Consortium GARR
THE ITALIAN EDUCATION & RESEARCH NETWORK

Autenticazione federata

Davide Vaghetti <davide.vaghetti@garr.it>

Università degli Studi Roma Tre, 07-10-2019

Workshop GARR 2019 "Net Makers"

Agenda

- Cosa è e a cosa serve l'autenticazione federata?
- SAML
- Identificatori e attributi
- Federazioni di Identità e eduGAIN
- Entity Category

Autenticazione e autorizzazione

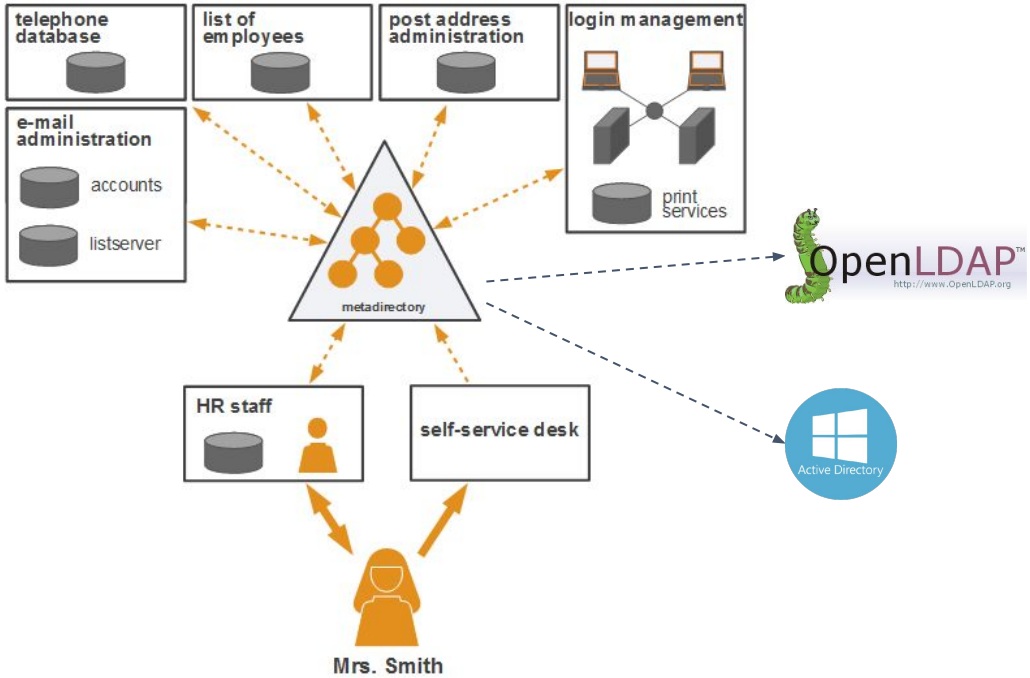
Autenticazione

L'atto di conferma della veridicità di un attributo relativo ad un dato o ad una informazione. Ad esempio, l'atto di convalida di un certificato X.509 relativo ad una persona è ciò che ci permette di autenticarla.

Autorizzazione

L'atto di assegnare diritti su una risorsa. L'autorizzazione è spesso basata sul ruolo --- RBAC Role Based Access Control --- o su di una serie di attributi che si mappano sui diritti delle risorse interessate --- ABAC Attribute Based Access Control.

Directory e IDMS



Imoge courtesy of DAASI International - https://daasi.de

I sistemi di gestione delle identità sono i sistemi che permettono di amministrare --- memorizzare, cambiare, versionare, ecc. --- le informazioni relative alle identità degli appartenenti alla propria organizzazione.

Gli IDMS in ambiente enterprise sono quasi sempre basati su servizi di Directory, come OpenLDAP e Active Directory, che comprendono la gestione di credenziali basate su password.

SAML

OASIS
Advancing open standards for the information society

- Security Assertion Markup Language
- Standard OASIS
- Regole per lo scambio di dati di autenticazione e autorizzazione
- Basato su XML
- Web browser SSO (Single Sign On)

Autenticazione locale, centralizzata e SSO

	Locale	Centralizzata	Single Sign On
Utenti	Ogni applicazione ha il proprio database utenti.	Un unico database/directory per tutta l'organizzazione.	Utenti e autenticazione sono disaccoppiati: il SSO può usare un solo Database utenti o più di uno.
Gestione Credenziali	Ogni applicazione memorizza e gestisce le credenziali dei propri utenti.	Le applicazioni raccolgono le credenziali e le trasmettono al sistema centralizzato per l'autenticazione.	Accesso alle applicazioni e autenticazione sono disaccoppiati: solo il sistema di SSO gestisce le credenziali di autenticazione.

