Identity Management Practice Statement:
DOPAU 2.0 on-line

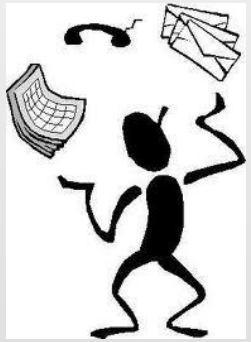
#Burocrazia in 30 minuti

Sandro Tumini - Università Politecnica delle Marche

DOCUMENTI DELLA FEDERAZIONE IDEM

Informazioni e raccomandazioni per evitare confusioni:

- DOPAU 2.0;
- IDEM METADATA PROFILE;
- RACCOMANDAZIONE SULL'USO DELL'ATTRIBUTO EPSA;



Nel 2009 ci eravamo lasciati …….

Come scrivere il Documento del Processo di Accreditamento degli Utenti (DOPAU)

in 1 giorno

http://www.garr.it/eventiGARR/idem-day/docs/sacca_pres_idemday09.pdf

info tratte dalla presentazione Ing. Angelo Saccà - Università degli Studi di Torino

Nel 2014 dal portale della federazione..

‘Al fine di assicurare che le asserzioni sugli attributi che vengono inviate dagli Identity Provider ai Service Provider siano sufficientemente robuste e fidate per gestire l'accesso ad importanti risorse protette, ***ci si aspetta dagli Identity Provider*** che essi gestiscano le identità digitali in modo accurato e nel rispetto dei ‘*vincoli di privacy*’ imposti dalla legislazione corrente e dalla Federazione.’

FEDERATION TRUST: Obiettivo e Strumento

Per raggiungere tale obiettivo **IDEM** richiede che ogni Partecipante renda disponibile agli altri Partecipanti certe **informazioni di base** riguardanti il proprio sistema di **identity management**, incluse le informazioni relative agli attributi che vengono utilizzati per la Federazione.

Per fornire alla Federazione le informazioni richieste occorre redigere il **DOPAU** (Documento descrittivo del Processo di Accreditamento degli Utenti dell'Organizzazione)

Documento descrittivo del Processo di Accreditamento degli Utenti dell'Organizzazione

Cosa si chiede agli ENTI:

Ha quindi come finalità la consapevolezza e la responsabilità degli enti che vi partecipano ai quali si chiede il **'reale'** processo di accreditamento dei propri utenti a garanzia e tutela di tutti i partecipanti alla Federazione.

PER POTER GARANTIRE A TUTTI ……

Documento descrittivo del Processo di Accreditamento degli Utenti dell'Organizzazione

Avevamo correttamente detto che il DoPAU non è un DPS (doc. Programmatico della sicurezza)

Ma sicuramente incluso nel documento riassuntivo delle scelte organizzative e delle strategie di sviluppo

DoPAU ⊆ Manuale della qualità

Le procedure primarie (come si svolgono le attività che costituiscono la mission dell'organizzazione)

Le procedure secondarie (come si svolgono le attività di controllo del sistema di gestione verifiche ispettive periodiche, riesami della direzione, gestione di non conformità e reclami, azioni correttive del sistema ed azioni per il miglioramento).

Quindi non una seccatura burocratica ma un'opportunità per fare un pò di chiarezza dentro la propria organizzazione ;-)

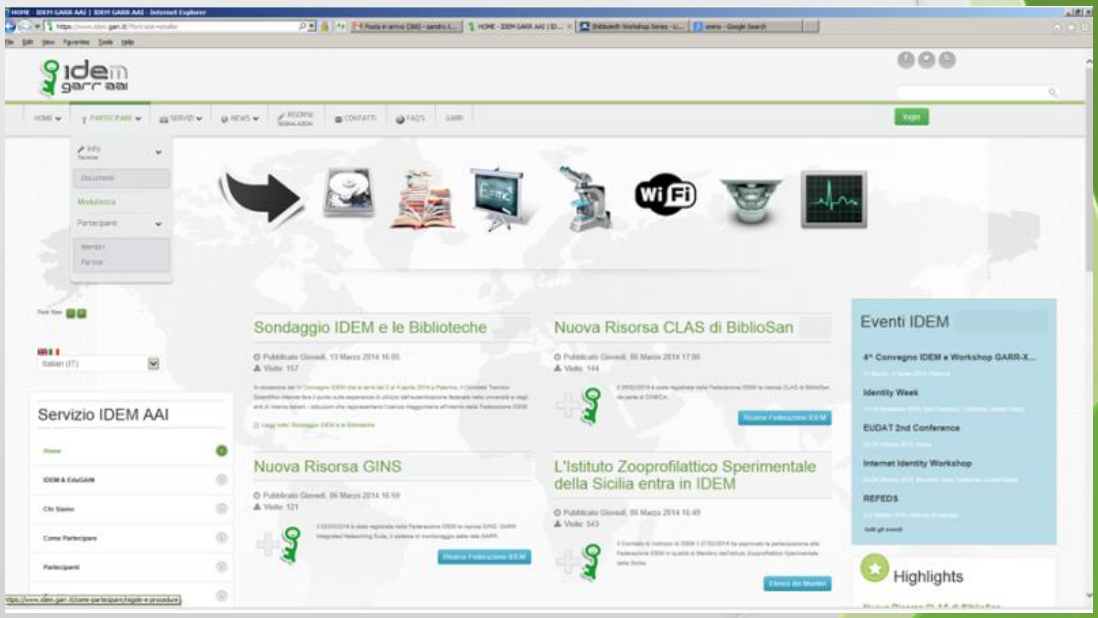
Qual'è l'impegno della Federazione.....

