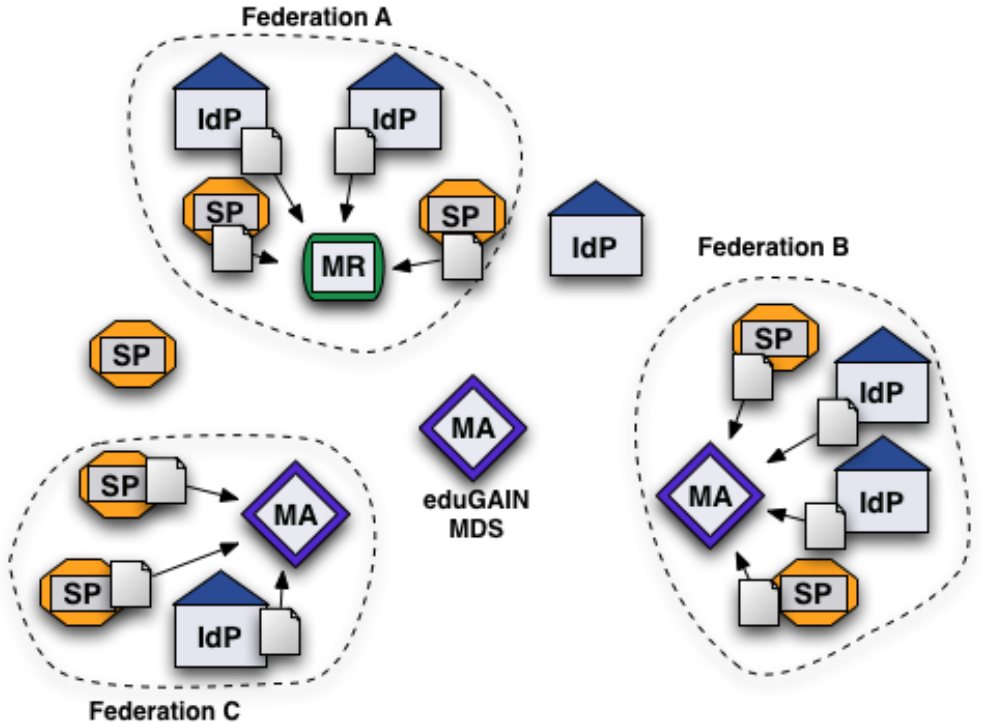
I software – Principali funzionalità

- Workflow management
- Funzioni di controllo sui dati
- Import/export dei metadati
- Aderenza agli standard SAML + estensioni
- Attribute Release Policy (ARP)
- Firma dei metadati
- Pubblicazione delle risorse
- Supporto multilingue
- User-Friendly

Metadata software - definizioni

- Ruoli:
  - *Metadata Publishers* (MP)
  - *Metadata Consumer* (MC)

- Componenti:
  - *Identity Provider* (IdP)
  - *Service Provider* (SP)
  - *Metadata Aggregator* (MA)
  - *Metadata Registrar* (MR)



https://rnd.feide.no/2010/01/05/metadata_aggregation_requirements_specification

Metadata software - elenco

- Registries:
  - Switch AAI Resource Registry
  - Australian Access Federation Resource Registry
  - Peer
  - Edugate Resource Registry
  - Janus
- Aggregators:
  - Shibboleth Metadata Aggregator
  - phyton Federation Feeder
  - eduGAIN MDS
  - simpleSAMLphp Aggregator

