eduGAIN allarga i confini di IDEM

Barbara Monticini

Convegno IDEM

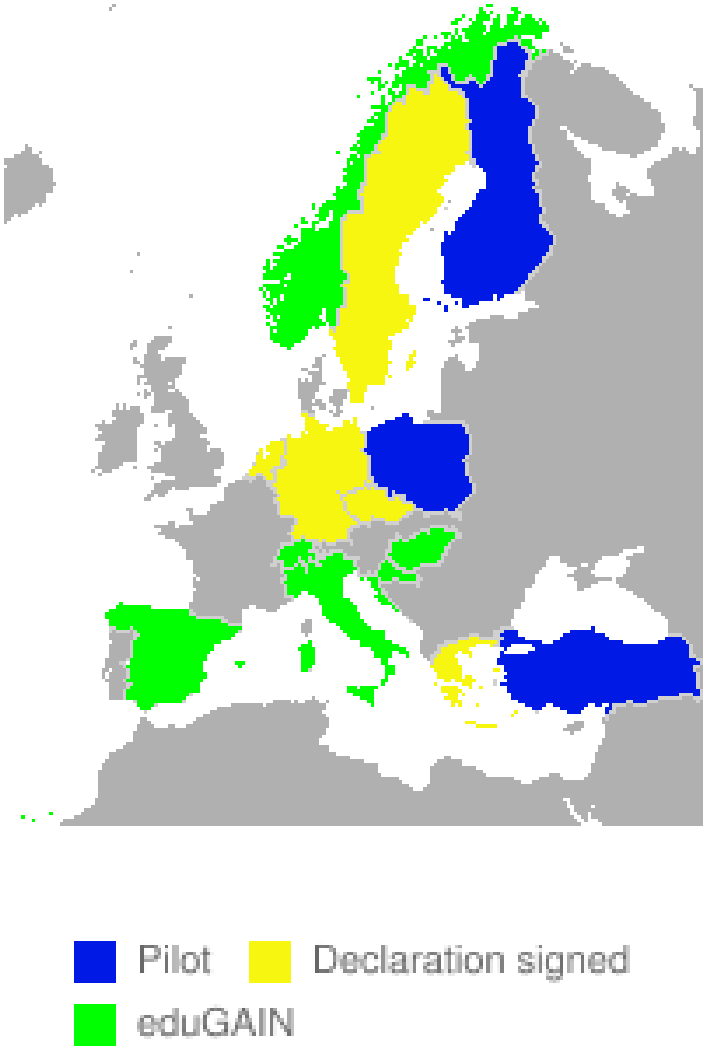
Bologna, 9 novembre 2011

Contenuti

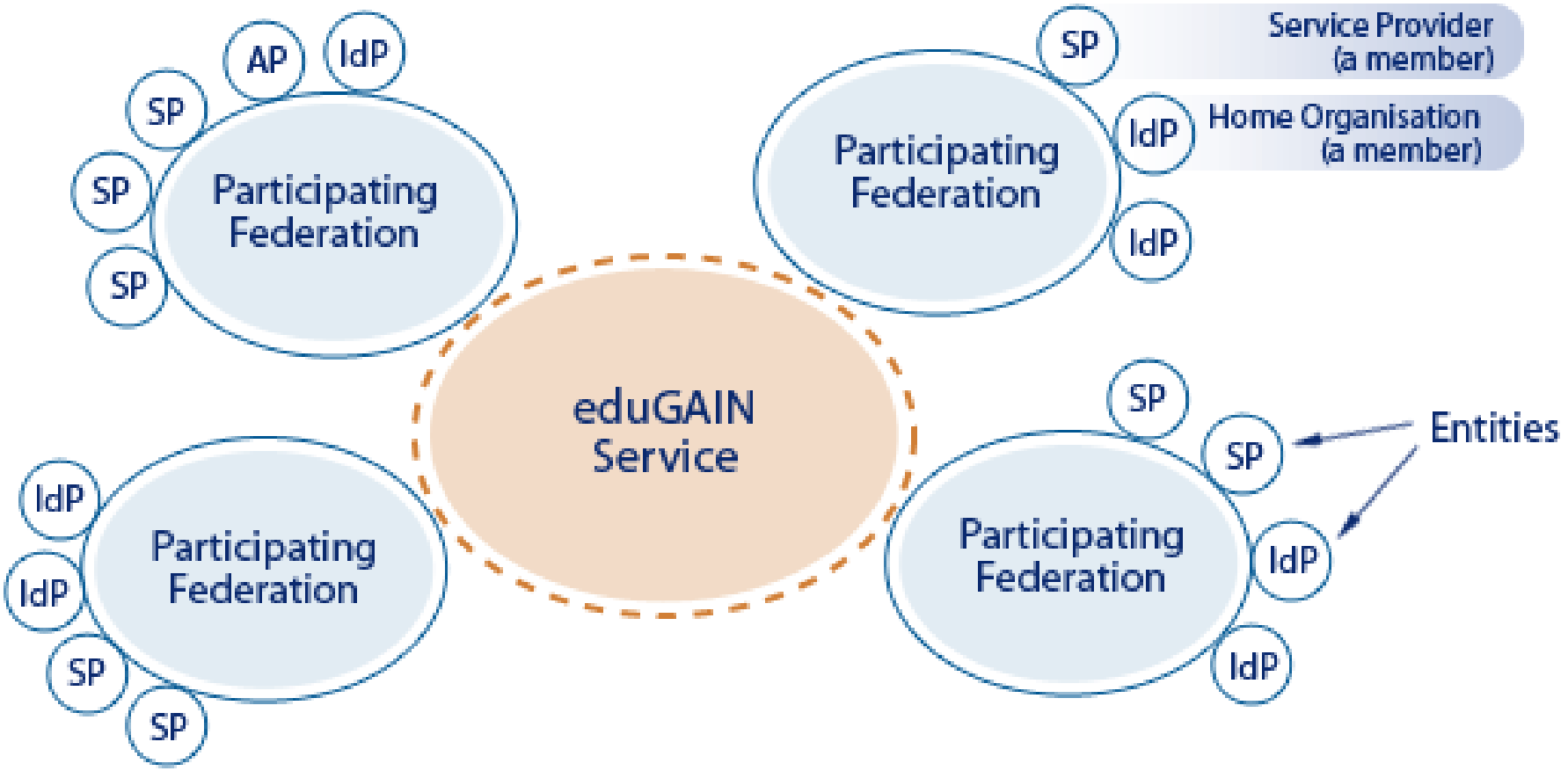
- Introduzione a eduGAIN
- eduGAIN Policy Framework
- IDEM entra in eduGAIN: work in progress
- Gli aspetti legali non saranno trattati

