Come gestire gli incidenti di sicurezza e l'accesso alle risorse in ambito federato

IDEM DAYS 2021

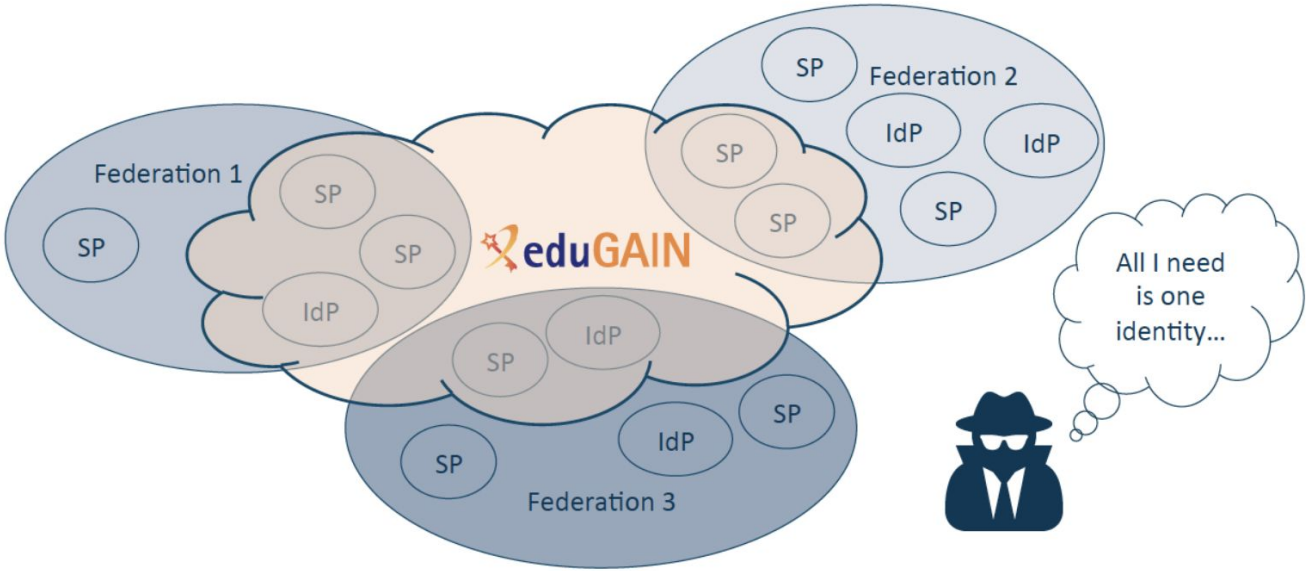
Marco Malavolti - marco.malavolti@garr.it

Davide Vaghetti - davide.vaghetti@garr.it

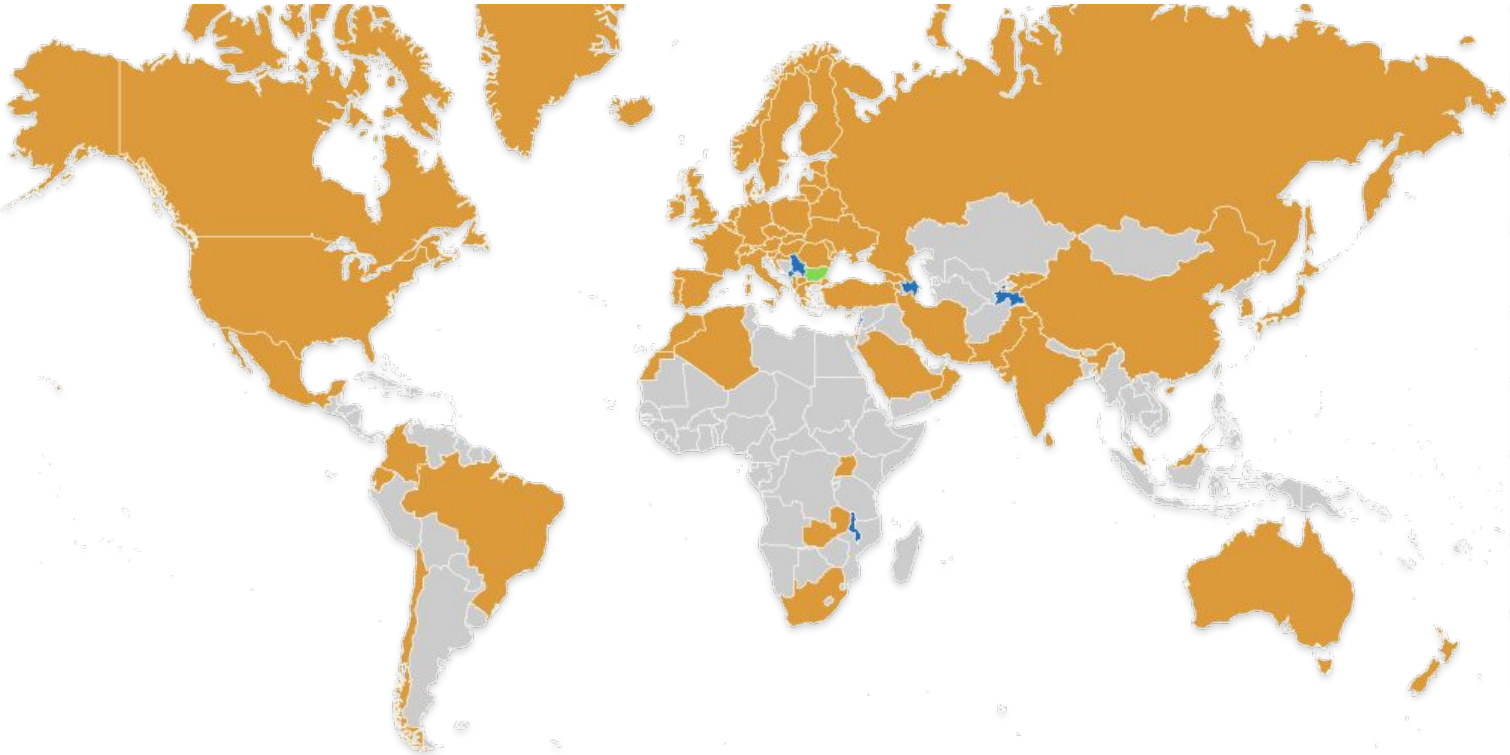
Gestione degli incidenti di sicurezza in ambito federato