https://www.terena.org/mail-archives/tf-emc2/msg02263.html

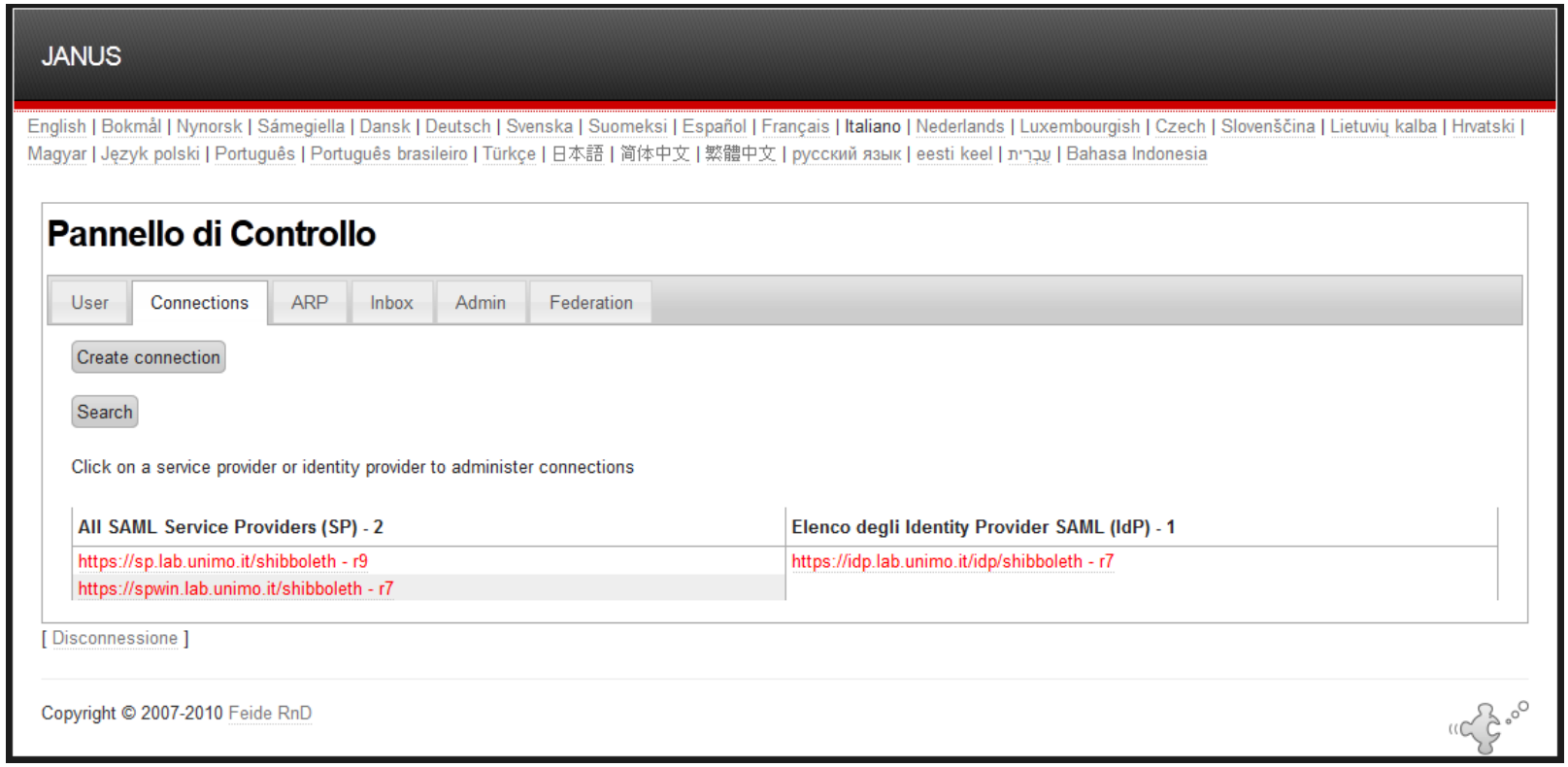
Nel pratico …… Federare una risorsa

- Passi per federare una risorsa – situazione attuale
  1. Installo il mio Idp/SP
  2. Edito il file di metadati ottenuto dal software e vi aggiungo i tag necessari (contacts, etc..)
  3. invio il file ad idem-help@garr.it per ottenere l'inserimento nella federazione di test
  4. eventuale scambio di mail per correggere problemi nel file
  5. inserimento nella federazione di test
  6. invio moduli di adesione cartacei
  7. verifica moduli di adesione/ confronto con i metadati
  8. approvazione
  9. inserimento frammento metadati nella federazione di produzione (copia ed incolla)
  10. Aggiunta risorsa al WAYF (se IdP) (copia ed incolla)

