Documento descrittivo del processo di accreditamento degli utenti dell'Organizzazione ……..

Le informazioni fornite in questo documento sono accurate alla data del ……

Revisioni

Data	Versione	Descrizione modifica	Autore
03/04/2009	0.1	Bozza	Roberto Gaffuri
29/05/2009	0.2	Bozza	MLM
31/072009	0.3	Rilasciato	MLM
02/12/09	0.4	Corretta la nota introduttiva sulla pubblicità del documento	rc

Nota introduttiva

La partecipazione alla Federazione IDEM ("Federazione") abilita l'organizzazione partecipante ("Partecipante") ad utilizzare la tecnologia ~~di Shibboleth~~ SAML di condivisione degli attributi

La nota introduttiva dovrebbe essere comprensibile per chi (almeno inizialmente) pensavamo dovesse firmarlo? o essere usabile per sensibilizzare qualche decisore dell'organizzazione? Tiziana 27/09/2010

relativi alle identità per gestire l'accesso alle risorse on-line che possono essere rese disponibili all'interno della comunità IDEM. Un obiettivo della Federazione è quello di sviluppare, nel tempo, degli standard per le organizzazioni al fine di assicurare che le asserzioni sugli attributi che vengono scambiate siano sufficientemente robuste e fidate per gestire l'accesso ad importanti risorse protette. Con la crescita della fiducia interna, la Federazione spera che i Partecipanti alla fine possano fidarsi dei sistemi di identity management e dei sistemi di gestione di accesso alle risorse degli altri partecipanti come si fidano dei propri.

Fondamentalmente ci si aspetta dai Partecipanti che essi forniscano agli altri Partecipanti asserzioni sugli attributi autorevoli e accurate e che ciascuno riceva asserzioni sugli attributi protette e nel rispetto dei vincoli di privacy imposti dalla Federazione o dalla fonte delle informazioni. 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.

I due criteri per garantire che gli Identity Provider forniscano asserzioni di attributi fidate sono: (1) che il sistema di gestione delle identità ricada sotto la supervisione degli organismi che hanno responsabilità direttive e gestionali nell'Organizzazione e che (2) il sistema che emette le credenziali per gli utenti finali (e.g., PKI certificates, userids/passwords, Kerberos principals, etc.) sia dotato di appropriate misure di gestione del rischio (e.g., authentication and authorization standards, security practices, risk assessment, change management controls, audit trails, etc.)

Il Documento DOPAU prodotto dal Partecipante DEVE contenere le informazioni elencate nel presente modello.

In caso di modifica delle procedure o informazioni descritte nel documento, esso DEVE essere prontamente aggiornato e ne deve essere data comunicazione alla Federazione.

Abbreviazioni

[Dove vengono descritte le abbreviazioni del documento]

tutto chiaro

Gestore dell’accreditamento

[Dove viene descritto chi è il responsabile (quale area o servizio) del processo di accreditamento degli utenti che afferiscono al proprio Ente. Dove cioè viene detto chi è responsabile dell’assegnazione, del mantenimento e della cancellazione di un’ identità digitale presso il proprio Ente.]

specificare meglio che stiamo chiedendo quale e' la struttura (dipartimento, centro) che e' responsabile del procedimento, non l'ufficio incaricato di effettuare l'operazione di identificazione o consegna le credenziali o creazione *informatica* dell'entry.

Capisco che lo scopo è evidenziare la rilevanza del processo e della relativa responsabilità, ma per comodità sposterei ugualmente il punto nella descrizione del processo di accreditamento della singola categoria o, almeno, dopo il punto successivo.

Tiziana 27/09/2010

Utenti gestiti

[Dove vengono descritte <u>tutte</u> le categorie di utenti gestite dal proprio ente. Specificare a quali categorie viene dato l’accesso ai servizio della Federazione (cioè sono incluse nell’IdP) Specificare anche la cardinalità degli insiemi indicati. Le categorie per un Ateneo potrebbero essere strutturate come segue..]