SAML, gli attori

Principal

- l'utente

User Agent

- Il browser dell'utente.

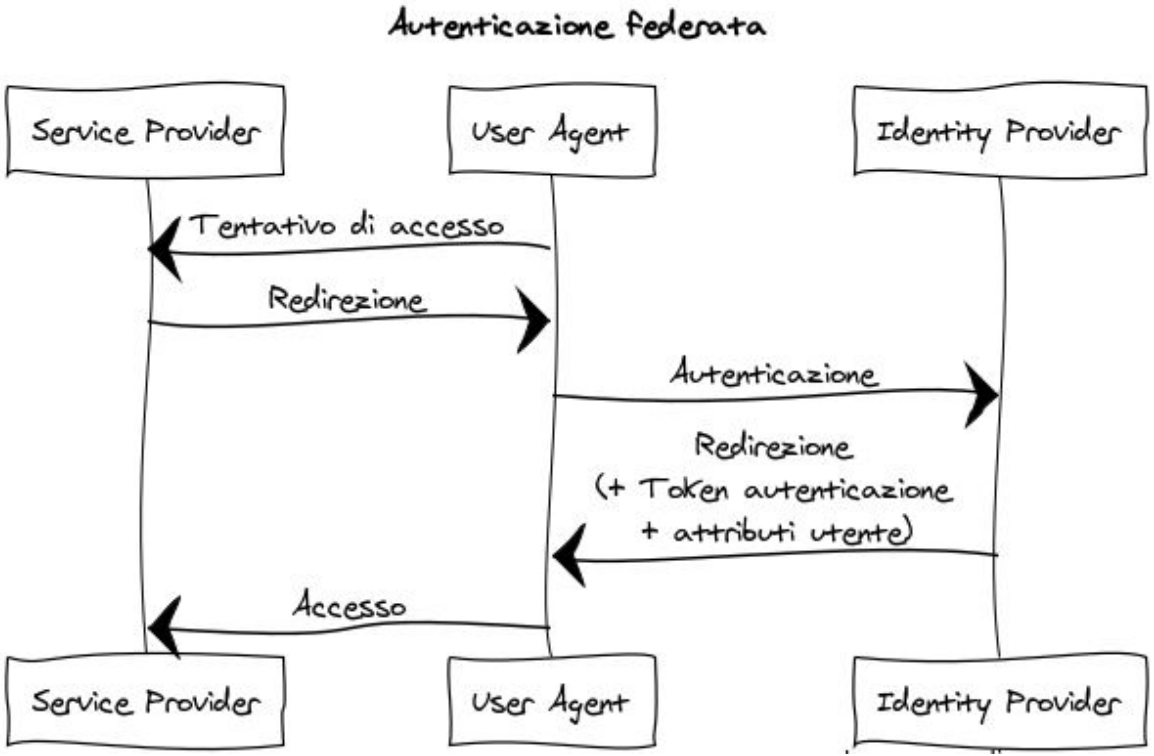
Identity Provider

- Collegato a DB utenti (tipicamente una directory)
- Implementa l'autenticazione
- Rilascia gli attributi