Verifiche: *verifica vs. XSD usando le funzioni di libxml2*

Nel pratico ..... Federare una risorsa

JANUS

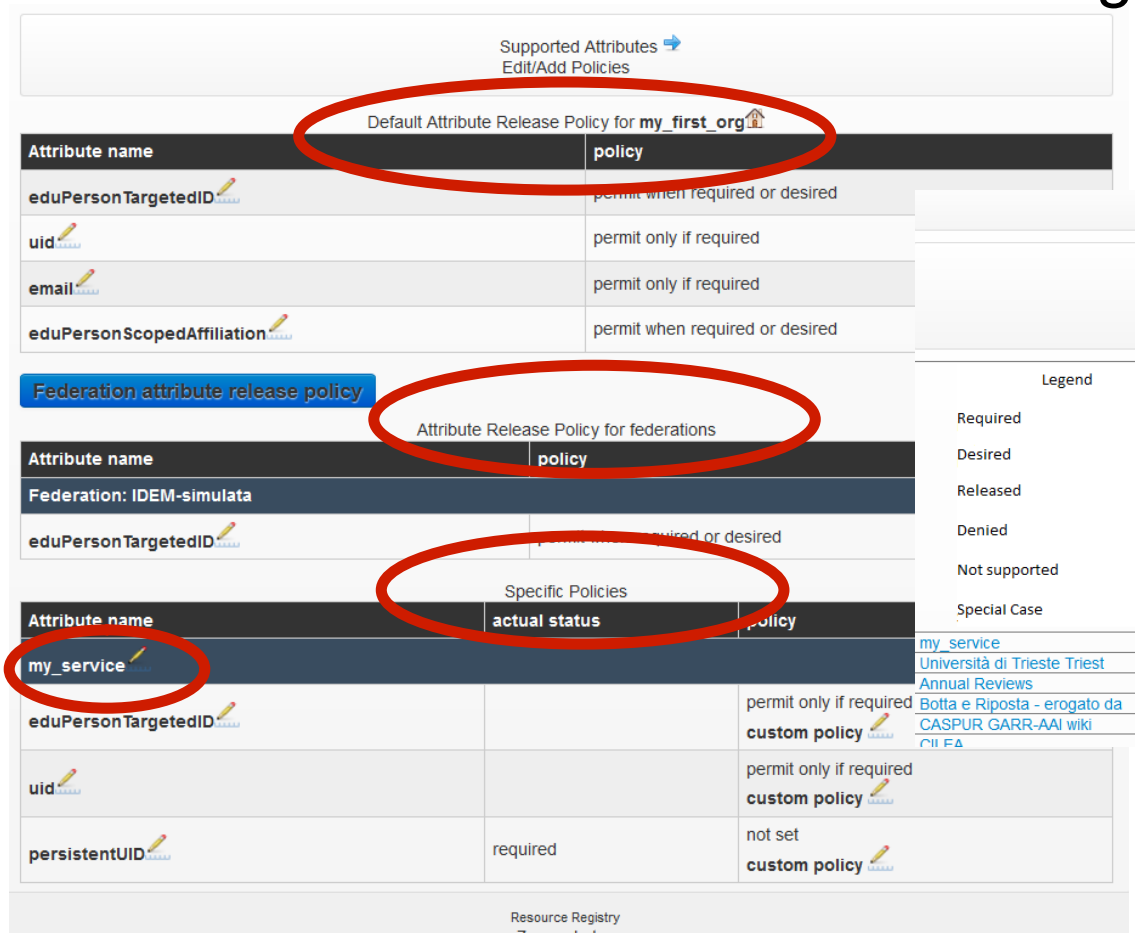


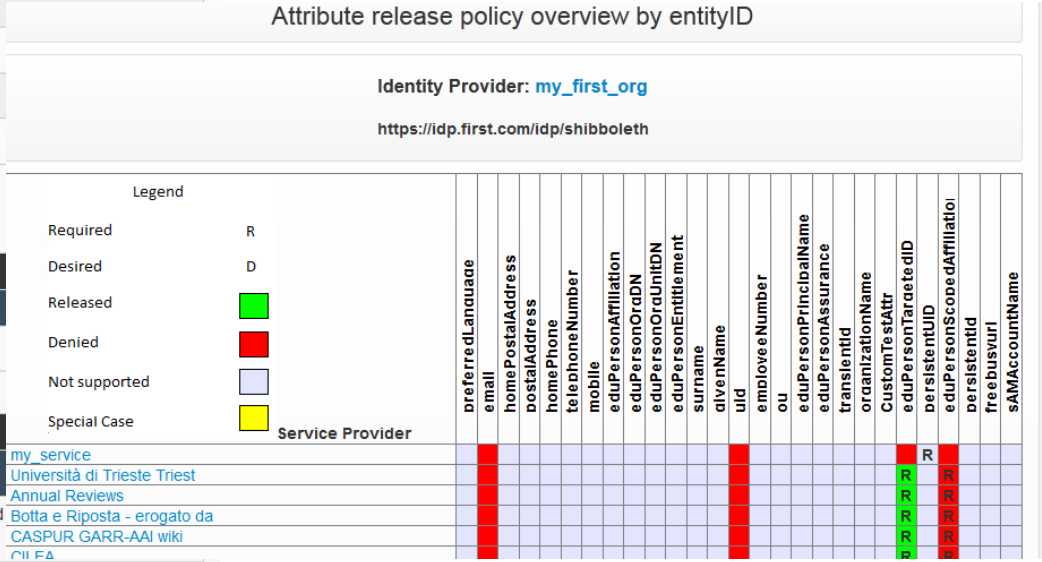
[Download Demo JANUS]

Nel pratico ..... Esempio di ARP

- https://metadata.uniparthenope.it/rr3/my_arp.xml

Edugate Resource Registry





Conclusioni

- L'autenticazione federata è costantemente in crescita, amplificata anche dai progetti di interfederazioni.
- I metadati stanno assumendo in questo scenario un ruolo sempre più importante.
- Vista la mole di informazioni e le operazioni richieste, la gestione dei metadati richiede un grosso carico di lavoro che può essere enormemente abbassato con l'utilizzo di software specifici.
- I software attualmente disponibili hanno raggiunto un sufficiente grado di maturazione.