Cos'è eduGAIN

- É un servizio di **interconnessione per federazioni** basato su SAML
  - E' sviluppato e gestito all'interno del progetto **GÉANT**
- É entrato in produzione ad Aprile 2011
- →http://www.edugain.org



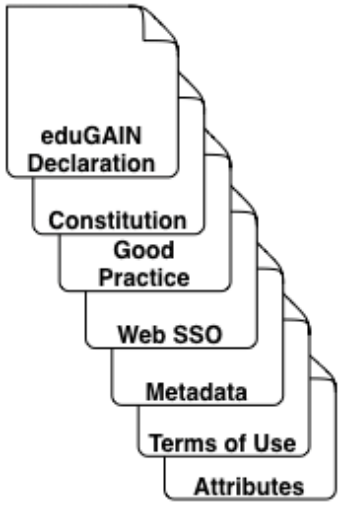
Uno sguardo d'insieme

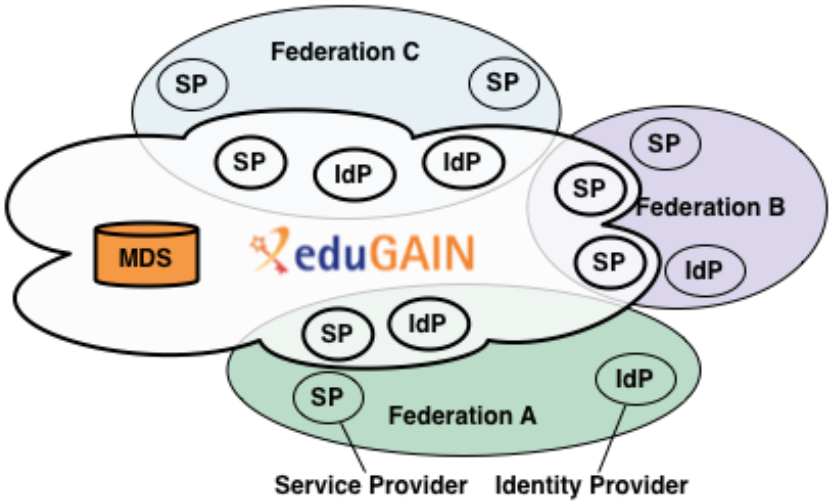


Vantaggi di eduGAIN

- Per gli utenti:
  - Estendere l'uso della propria identità digitale verso l'area della Ricerca europea
  - Accesso a nuove risorse
- Per i fornitori di servizi:
  - Allargare il bacino di utenza oltre i confini della federazione/paese di appartenenza
  - Riduzione dei costi di sviluppo e operatività del servizio
- Per le federazioni:
  - Offrire nuovi servizi evitando il ricorso ad accordi bilaterali tra federazioni