Service Provider

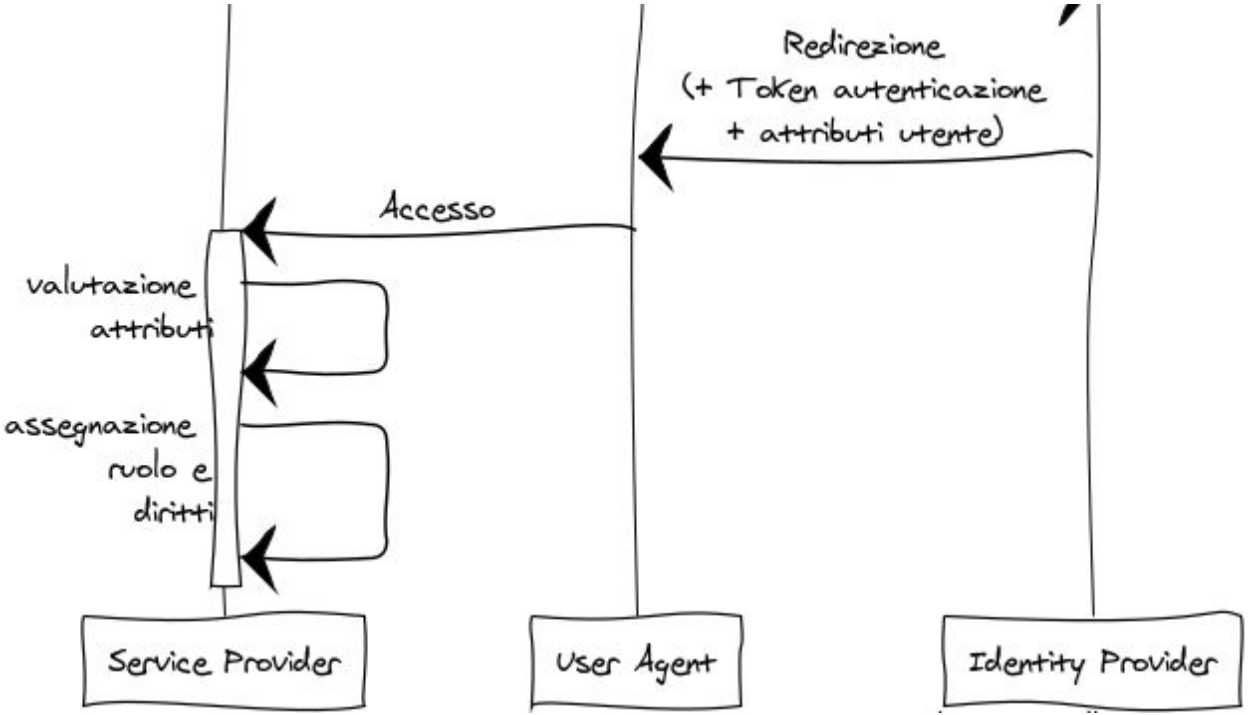
- Protegge l'accesso ad un servizio
- Implementa l'autorizzazione
- Consuma gli attributi

Autenticazione federata



1. L'utente tenta di accedere ad una applicazione protetta da un Service Provider.
2. Il Service Provider richiede l'autenticazione federata.
3. L'utente sceglie la propria organizzazione e viene rediretto al Identity Provider.
4. L'utente si autentica.
5. Il Identity Provider redirige l'utente al servizio con un token di autenticazione ed una serie di attributi.
6. L'utente accede al servizio.

Autorizzazione federata



1. L'utente si ripresenta al servizio con token di autenticazione (asserzione SAML) e un insieme di attributi.
2. L'utente accede al servizio:
   a. Il servizio valuta gli attributi.
   b. Il servizio assegna un ruolo locale e un insieme di diritti all'utente.

SAML: identificatori

Identifier / Attribute	Persistent	Revocable	Reassignable	Opaque	Targeted	Portable	Global	Qualifier
SAML2 Transient NameID	No	N/A	N/A	Yes	N/A	N/A	Yes	N/A
SAML2 Persistent NameID	Yes	Yes	No	Yes	Yes	Yes	No	Issuer ID
eduPersonTargetedID	Yes	Yes	No	Yes	Yes	Yes	No	Issuer ID
eduPersonPrincipalName	Yes	Yes	Yes	No	No	No	Yes	Scoped
eduPersonUniqueId	Yes	Yes	No	Yes	No	No	Yes	Scoped
Social Security Number	Yes	No	N/A	No	No	Yes	No	US Citizens
Phone Number	Yes	Yes	Yes	No	No	No	Yes	N/A
OIDC public sub claim	Yes	Yes	No	N/A	No	No	No	Issuer ID
OIDC pairwise sub claim	Yes	Yes	No	N/A	Yes	No	No	Issuer ID
ORCID	Yes	Yes	No	Yes	No	Yes	Yes	N/A