Perché incidenti di sicurezza in ambito federato?

- eduGAIN rappresenta un'ampia superficie di attacco.
- Mancanza di un CSIRT centralizzato.
- Tutti i partecipanti devono collaborare per gestire gli incidenti di sicurezza.



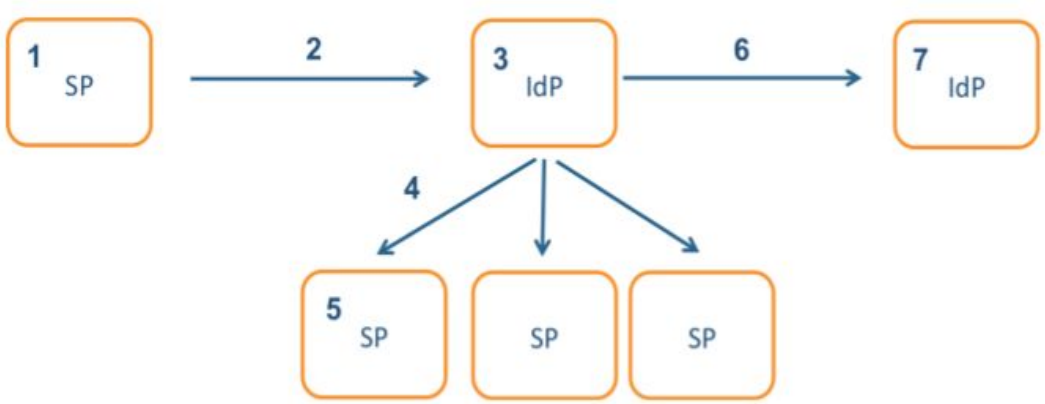
eduGAIN



Federations in eduGAIN	
Participants	71
Voting-only Members	2
Candidates	7
Entities in eduGAIN	
All entities	7352
IdPs	4172
SPs	3186
Standalone AAs	3

L’esigenza di un trust framework

Deliverable DNA3.2:DNA3.2 -Security Incident Response Procedure
https://aarc-project.eu/wp-content/uploads/2017/02/DNA3.2-Security-Incident-Response-Procedure-v1.0.pdf



1. Intrusion involving a federated identity is suspected at an SP

2. SP notifies the IdP associated with the identity

3. IdP discovers that they are fully compromised due to a software vulnerability, contains the security incident and begins recovery process