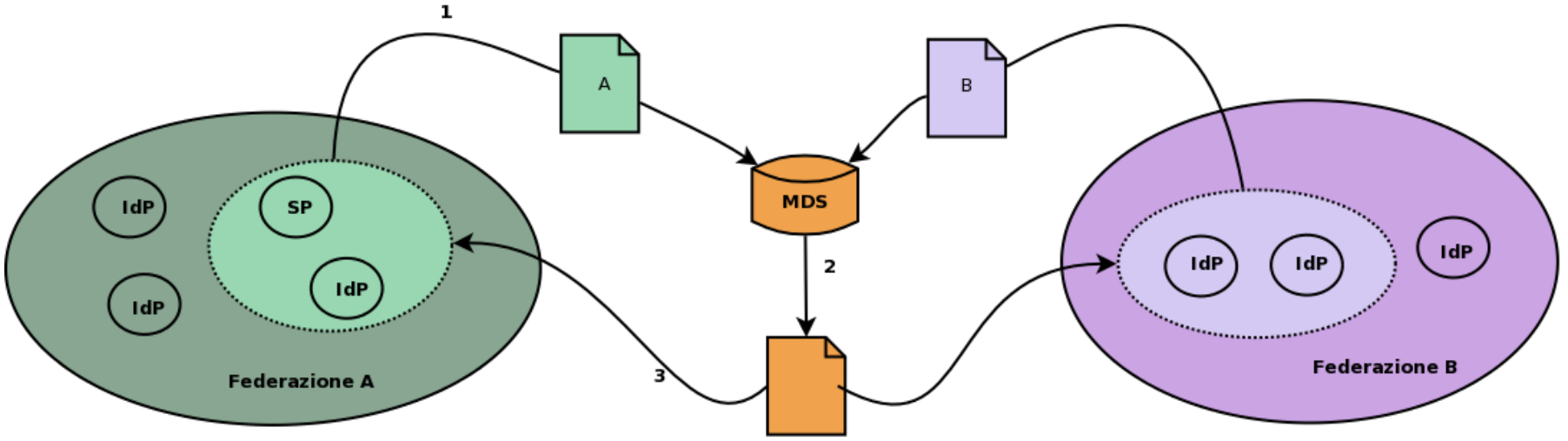
Architettura di eduGAIN





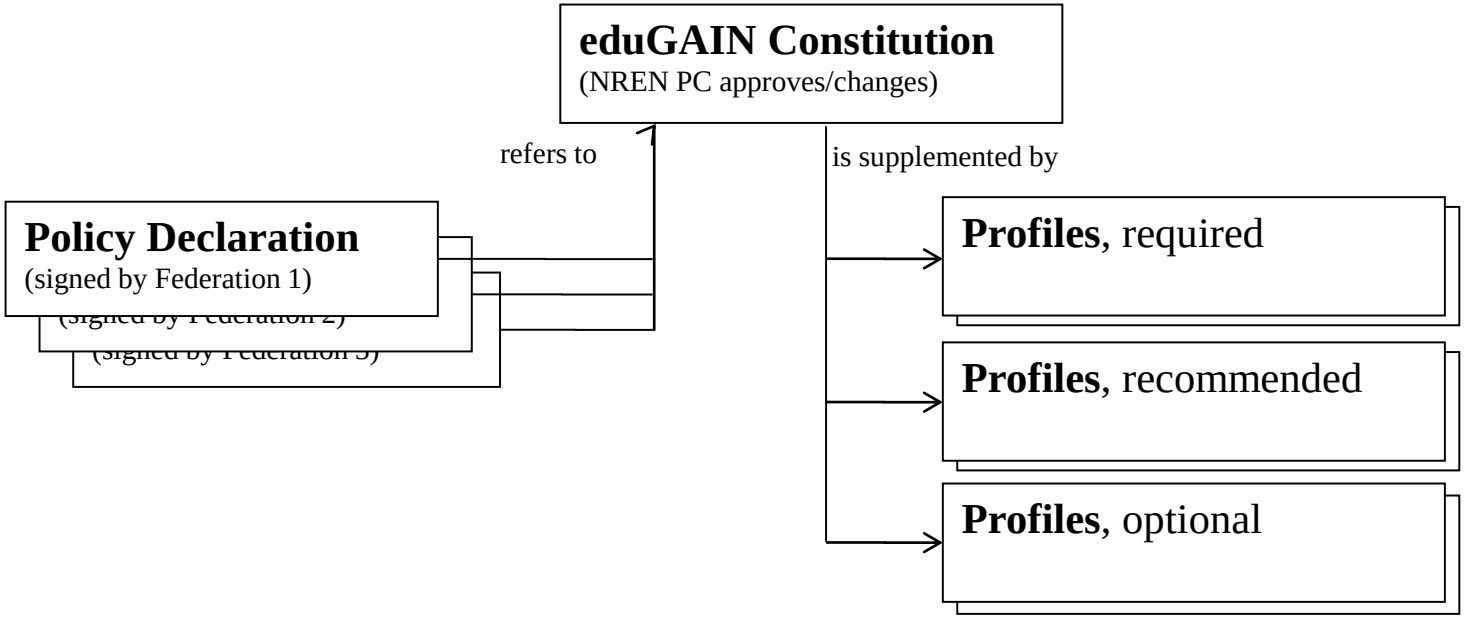
- Solo un sottoinsieme delle entità in federazione
- SAML Metadata repository centrale (MDS)
- Varie Policy per l'armonizzazione dell'ambiente