Fonte https://wiki.shibboleth.net/confluence/display/CONCEPT/NameIdentifiers

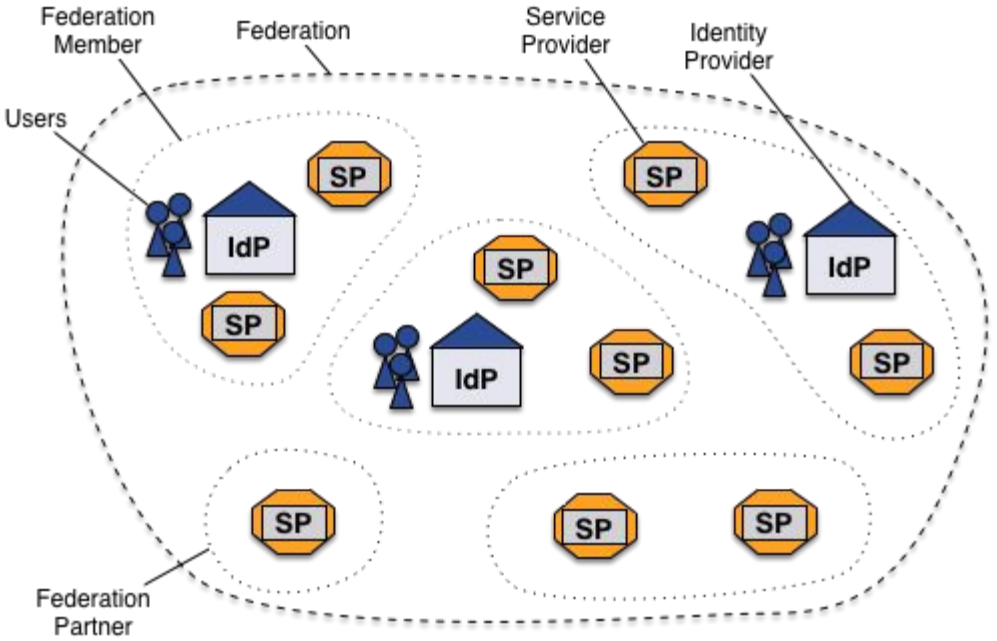
SAML: attributi

Attributo	Semantica	Sintassi	Fonte
givenName	nome o parti del nome di una persona.	stringa, multiplo	RFC4519 (inetOrgPerson)
sn	cognome o parti del cognome.	stringa, multiplo	RFC4519 (person)
mail	indirizzo di posta elettronica	stringa, multiplo	RFC4524 (inetOrgPerson)
eduPersonAffiliation	tipo di affiliazione con l'organizzazione	stringa, multiplo	eduPerson
eduPersonScopedAffiliation	tipo di affiliazione con l'organizzazione	stringa+dominio, multiplo	eduPerson
eduPersonEntitlement	indica un insieme di diritti su una risorsa	URI, multiplo	eduPerson