4. IdP notifies any SPs contacted by compromised identities

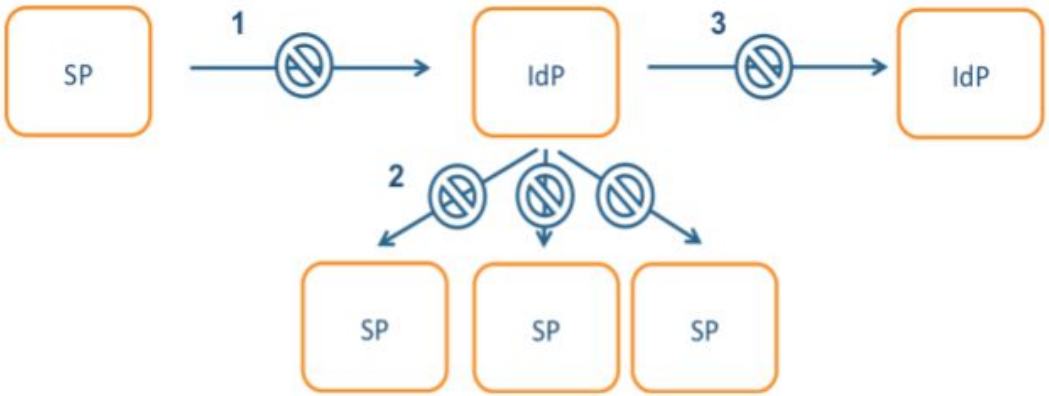
5. SPs begin investigation of activity performed by compromised identities

6. IdP distributes information on the security incident appropriately, alerting an additional IdP using the software that led to the compromise

7. IdP begins their own investigation

L’esigenza di un trust framework

Deliverable DNA3.2:DNA3.2 -Security Incident Response Procedure
https://aarc-project.eu/wp-content/uploads/2017/02/DNA3.2-Security-Incident-Response-Procedure-v1.0.pdf



1. SP does not inform the IdP since federated identities are outside the scope of the SP’s security mandate

2. IdP does not inform the affected SPs either due to fear of a leak of sensitive information and damage to their reputation or to being out of scope of their mandate

3. IdP does not alert additional IdP since there is no established channel of communication between participants

Domande

REFEDS Sirtfi

Security Incident Response Trust Framework for Federated Identity

Operational Security

information resources … availability and integrity ... confidentiality of sensitive information

Traceability

be able to answer the basic questions "who, what, where, and when" concerning a security incident

Incident Response

a security incident response capability exists within the organisation

Participant Responsibilities

All participants (IdPs and SPs) in the federations need to rely on appropriate behavior.

Sirtfi - Operational Security

[OS1] Security patches in operating system and application software are applied in a timely manner.
[OS2] A process is used to manage vulnerabilities in software operated by the organisation.
[OS3] Mechanisms are deployed to detect possible intrusions and protect information systems from significant and immediate threats.
[OS4] A user's access rights can be suspended, modified or terminated in a timely manner.
[OS5] Users and Service Owners (as defined by ITIL [ITIL]) within the organisation can be contacted.
[OS6] A security incident response capability exists within the organisation with sufficient authority to mitigate, contain the spread of, and remediate the effects of a security incident.

Sirtfi - Incident Response

[IR1] Provide security incident response contact information as may be requested by an R&E federation to which your organization belongs.
[IR2] Respond to requests for assistance with a security incident from other organisations participating in the Sirtfi trust framework in a timely manner.
[IR3] Be able and willing to collaborate in the management of a security incident with affected organisations that participate in the Sirtfi trust 4 TITLE /REFERENCE: SIRTFI framework.
[IR4] Follow security incident response procedures established for the organisation.
[IR5] Respect user privacy as determined by the organisations policies or legal counsel.
[IR6] Respect and use the Traffic Light Protocol [TLP] information disclosure policy.

Sirtfi - Traceability

[TR1] Relevant system generated information, including accurate timestamps and identifiers of system components and actors, are retained and available for use in security incident response procedures.
[TR2] Information attested to in [TR1] is retained in conformance with the organisation's security incident response policy or practices.

Sirtfi - Participant Responsibilities

[PR1] The participant has an Acceptable Use Policy (AUP).
[PR2] There is a process to ensure that all users are aware of and accept the requirement to abide by the AUP, for example during a registration or renewal process.

Domande

Traffic Light Protocol

https://www.first.org/tlp/

TLP:RED	Not for disclosure, restricted to participants only.
TLP:AMBER	Limited disclosure, restricted to participants' organizations.
TLP:GREEN	Limited disclosure, restricted to the community.
TLP:WHITE	Disclosure is not limited.

TLP - Tratti essenziali

- Facilita la **condivisione** di informazioni sensibili tra gli attori coinvolti.
- Fornisce uno schema **semplice** ed intuitivo per la condivisione.
- E' **facile da adottare** e da comprendere.
- Compatibile con **altre regole di condivisione** (*Chatham House Rule*).
- Il **mittente verifica il rispetto di TLP** per tutti gli attori coinvolti.
- Richiede il **permesso della fonte** per condivisione più ampia.