Conclusioni

- L'autenticazione federata è costantemente in crescita, amplificata anche dai progetti di interfederazioni.
- I metadati stanno assumendo in questo scenario un ruolo sempre più importante.
- Vista la mole di informazioni e le operazioni necessarie, la gestione dei metadati richiede un grosso carico di lavoro che può essere enormemente abbassato con l'utilizzo di software specifici.
- I software attualmente disponibili hanno raggiunto un sufficiente grado di maturazione.

Conclusioni

Domande?

Grazie per la vostra attenzione

Riferimenti

- Malavolti M.
  Studio comparativo dei sistemi di gestione dei metadati per le federazioni di identità. Alma Mater Studiorum Università di Bologna, 2012
- Software
  - Switch AAI Resource Registry
  - Australian Access Federation Resource Registry
  - Peer
  - Edugate Resource Registry
  - Janus
  - Shibboleth Metadata Aggregator
  - phyton Federation Feeder
  - eduGAIN MDS
  - simpleSAMLphp Aggregator
  - Edugain metadata validator https://aai.pionier.net.pl/Metadata/
  - Edugain metadata processing http://www.edugain.org/technical/metadata_processing.php
  - Terena metadata explorer tool http://beta.terena-met.yaco.es/met/federation/idem

Approfondimenti – Tabella comparativa delle funzionalità fra i software (I)

- Valutazioni di massima sui Metadata Registries:
  - Switch AAI Resource Registry
    - E' molto completo ma estremamente customizzato per gli usi della federazione Switch (supporto per shibboleth e procedure di switch).
  - Australian Access Federation Resource Registry
    - derivato da AAI di switch e quindi ha più o meno gli stessi pregi e difetti.
  - Peer
    - Fortemente ispirato alla INTERfederazione, poco flessibile per usi INTRAfederazione, ancora in release BETA.
  - Janus
    - Molto flessibile, buon gruppo di sviluppo, scarso sulla gestione delle ARP.
  - Edugate Resource Registry
    - Tutte le funzionalità degli altri tool, flessibile, previste nuove funzionalità

Approfondimenti – Tabella comparativa delle funzionalità fra i software (II)

Feature/Software	RR (switch)	Janus	PEER	RR (edugate)
E' possibile aggiungere elementi ai metadati dell'entità?	si	si	si, ma solo quelli da lui definiti	si
Viene controllata l'unicità del nome delle entità?	si	si	si	si
E' possibile aggiungere una descrizione dell'entità?	si	si	si	si
E' possibile aggiungere l'organizzazione che ospita l'entità?	si	si	si	si
Quali estensioni dei metadati sono supportate?	MDUI	MDUI , Attribute	MDUI	MDUI
E' possibile riconoscere eventuali mancanze/errori presenti nei metadati?	si	si	si	si
E' possibile visualizzare quali attributi un IdP può rilasciare?	si	no	no	si
E' possibile visualizzare quali attributi un SP richiede?	si	no	no	si
E' possibile esportare i metadati di una sola entità?	no	si	si	si
E' possibile esportare metadati che non rispettano i requisiti della Federazione?	no	no	si	si
E' possibile definire le Attribute Release Policy per i propri IdP?	si	no	no	si
E' possibile aggiungere entità SAML 1.0?	si	si	si	si
E' possibile aggiungere entità SAML 2.0?	si	si	si	si
Quali tipologie di entità gestisce?	IdP e SP	IdP e SP	IdP e SP	IdP e SP
Espone un Catalogo degli SP e degli IdP disponibili nella Federazione?	si	si	si	si
Linguaggi utilizzati per lo sviluppo dell'applicazione	PHP, javascript	PHP, JSON	Python, javascript	PHP
E' di facile installazione?	no	si	si	si
Possiede il supporto multi-lingue?	no	si	no	si
Gestisce correttamente i certificati delle entità?	si	non in modo predefinito	si	si
Riesce a gestire anche le entità interfederate?	si	si	si	si
E' possibile gestire le ARP?	si	si	no	si
E' concepita per evolversi?	no	si	si	si
Riesce a verificare i "validUntil" dei metadai inseriti?				??
Permette il ripristino a versioni precedenti dei metadati?	no	si	si	??
Riesce a firmare digitalmente i metadati della Federazione?	no	si	no	si
E' in grado di pubblicare i metadati delle Federazione?	si	si	si, ma solo singolarmente	si