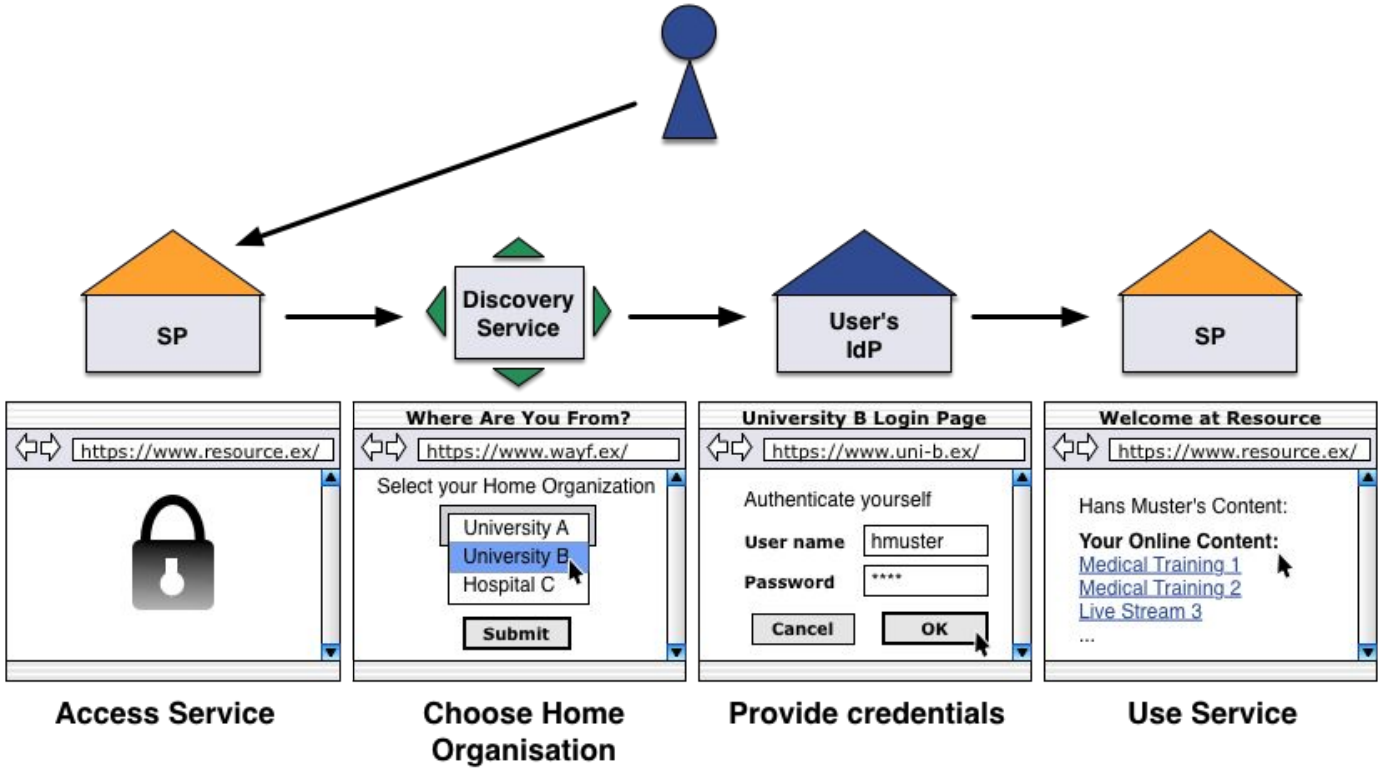
Federazioni di identità

Le federazioni di identità sono gruppi di organizzazioni che concordano di inter-operare secondo regole condivise, in particolare condividono uno specifico **quadro legale, dei regolamenti e delle specifiche tecniche**.

Le federazioni agiscono come **terza parte fidata** nello scambio di **informazioni di identità** tra le organizzazioni degli utenti e i fornitori di servizi che offrono **l'accesso alle risorse**.



Accesso alle risorse con più organizzazioni: Discovery Service



Entità e metadata

Ogni entità partecipante, principalmente IdP e SP, registra i propri metadata nella federazione.

La federazione valida e aggrega i metadata creano uno o più feed di federazione.

La federazione firma il/i feed con la chiave di federazione e li distribuisce tramite un Metadata Distribution System (MDS)

eduGAIN

Federations' upstream feed

Participating Federations provide a metadata aggregate of entities to be exported to eduGAIN

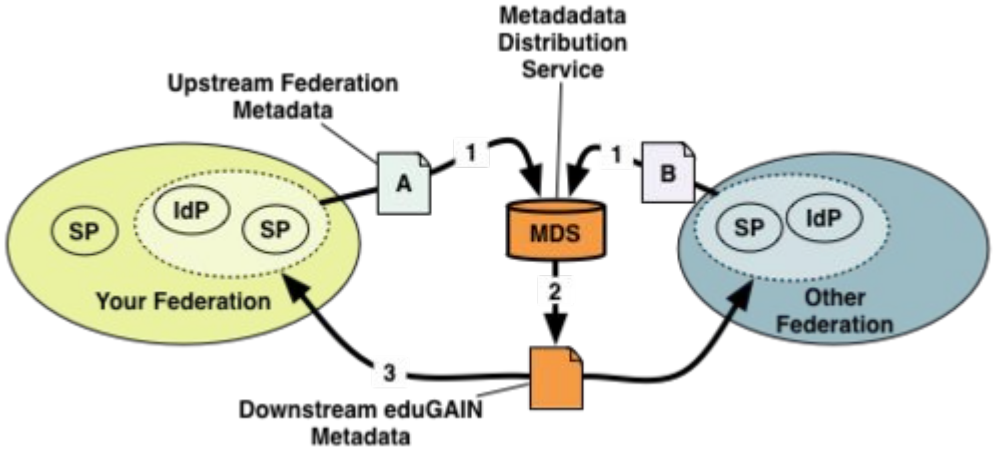
The eduGAIN feed

Federations' metadata aggregates are picked up, validated and aggregated in the so called eduGAIN feed

Signing & Distribution

The eduGAIN feed is signed with the eduGAIN key and distributed through the eduGAIN MDS:

.