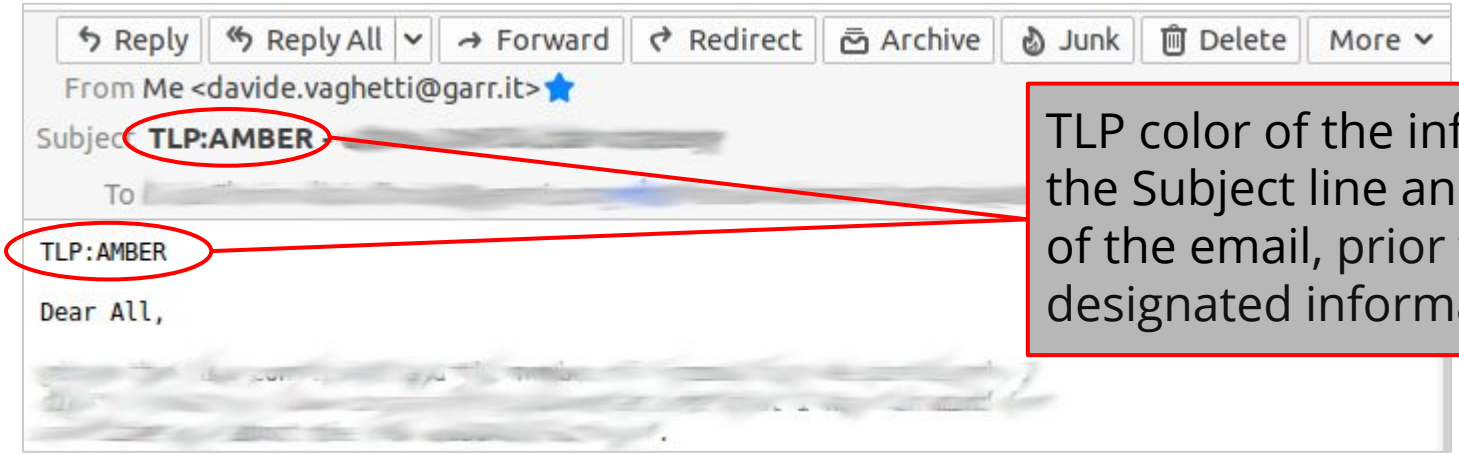
TLP:RED	Not for disclosure, restricted to participants only.
	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused. Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.

TLP:AMBER	Limited disclosure, restricted to participants' organizations.
	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**

TLP:GREEN	Limited disclosure, restricted to the community.
	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.

TLP:WHITE	Disclosure is not limited.
	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

TLP - email



TLP color of the information in the Subject line and in the body of the email, prior to the designated information itself.

Chatham House Rule

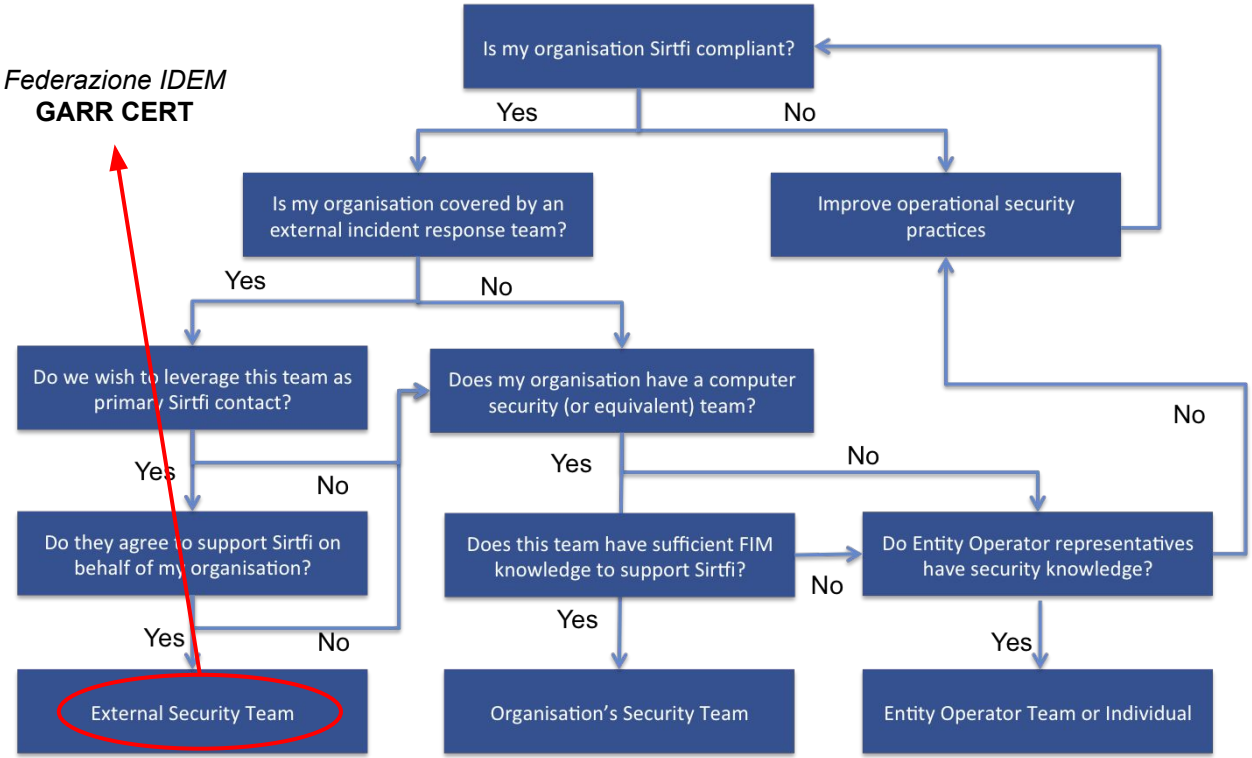
“When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.”