L'elenco che segue è fuorviante, in quanto diverso da quello riportato in STA.
Se pensiamo che la tabella in STA sia comprensibile e sufficientemente esaustiva inseriamola 2 volte: per chiedere la categoria definita internamente all'Ateneo e per chiedere di indicare la mappatura (oppure la inseriamo una volta sola, se cio' sembra non generare confusione).

Qualcuno può pazientemente spiegarmi con qualche esempio il criterio col quale viene decisa l'affiliazione e il valore che consente l'accesso alle risorse?

Nell'occasione possiamo anche formulare una proposta per recuperare i disallineamenti rilevati nei DOPAU.

Tiziana 27/09/2010

Quasi nessun DOPAU contiene il dato sulla cardinalità.
Si potrebbe provare ad elencare una serie di fasce numeriche fra cui scegliere e specificare che va fatto riferimento agli utenti attivi (ovvero non disabilitati)

Tiziana 27/09/2010

Staff

[Personale docente
Ricercatori
Personale tecnico/amministrativo a tempo indeterminato/determinato
Collaboratori tecnico/amministrativi
Collaboratori membri di commissioni

Collaboratori alla didattica
Collaboratori alla ricerca
Assegnisti di ricerca
Docenti a contratto
Interinali...]

Student

[Studenti iscritti ad un qualunque corso di studi di primo e secondo livello
Dottorandi
Master
Scuole di specializzazione...]

Alumn~~n~~

[Laureati di un qualunque corso di studi/ dottorato/ master]

Affiliate

[Visitatori
Operatori di Aziende
Paganti servizi bibliotecari
Convegnisti
Partecipanti a progetti di ricerca…]

B2B / Servizi

[Utenti associati a servizi. Possono essere credenziali o certificati digitali]

Mappatura degli utenti sulle affiliazioni IDEM

[Dove si descrive come i propri utenti vengono mappati sulle affiliazioni definite in IDEM]

Visione di insieme del processo di accreditamento degli utenti

[Dove si descrive (possibilmente con un diagramma) l'architettura complessiva di provisioning degli utenti: dalle applicazioni che alimentano i DB fino alla loro propagazione nei Directories Service. Vanno descritti inoltre i punti in cui l'utente utilizza le credenziali ottenute]

In questo momento non capisco/non ricordo cose significa *punti in cui l'utente utilizza le credenziali ottenute* Tiziana 27/09/2010

Il processo di accreditamento per la categoria di utenti X

[Dove si descrive in dettaglio il processo di accreditamento per una certa categoria. Questo capitolo è iterato per tutte le categorie significative. Il processo è ben descritto dai seguenti paragrafi…]

Anzichè scrivere di descrivere il processo *per tutte le categorie significative* potremmo scrivere *per tutte le categorie a cui viene dato accesso ai servizi via IDEM* .. e specificare che il DOPAU dovrà essere integrato per poter dare accesso a ulteriori categorie.

Tiziana 27/09/2010

Il processo

[Dove si rappresenta il processo in modo sintetico con gli attori coinvolti- Ideale usare un Activity Diagram UML]

Modalità di riconoscimento della persona

[Dove si dice come avviene il riconoscimento della persona, cioè il processo amministrativo per attribuire una identità digitale che fa sì che per quella certa persona venga creato un record nel database delle identità digitali. Identificare gli uffici preposti (ad es. Segreteria studenti, Risorse Umane, Desk delle biblioteche, ecc…).
]

Caratteristiche dell'identità digitale

[Dove si dice quali caratteristiche (attributi) vengono associate all'identità digitale che viene creata (ad es. nome, cognome, codice fiscale, matricola, emial, telefono, unità organizzativa di afferenza, ecc…]

[Quali delle caratteristiche/attributi possono essere considerati pubblici e vengono forniti a chiunque ne faccia richiesta?]

La compilazione di questo punto è raramente significativa.

A noi cosa interessa? far riflettere chi compila il DOPAU? conoscere l'orientamento dell'organizzazione in merito al trasferimento di dati personali?

Ci interessa conoscere i criteri per il rilascio degli attributi via IDEM?

Tiziana 27/09/2010

Gestione del ciclo di vita

[Dove si dice come viene mantenuta aggiornata la situazione della persona nel database delle identità digitali in concomitanza di cambiamenti (es: cambio struttura, cambio corso, cambio ruolo, uscita, ...]