Entity Category

- Le Entity Category raggruppano entità con caratteristiche comuni
- Sono estensioni dei metadata delle entità
- Valide sia per Service Provider, sia per Identity Provider
- Diversi casi d'uso:
  - Facilitare e semplificare il rilascio degli attributi ai Service Provider.
  - Verificare l'aderenza a requisiti di privacy e trattamento dati per poter rilasciare attributi ai Service Provider.
- Due tipi di attributi:
  - **Name="http://macedir.org/entity-category"** per asserire l'appartenenza alla categoria indicata
  - **Name="http://macedir.org/entity-category-support"** per asserire interoperabilita' con, o supporto per, le entita' della categoria indicata

Entity Category Attribute

```
<EntityDescriptor entityID=$$ENTITY_ID$$>
  <Extensions>
    <mdattr:EntityAttributes>
      <saml:Attribute  Name="http://macedir.org/entity-category"
                       NameFormat=”urn:oasis:names:tc:SAML:2.0:attrname-format:uri”>
        <saml:AttributeValue>
          $$ENTITY-CATEGORY-URI$$
        </saml:AttributeValue>
      </saml:Attribute>
    </mdattr:EntityAttributes>
</Extensions>
[..]
</EntityDescriptor>
```

Entity Categories

REFEDS Research and Scholarship *(R&S)

https://refeds.org/category/research-and-scholarship

REFEDS Hide from discovery

https://refeds.org/category/hide-from-discovery

GÉANT Data Protection Code of Conduct (CoCo)

https://wiki.refeds.org/display/CODE/Data+Protection+Code+of+Conduct+Home

(proposed) REFEDS Academia

https://github.com/leifj/academia-category

REFEDS Research and Scholarship Entity Category

Entity Category disegnata per:

- **Rilasciare attributi**: un set di attributi limitato e ben definito per i Service Provider *supporting research and scholarship interaction, collaboration or management, at least in part*.
  - **SI**: wiki, sistemi di vconf delle NREN, cloud private delle NREN, blog, strumenti di gestione di progetti e fondi di ricerca, ecc.
  - **NO**: servizi di accesso alle risorse elettroniche a licenza come le riviste elettroniche, o Software as a Service.
- **Scalare**: tramite l'utilizzo di un Entity Category specifica permette di costruire filtri dinamici, e quindi evita configurazioni *ad hoc* per ogni Service Provider.
- **Semplificare**: l'uso di risorse condivise e distribuite su piu' Service Provider e' reso possibile tramite il rilascio di un identificatore condiviso.

R&S attributes bundle e IDEM

Definizioni	Rilascio	REFEDS attributes	IDEM
shared user identifier	obbligatorio	`eduPersonPrincipalName` (if non-reassigned)	`eduPersonPrincipalName` non e' riassegnabile per regole federazione Il rilascio di `eduPersonTargetedID` è fortemente raccomandato
		`eduPersonPrincipalName` + `eduPersonTargetedID`	
person Name	obbligatorio	`displayName`	Supporto attributi raccomandati
		`givenName` + `sn`	
email address	obbligatorio	`mail`	Supporto attributo raccomandato
affiliation	opzionale	`eduPersonScopedAffiliation` (ePSA)	Rilascio fortemente raccomandato

GÉANT Data Protection CoCo

GÉANT Data Protection Code of Conduct v1.0 14 Giugno 2013

- Progetto congiunto REFEDS GN3+
- Ambito di applicazione:
  - EU
  - Area Economica Europea (EEA)
  - *countries with adequate data protection pursuant to Article 25.6 of the directive 95/46/EC*
- Normativa di riferimento:
  - Direttiva UE sulla protezione dei dati (95/46/EC - 24/10/1995)

GÉANT Data Protection CoCo e Service Provider

Obblighi per i Service Provider:

- Entity Category Code of Conduct
- Elenco degli attributi richiesti in `<md:requestedAttributes>`
  - Gli attributi DEVONO essere richiesti con l'opzione `isRequired="true"`
  - Se il SP ha bisogno di un valore specifico per un attributo, lo DEVE richiedere esplicitamente utilizzando l'elemento `<saml:AttributeValue>`.
- Privacy policy pubblicata e referenziata in `<mdui:privacyStatementURL>`
- Nome (significativo) del servizio in `<mdui:displayName>`
- Gli elementi `<mdui>` DEVONO avere anche una descrizione in inglese (`xml:lang="en"`)
- Descrizione (significativa) del servizio in `<mdui:Description>`

Consortium GARR
THE ITALIAN EDUCATION & RESEARCH NETWORK

Fine

Domande?

Davide Vaghetti (davide.vaghetti@garr.it)
Marco Malavolti (marco.malavolti@garr.it)