Domande

Sirtfi e IDEM

1. Autovalutazione dei requisiti.
2. Scelta del security contact.
3. Richiesta tramite registry.
4. Valutazione del servizio e approvazione.

Sirtfi: scelta del security contact



Fonte: https://wiki.refeds.org/display/SIRTFI/Choosing+a+Sirtfi+Contact

Federazione IDEM

GARR mette a disposizione GARR-CERT come "External Security Team" a disposizione dei membri della Federazione IDEM come contatto per la gestione degli incidenti di sicurezza.

Sirtfi metadata: security contact

Aggiunta del REFEDS security contact nei metadata dell'entità

```
<EntityDescriptor entityID=$$IDEM-MEMBER-ENTITYID$$>
[...]
    <ContactPerson
       contactType="other"
       remd:contactType="http://refeds.org/metadata/contactType/security">
        <GivenName>GARR-CERT</GivenName>
        <EmailAddress>mailto:cert@garr.it</EmailAddress>
    </ContactPerson>
</EntityDescriptor>
```

Sirtfi metadata: entity attribute

Aggiunta dell'asserzione per indicare l'adesione a Sirtfi

```
<mdattr:EntityAttributes
        xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
  <saml:Attribute
        xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
        Name="urn:oasis:names:tc:SAML:attribute:assurance-certification">
      <saml:AttributeValue>https://refeds.org/sirtfi</saml:AttributeValue>
  </saml:Attribute>
</mdattr:EntityAttributes>
```

Domande

For computer security emergencies or in case a security incident is suspected:
Contact the eduGAIN Security Team: abuse@edugain.org

<eduGAIN Security Team PGP key file>
PGP key fingerprint: F9FF B82B 9700 72D1 F753 25CF 5E3C 31D7 CE43 BCB8

https://wiki.geant.org/display/eduGAIN/eduGAIN+Security

eduGAIN Security Incident Response Handbook

https://wiki.refeds.org/display/CON/Consultation%3A+eduGAIN+Security+Incident+Response+Handbook

Entity Categories

Entity Categories

OASIS Technical Committee

SAML V2.0 Metadata Extension for Entity Attributes

https://wiki.oasis-open.org/security/SAML2MetadataAttr

REFEDS Entity Categories Working Group

The Entity Category SAML Attribute Types

https://tools.ietf.org/html/draft-young-entity-category-07

Entity Attributes Metadata Extension

Un meccanismo per inserire ulteriori informazioni all'interno dei metadata di ogni entità.

Riferimento esplicito ai federation operatores come agente dell'inserimento (o, per estensione, la parte fidata che tramite la firma valida metadata).

Estensione per i tag `<md:EntityDescriptor>` e `<md:EntitiesDescriptor>`

- Supporta sia Service Provider sia Identity Provider
- Supporta sia `<saml:Attribute>` sia `<saml:Assertion>` (solo se riguarda un un'unica entità)

Entity Attributes Metadata Extension

Extension schema:

```
<element name="EntityAttributes"
type="mdattr:EntityAttributesType"/>
<complexType name="EntityAttributesType">
  <choice maxOccurs="unbounded">
    <element ref="saml:Attribute"/>
    <element ref="saml:Assertion"/>
  </sequence>
</complexType>
```

Entity Attributes Metadata Extension

Extension XML example template:

```
<EntityDescriptor entityID=$$ENTITY_ID$$>
  <Extensions>
    <mdattr:EntityAttributes>
      <saml:Attribute  Name=$$ATTRIBUTE-NAME$$
                       NameFormat=$$ATTRIBUTE-NAME_FORMAT$$>
        <saml:AttributeValue>
          $$ATTRIBUTE-VALUE$$
        </saml:AttributeValue>
      </saml:Attribute>
    </mdattr:EntityAttributes>
</Extensions>
[..]
</EntityDescriptor>
```

Entity Category Attribute Types

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.
- ecc.