Produrre un DoPAU che sia:

- Essenziale;
- Immediato;
- Paperless;

 # La compilazione del questionario richiede circa 30 minuti

ON LINE



 # la compilazione del questionario può essere interrotta e salvata

Quale impegno per i partecipanti....

Ente Federato

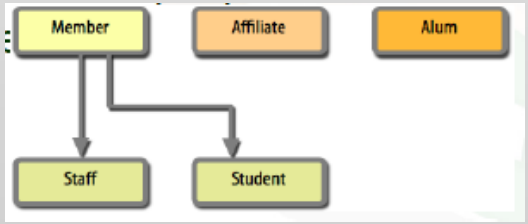
Referente Organizzativo

Referente Tecnico

1 - Redigere DoPAU

2 - Audit Periodici

Identity Management



3 - Trust con la IDEM Fed.

Es. Università / Scuole

Schema del Dopau 2.0: elementi essenziali

Organizzazione/Ente: .....

Nome e cognome di chi compila il questionario: .....

Parte I – I processi di accreditamento

- ❑ Informazione sul processo di accreditamento
- ❑ La gestione delle Identità

Parte II – Il sistema di Identity Management

- ❑ L'informazione all'utente e il consenso
- ❑ Informazione sul sistema di Identity Management

DoPAU 2.0: cosa cambia

Il questionario si suddivide in **due parti**:

La **prima parte** riguarda domande relative ad ogni processo di accreditamento e gestione delle identità che genera credenziali utilizzate per l'accesso a risorse federate.
Il questionario riguarda esclusivamente il ciclo di vita delle identità che hanno accesso alle risorse delle federazione.
E' necessario, quindi, prima di compilare questa parte che l'organizzazione partecipante individui tutti i processi di accreditamento presenti all'interno del suo ente finalizzati al rilascio di credenziali utili per accedere alle risorse federate.
Per ogni processo individuato verranno poste delle domande volte a comprendere il funzionamento dello stesso.
Esse saranno suddivise in due sezioni: *Informazioni sul processo di accreditamento, La gestione delle Identità*

La **seconda parte** riguarda in generale il sistema di Identity Management dell'organizzazione e l'informazione all'utente e il consenso in relazione ai servizi accessibili con autenticazione federata.

Per processo di accreditamento si intende l'insieme delle fasi necessarie per la creazione dell'identità digitale

Prossimo passaggio.... 'idem metadata profile'

IDEM METADATA PROFILE V1.0

- Autenticità e integrità dei metadati
  - Considerazioni sulla Sicurezza

- Requisiti per il produttore dei Metadati: esempio
  - eduGAIN
  - Informazioni relative all'Interfaccia Utente

[SAMLMetaIoP] SAML V2.0 Metadata Interoperability Profile

idem-metadata profile vers. 1.0: un rapido richiamo...

IDEM Metadata Profile definisce delle regole per coloro che, nella Federazione IDEM, producono metadati SAML (nei ruoli di registranti o aggregatori) e per i consumatori di metadati che partecipano alla Federazione IDEM.

L'adozione di questo profilo pone le basi per **un'interoperabilità scalabile**

[Σ frammenti di metadati coerentemente ordinati] ottenuta grazie al protocollo SAML.