Formato e regole delle credenziali

[Dove si descrive la tipologia delle credenziali utilizzate nell'organizzazione credentials (e.g., Kerberos, userID/password, PKI, ...) il loro formato, la loro durata, ecc
Se viene usato più di un tipo di credenziali elettroniche come si può determinare chi ha ricevuto quali?

Perchè chiediamo *chi ha ricevuto quali*? Tiziana 27/09/2010

Che politiche ci sono per il~~i~~ rilascio e la gestione di credenziali di tipologie diverse alla stessa persona?

Eventuale presenza di credenziali multiple per la stessa persona

[Dove si descrive se e perché vengono rilasciate credenziali diverse della stessa tipologia per la stessa persona]

Tutti rispondono di no: possibile? Si potrebbero inserire 1-2 esempi. Tiziana 27/09/2010

Modalità di consegna delle credenziali

[Dove si descrive come avviene la consegna delle credenziali]

Modalità di recupero delle credenziali smarrite

[Dove si descrive come avviene la riconsegna della password se dimenticata]

Modalità di gestione smarrimento smartcard/token

[Dove si descrive come avviene la gestione dell'eventuale smarrimento di una smartcard se utilizzata]

Durata dell'accreditamento

[Dove si descrive la durata dell'accreditamento per la categoria in esame]

Disabilitazione utente

[Dove si descrivono le modalità di disabilitazione - sincrone o asincrone con la scadenza dei contratti – degli utenti e dove si descrivono gli effetti delle disabilitazioni]

Cancellazione definitiva utente

[Quando e come avviene la cancellazione definitiva di un utente]

Rischi specifici associati alla categoria di utenti

[Dove si descrivono i rischi e i problemi associati a questa categoria e le misure in fase di attuazione per superare le criticità]

La risposta tipica è "nessun rischio"
Perchè chi compila teme che il DOPAU non prenda la sufficienza o perchè le criticità sono troppe ?
Potremmo sostituire la parola *criticità* a *rischi* e fare 1-2 esempi?

Tiziana 27/09/2010

La richiesta di informazioni sulle misure adottate per informare e sensibilizzare l'utente potrebbe essere inserita a questo punto.
A riguardo segnalo il DOPAU di unipv
http://aai.caspur.it/GARR-AAI-fed/index.php/Image:DOPAU-UNIPV.pdf
(pag.8 e pag. 15) : cosa ve ne sembra?

Tiziana 27/09/2010

Interoperabilità tra credenziali deboli (username+pwd) ed eventuali credenziali forti (smartcard)

[Dove si descrive come interoperano eventuali credenziali forti e deboli associate alla persona]

Il sistema di autenticazione e autorizzazione interno

[Per quali applicazioni interne all'organizzazione viene utilizzato questo sistema di gestione delle identità?]

[Gli identificatori principali di ogni persona, come "net ID," eduPersonPrincipalName, o eduPersonTargetedID, sono univoci una volta assegnati? Possono venire riutilizzati? In quali casi?]

[Se nell'organizzazione è fornito il "single sign-on" (SSO) o la possibilità di avere un sistema unico di autenticazione per più applicazioni e l'organizzazione vuole utilizzare questo sistema per autenticare l'accesso ai servizi della Federazione, si descrivano gli aspetti chiave della sicurezza di questo sistema includendo la descrizione dei timeout imposti dal sistema e della terminazione delle sessioni.]

Io chiederei solo se hanno un sistema di SSO e se intendono utilizzarlo per autenticare l'accesso ai servizi della Federazione lasciando i dettagli tecnici all'interazione col servizio IDEM GARR AAI.
Se i dati sono rilevanti penso sia preferibile inserire qualche raccomandazione in ST.

Tiziana 27/09/2010

Partecipazione ad altre federazioni

[L'organizzazione partecipa ad altre Federazioni di Autenticazione e Autorizzazione? Se sì, quali? Descrivere gli elementi che possono essere di interesse per gli altri partecipanti ed eventuali problematiche.]

Inserire 1-2 esempi Tiziana 27/09/2010