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

Formato e valore di ambedue gli attributi sono gli stessi:

- `NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"`
- Una URI valida (MUST) che punti ad una pagina in cui e' descritta la entity category

Entity Category Attribute Types

Entity Category Attribute

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

Entity Category Attribute Types

Entity Category Support 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>
```

International 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

REFEDS Research and Scholarship

Rilasciare attributi per la ricerca
- **SI**: wiki, cloud private, ecc.
- **NO**: risorse elettroniche a licenza

Scalare: filtri dinamici, e quindi evita configurazioni *ad hoc* per ogni Service Provider.

Semplificare: identificatore condiviso.

REFEDS Research and Scholarship

Requisiti per i Service Provider:

4.1 The service enhances the research and scholarship activities of some subset of the user community.

4.2 Service metadata has been submitted to the registrar for publication.

4.3 The service meets the following technical requirements:

- *4.3.1 The Service Provider is a production SAML deployment that supports SAML V2.0 HTTP-POST binding.*
- *4.3.2 The Service Provider claims to refresh federation metadata at least daily.*
- *4.3.3 The Service Provider provides an mdui:DisplayName and mdui:InformationURL in metadata (an english language version xml:lang="en" is RECOMMENDED).*
- *4.3.4 The Service Provider provides one or more technical contacts in metadata.*

REFEDS Research and Scholarship

R&S attribute 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

REFEDS Research and Scholarship

R&S Entity Category per Service Provider

```
<mdattr:EntityAttributes xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
  <saml:Attribute
      xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
      Name="http://macedir.org/entity-category"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
    <saml:AttributeValue>
        http://refeds.org/category/research-and-scholarship
    </saml:AttributeValue>
  </saml:Attribute>
</mdattr:EntityAttributes>
```

REFEDS Research and Scholarship

R&S Entity Category Support per Identity Provider

```
<mdattr:EntityAttributes xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
  <saml:Attribute
      Name="http://macedir.org/entity-category-support"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
    <saml:AttributeValue>
        http://refeds.org/category/research-and-scholarship
    </saml:AttributeValue>
  </saml:Attribute>
</mdattr:EntityAttributes>
```

REFEDS Research and Scholarship

Versione 2 (R&Sv2) attualmente in sviluppo:

- Support per OpenID Connect.
- nuovo identificatore SAML: *subject-id*.
- affiliazione inclusa di default.

Domande

REFEDS Hide from discovery

- Solo per Identity Provider (IdP)
- Segnala ai servizi di discovery che questo IdP non deve essere mostrato tra le scelte possibili.
- Casi d'uso:
  - IdP non ancora in produzione (IDEM ha gia' una federazione di test per questo caso d'uso).
  - Due IdP dello stesso ente (test e produzione) con nomi simili.
  - IdP ad accesso limitato (ad es. solo da certe reti).
  - IdP con problemi operativi temporanei ma di durata tale da giustificare la rimozione dal discovery.

REFEDS Hide from discovery

REFEDS Hide from discovery Metadata