Obiettivo:

Questo modo di operare pone le basi per avere un sistema rapido e automatizzato

per l'aggiornamento dei metadati della federazione

https://idem.garr.it/documenti/doc_download/263-idem-metadata-profile-v1-0-ita-eng

Chiarimenti sull'uso corretto di eduPersonScopedAffiliation (ePSA) nella Federazione IDEM

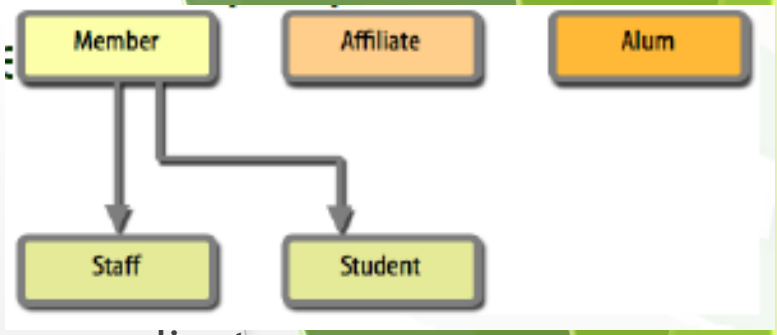
estate del 2012

Il questionario sulla valorizzazione dell'attributo ePSA, agli Enti Membri, ha evidenziato una disomogeneità nell'uso di alcuni valori negli IdP e, a volte, una comprensione parziale delle specifiche dettate dallo schema eduPerson.

Obiettivo:

Si vuole fornire una chiara ed esaustiva interpretazione dei valori di ePSA risultati più ambigui all'interno della Federazione IDEM, anche integrando la specifica eduPerson quando non sufficientemente precisa, al fine di promuoverne un uso uniforme e coerente negli IdP degli Enti Membri.

(ePSA) nella Federazione IDEM



ePSA esprime l'affiliazione dell'utente presso l'organizzazione di appartenenza mediante uno o più valori nella forma:

<affiliazione>@<organizzazione>

<affiliazione>, secondo lo schema eduPerson, può essere uno tra i seguenti valori:
faculty, student, staff, alum, member, affiliate, employee, library-walk-in. ST-A (ver. 2.2)

<organizzazione> è il nome DNS dell'organizzazione di appartenenza

Qualunque altro valore di <affiliazione> non presente nell'elenco sopra riportato non è ammesso.

(ePSA) nella Federazione IDEM
member uso corretto e alum

«generalizzazione/specializzazione» tra il valore member e i valori staff e student.

Se <affiliazione> assume uno dei valori staff e student deve sempre essere presente anche il valore member.

Altro caso non corretto: Tra gli enti della federazione ∞ **conbinazioni** <affiliazione> con il valore alum

Raccomandazione:

- <affiliazione>, quindi, assume il valore **alum** per tutti gli studenti di un Ateneo che abbiano ottenuto un titolo accademico (di primo, secondo o terzo livello, master di primo o secondo livello, etc.) presso l'Università stessa.

(ePSA) nella Federazione IDEM member vs affiliate

- <affiliazione> assume il valore **member** per tutti gli utenti per cui vi sia un rapporto istituzionale con l'organizzazione di appartenenza e a cui deve essere assicurato un insieme minimo di privilegi (es. personale docente e tecnico amministrativo, studenti, contrattisti, etc.),

- Gli utenti con <affiliazione> **affiliate**, in linea di principio, sono, quindi, utenti che hanno un qualche rapporto con l'organizzazione certificatrice dell'identità, ma che non possono essere considerati membri della stessa.

(ePSA) nella Federazione IDEM member vs affiliate

MEMBER:

- ❑ personale strutturato;
- ❑ co.co.co.;
- ❑ co.co.pro.;
- ❑ borsisti;
- ❑ assegnisti di ricerca;
- ❑ contrattisti di ricerca;
- ❑ altri tipologie di collaborazione con contratto diretto con l'ente;

AFFILIATE:

- ❑ ospiti e visitatori per brevi periodi di tempo;
- ❑ consulenti;
- ❑ fornitori;
- ❑ volontari;
- ❑ membri esterni di organi di governo;
- ❑ revisori ed external auditor;

Infine ePSA non deve essere valorizzato in tutti quei casi che non rientrano nelle definizioni di member, affiliate e alum.
personale cessato che non mantiene un rapporto attivo con l'ente;

- ❑ studenti pre-immatricolati;
- ❑ studenti rinunciatari;
- ❑ studenti decaduti;
- ❑ utenti registrati senza alcuna forma di riconoscimento;

Ringraziamenti CTS 2011-2013 &&&& Grazie per l'attenzione!!!!!!

Gruppo di Lavoro DOPAU 2.0

- Aldo Schiavina,
- Tiziana Podestà
- Paola Laguzzi (coord.)

IDEM Metadata Profile v1.0

- Maria Laura Mantovani

Gruppo di Lavoro Attributi:

- Marina Bianchi,
- Bonaria Biancu,
- Raffaele Conte,
- Paola Laguzzi,
- Maria Laura Mantovani,
- Tiziana Podestà,
- Aldo Schiavina (coordinatore)

Save the Date:

Entro Luglio 2014 => compilare DoPAU 2.0 e idem-metadata profile