Flusso dei metadati in eduGAIN



1. Le federazioni caricano i metadati verso MDS
2. MDS aggrega i metadati ricevuti e li ripubblica
3. Le federazioni scaricano, elaborano, firmano e ripubblicano i metadati ad uso delle entità inter-federate

eduGAIN Policy Framework



1. Policy Declaration
2. Constitution
3. Metadata Terms of Access and Use
4. Metadata profile (MUST)
5. Web SSO profile (MAY)
6. Attribute profile (SHOULD)
7. Data protection good praticise profile (MAY)

SAML2 Metadata Profile (required)

- MUST: <mdrpi:PublicationInfo>
  - MUST: publisher
  - MUST: <mdrpi:UsagePolicy> with a link to Metadata ToU
  - SHOULD: creationInstant or publicationID
- <md:EntityDescriptor> elements
  - MUST: <md:ContactPerson> with contactType="technical“
    - MUST: <md:EmailAddress>
  - MUST: <mdrpi:RegistrationInfo>
    - MUST: registrationAuthority
    - SHOULD: registrationInstant, <mdrpi:RegistrationPolicy>
  - SHOULD: <md:Organization> with English and native values:
    - <md:OrganizationName>,<md:OrganizationDisplayName>,<md:OrganizationURL>

SAML2 Metadata Profile (required)

- If <md:EntityDescriptor> contains <md:IDPSSODescriptor> or <md:AttributeAuthorityDescriptor> or <md:SPSSODescriptor>
  - SHOULD: <mdui:DisplayName> and <mdui:Description> in English and native language(s)
- If <md:EntityDescriptor> contains <md:SPSSODescriptor>
  - MAY:<md:AttributeConsumingService>
- Aggregated <md:EntityDescriptor>
  - SHOULD: <mdrpi:PublicationPath>
- MUST: Conformance to SAML V2.0 Metadata Interoperability Profile
- MUST: signed with RSA private key >= 2048

Attribute Profile (recommended)

- RECOMMENDED attributes: displayName, common name, mail, eduPerson(Scoped)Affiliation, schacHomeOrganization and schacHomeOrganizationType
  - At least one schacHomeOrganizationType SHOULD be from international vocabulary urn:mace:terena.org:schac:homeOrganizationType:int
- MUST: eP(S)A vocabulary: member,faculty,student,alum,affiliate,library-walk-in
  - Semantics as defined by REFEDS comparison ver 0.13
- SAML2 persistent ID is RECOMMENDED as the unique ID
  - Placed in SAML assertion’s subject/nameID element and attribute statement

Considerazioni

- Aggregazione e scambio di SAML2 metadata
- Nessuna modifica alle regolamentazioni delle federazioni partecipanti
- Requisiti obbligatori per IdP e SP al minimo indispensabile
  - Requisiti presenti in Profili *recommended* e *optional*
- Il profilo degli attributi è *recommended*
- Inizialmente è definito solo il profilo SAML2 WebSSO
- Inizialmente solo federazioni europee nel bacino del progetto **GÉANT**

IDEM status

- Cosa è stato fatto
  - **eduGAIN Policy Declaration** firmata!
  - Metadati creati, firmati e rilasciati verso MDS
  - Prima entità in eduGAIN: *Id. Provider del GARR*

IDEM status

- Work in progress
  - Garantire che solo chi ha dato il consenso (**opt-in**) sia in eduGAIN
  - Gestire la procedura di consenso ed ingresso
  - Supporto a idp e sp per conformarsi alle regole di eduGAIN (rilascio attributi, discovery service)
  - Ri-pubblicazione dei metadati di eduGAIN: rimozione dei duplicati, gestione di numerose entità, blacklist & whitelist ...
  - Specifiche Tecniche Attributi ... in chiave eduGAIN

Riferimenti

- eduGAIN web site: http://www.edugain.org
- IDEM web site: eduGAIN faq
  https://www.idem.garr.it/it/informazioni-tecniche/283-faq-edugain