```
<Extensions xmlns:mdattr=”urn:oasis:names:tc:SAML:metadata:attribute”>
    <mdattr:EntityAttributes xmlns:saml=”urn:oasis:names:tc:SAML:2.0:assertion”>
        <saml:Attribute
          Name=”http://macedir.org/entity-category”
          NameFormat=”urn:oasis:names:tc:SAML:2.0:attrname-format:uri”>
            <saml:AttributeValue>
                http://refeds.org/category/hide-from-discovery
            </saml:AttributeValue>
        </saml:Attribute>
    </mdattr:EntityAttributes>
</Extensions>
```

Domande

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

GÉANT Data Protection Code of Conduct

https://geant3plus.archive.geant.net/uri/dataprotection-code-of-conduct/V1/Documents/GEANT_DP_CoC_ver1.0.pdf

Entity Category Specification: Data Protection Code of Conduct

https://wiki.refeds.org/download/attachments/1606124/GEANT_DP_CoCo_Entity_Category_ver1.2.pdf

SAML 2 Profile for the Data Protection Code of Conduct

https://geant3plus.archive.geant.net/uri/dataprotection-code-of-conduct/V1/Documents/GEANT_DP_CoCo_saml2_profile_ver1%201.pdf

GÉANT Data Protection CoCo

Service Provider:

https://wiki.geant.org/display/eduGAIN/CoCo+Recipe+for+a+Service+Provider

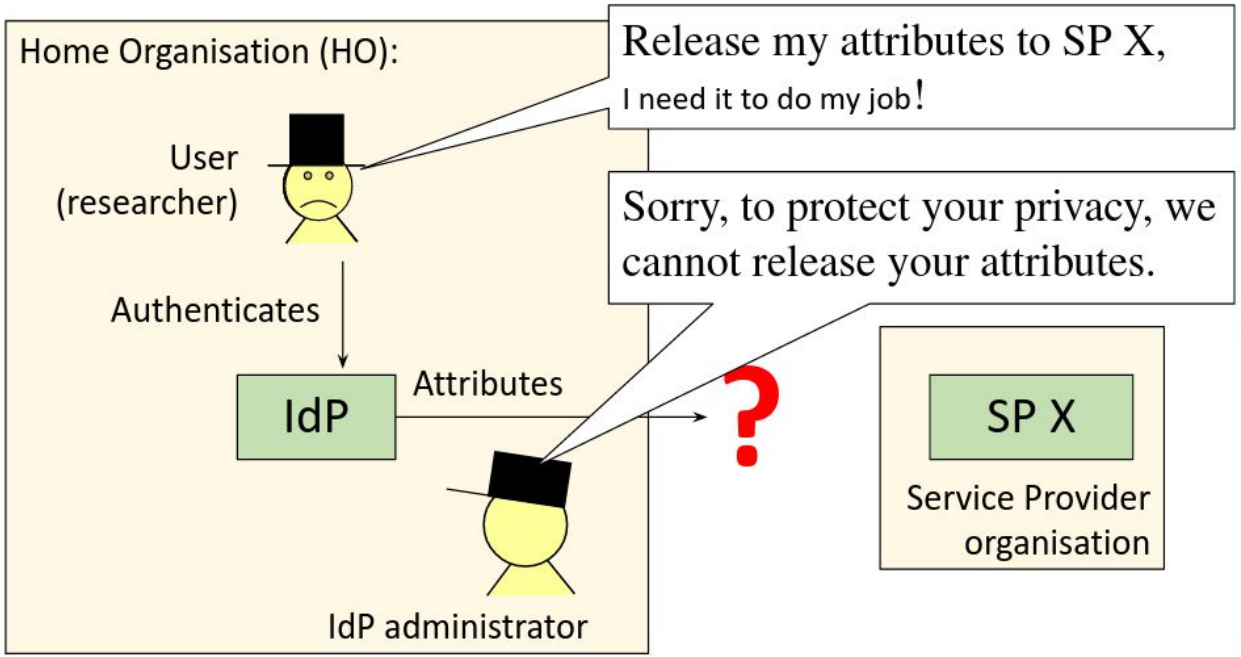
Home Organisation (Identity Provider):

https://wiki.geant.org/display/eduGAIN/CoCo+Recipe+for+a+Home+Organisation

Identity Federations:

https://wiki.geant.org/display/eduGAIN/Recipe+for+a+Federation+Operator

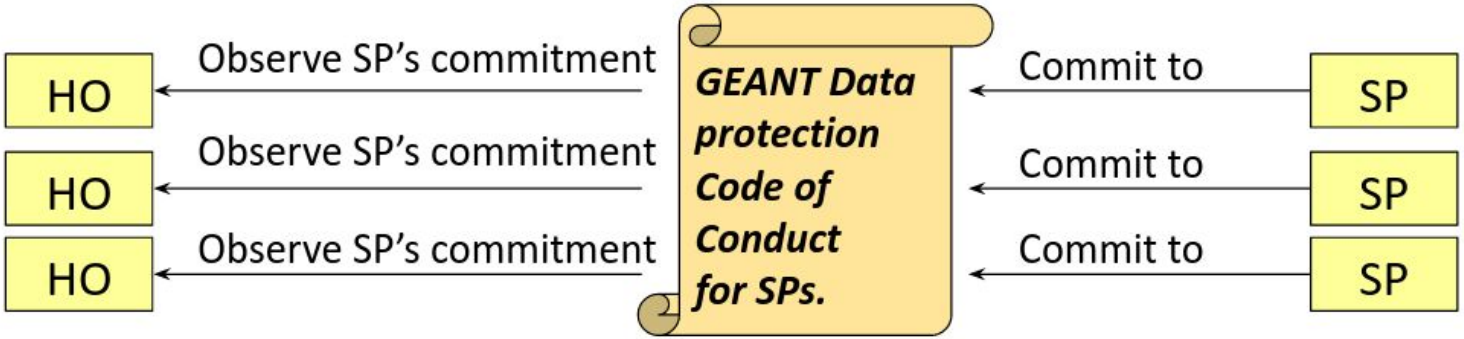
GÉANT Data Protection CoCo



Typical user attributes [personal data]:
- name
- e-mail address
- unique user identifier
- role and affiliation ("student@universityx.org")
- dedicated permissions to use the service

Mikael Linden, https://wiki.refeds.org/display/CODE/Code+of+Conduct+ver+2.0+project

GÉANT Data Protection CoCo



- Service Providers (SP) commits to the CoCo
- Identity federations (and eduGAIN) relays SPs' commitment to Home Organisations (HO)
- HO decides if it feels confident to release attributes to the SP

Mikael Linden, https://wiki.refeds.org/display/CODE/Code+of+Conduct+ver+2.0+project

GÉANT Data Protection CoCo

A. Legal compliance
B. Purpose limitation
C. Data minimisation
D. Deviating purposes
E. Data retention
F. Third parties
G. Security measures
H. Information duty towards End User
I. Information duty towards Home Organisation

A. Security Breaches
B. Liability
C. Transfer to third countries
D. Governing law and jurisdiction
E. Eligibility to execute
F. Termination of the Code of Conduct
G. Survival of the clauses
H. Precedence

GÉANT Data Protection CoCo

Requisiti per i Service Provider

Entity Category nei metadata

Privacy policy pubblicata e in

`<mdui:privacyStatementURL>`

Elenco attributi in

`<md:requestedAttributes>`

`<mdui:displayName>`

`<mdui:Description>`

`xml:lang="en"`

GÉANT Data Protection CoCo

Service Provider Metadata: Entity Category

```
<EntityAttributes xmlns="urn:oasis:names:tc:SAML:metadata:attribute">
    <Attribute
       xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
       NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
       Name="http://macedir.org/entity-category">
        <AttributeValue>
            http://www.geant.net/uri/dataprotection-code-of-conduct/v1
        </AttributeValue>
    </Attribute>
</EntityAttributes>
```

GÉANT Data Protection CoCo

Service Provider Metadata: mdui

```
<SPSSODescriptor>
   <Extensions>
      <UIInfo xmlns=”urn:oasis:names:tc:SAML:metadata:ui”>
         <DisplayName xml:lang="it">$$DISPLAY-NAME$$</DisplayName>
         <DisplayName xml:lang="en">$$DISPLAY-NAME$$</DisplayName>
         <Description xml:lang="it">$$DESCRIPTION$$</Description>
         <Description xml:lang="en">$$DESCRIPTION$$</Description>
         <PrivacyStatementURL xml:lang="it">$$PRIVACY-POLICY-URI$$</PrivacyStatementURL>
         <PrivacyStatementURL xml:lang="en">$$PRIVACY-POLICY-URI$$</PrivacyStatementURL>
      </UIInfo>
   </Extensions>
[...]
```

GÉANT Data Protection CoCo

Service Provider Metadata: requested attributes

```
<AttributeConsumingService>
    <RequestedAttribute
        FriendlyName="displayName"
        Name="urn:oid:2.16.840.1.113730.3.1.241"
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
        isRequired="true"/>
    <RequestedAttribute
        FriendlyName="eduPersonPrincipalName"
        Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
        isRequired="true"/>
</AttributeConsumingService>
```

GÉANT Data Protection CoCo

Obblighi per gli Identity Provider e Metadata:

IdPs MUST provide an Entity Category support attribute ..

```
<EntityAttributes xmlns="urn:oasis:names:tc:SAML:metadata:attribute">
    <Attribute
       xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
       NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
       Name="http://macedir.org/entity-category-support">
        <AttributeValue>
            http://www.geant.net/uri/dataprotection-code-of-conduct/v1
        </AttributeValue>
    </Attribute>
</EntityAttributes>
```

GÉANT Data Protection CoCo ver 2.0

- Una versione 2.0 è stata creata in modo da uniformarla al GDPR.
- Perché sia legalmente valido il CoCo deve essere registrato da un'autority nazionale.
- Al momento non può essere registrato dato che nelle linee guida dello European Data Protection Board non è definito il caso dei trasferimenti di dati internazionali.
- Dopo una consultazione interna alla comunità REFEDS è stato deciso di limitare l'ambito ai trasferimenti europei, ma **di fatto il lavoro si è arenato**.
- https://wiki.refeds.org/display/CODE/Code+of+Conduct+ver+2.0+project

Domande

Grazie per l'attenzione!
Domande?

IDEM DAYS 2021

Marco Malavolti - marco.malavolti@garr.it

Davide Vaghetti - davide.vaghetti@garr.it