Documento descrittivo del processo di accreditamento degli utenti dell'Organizzazione CINECA

Le informazioni fornite in questo documento sono accurate alla data del 17/02/2011

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 di condivisione degli attributi 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]

Gestore dell'accreditamento

Il processo di accreditamento degli utenti CINECA viene svolto dall'Ufficio del Personale. Tale ente è responsabile dell'assegnazione, del mantenimento e della cancellazione delle identità digitali.

Utenti gestiti

L'identity provider con cui si intende aderire a IDEM è già in uso al CINECA la pressoché totalità dei servizi interni. Volendo garantire tali servizi a tutto il personale la scelta che si è fatta è quella di censirlo sempre e comunque nelle anagrafiche centralizzate. Per questa ragione a tutte le categorie di seguito elencate viene dato l'accesso al servizio della Federazione. Il valore indicato tra parentesi quadre fornisce una stima sulla cardinalità di ciascuna categoria.

Staff

- Dipendenti CINECA [400]
- Collaboratori a progetto [100]
- Partecipanti a stage [20]
- Titolari di una borsa di studio [20]

Affiliate

- Consulenti esterni che partecipino con continuità a progetti CINECA [30]
- Partecipanti a progetti di ricerca [10]

B2B/Servizi

- Clienti [50]
- Fornitori [50]

Mappatura degli utenti sulle affiliazioni IDEM

L'attributo di affiliazione può assumere solo questi valori:

- "**staff**": tutto il personale in servizio presso CINECA con contratto a tempo indeterminato o determinato;
- "**member**": personale CINECA con qualunque altro tipo di contratto, anche a tempo determinato, oppure rientrante nei contratti cosiddetti atipici (co.co.co, prestazioni professionali, interinali, ecc...);
- "**affiliate**": tutti gli altri. Si applica alle persone con le quali CINECA ha una qualsiasi forma di rapporto ed alle quali è necessario attribuire una identità di utente, ma alle quali non vengono estesi i privilegi derivanti dall'essere membri di "staff" (ad esempio consulenti, clienti o fornitori).

Visione di insieme del processo di accreditamento degli utenti

L'abilitazione a qualunque servizio dipende dal preventivo censimento in anagrafica del titolare del servizio stesso. Come abbiamo già detto, dell'inserimento in anagrafica è unico responsabile l'ufficio del personale.
L'applicativo di cui CINECA si serve per gestire le anagrafiche è "U-GOV".
Una volta inserito in anagrafica, un'altra applicazione consente di definire l'associazione tra persone e servizi attraverso la creazione di username di servizio. Questa funzione viene messa a disposizione dei responsabili di settore, dei coordinatori oppure direttamente dei responsabili del servizio. Il processo di abilitazione prevede che si specifichi un intervallo temporale di validità. Se questo non viene specificato e se il servizio non è catalogato come "critico", l'intervallo temporale viene derivato dal record del titolare: se questo è un dipendente a tempo indeterminato, la data di scadenza viene comunque impostata al 02/02/2222; se si tratta di un dipendente a tempo determinato o un collaboratore a progetto, la data di scadenza dell'abilitazione coincide con quella di scadenza del contratto; se si tratta di personale esterno (consulente, cliente o fornitore), la data specificata non può essere maggiore di un anno.
Se la collaborazione termina anzitempo, le procedure interne comunque prevedono (e impongono) di modificare il record relativo a quell'identità indicando la data in cui cessa la collaborazione. La rimozione delle associazioni (persona,servizio) è a carico di una procedura che quotidianamente analizza le abilitazioni alla ricerca di quelle relative ad "anagrafiche scadute".
Per tutte le richieste di abilitazione (e rimozione di abilitazioni) è definito un workflow. In base al servizio alcuni workflow prevedono, oltre al responsabile dell'approvazione tecnica necessaria all'evasione della richiesta, anche un responsabile della approvazione della richiesta (ad esempio l'abilitazione a un servizio che preveda la gestione di dati personali e/o sensibili).
Pur essendo contemplato il caso in cui le credenziali di accesso differiscano da un servizio all'altro, la maggior parte dei servizi è configurata per servirsi delle stesse credenziali forniti dall'utente nell'autenticazione da parte dell'IdP ("single password").
Attualmente la stessa coppia (username,password) consente agli utenti abilitati di accedere ai servizi web (U-GOV, trouble-ticket-system, intranet eccetera) e alla casella di posta e a servizi di connettività RADIUS (VPN e WiFi).
Sulla password principale insiste una policy che ne prevede e impone la modifica almeno ogni sei mesi.

Il processo di accreditamento

Il processo di accreditamento è il medesimo per ciascuna categoria di anagrafiche.

Il processo

Come abbiamo detto, i membri dell'ufficio del personale sono gli unici autorizzati a modificare i dati in anagrafica.

Modalità di riconoscimento della persona

Che si tratti di un dipendente, collaboratore, consulente, cliente o fornitore, questo è invitato a recarsi fisicamente nell'ufficio del personale. Lo staff preposto al censimento fa richiesta di un documento di identità, effettua il confronto dei tratti somatici della persona con quelli della foto nel documento, ne verifica la validità e infine se ne serve per inserire in U-GOV tutti i dati obbligatori.

Caratteristiche dell'identità digitale

Sia di un membro di "staff", "member" o "affiliate" vengono conservati:

- numero di matricola: un identificativo univoco che, nel caso di un dipendente, fornisce un riferimento al contratto;
- nome;
- cognome;
- data di nascita;
- luogo di nascita;
- codice fiscale;
- ente di appartenenza;
- indirizzo email (nel dominio "cineca.it" solo se appartenente ai gruppi "staff" o "member")

Dei dipendenti vengono inoltre conservati, oltre ai dati di residenza e a quelli legati al contratto (ivi comprese le coordinate bancarie per l'accredito dello stipendio), vengono anche conservate informazioni che descrivono il ciclo di vita all'interno dell'azienda:

- dipartimento di appartenenza
- ruolo
- responsabile

L'indirizzo email è generalmente utilizzato come username di accesso ai servizi e può essere esposto in servizi della federazione. Nessuno degli attributi conservati può comunque essere considerato di pubblico dominio.

Gestione del ciclo di vita

I dati relativi all'identità digitale possono essere suddivisi in due categorie:

- quelli relativi alla posizione nei confronti dell'azienda, e della cui modifica è responsabile l'ufficio del personale
- residenza, recapiti telefonici e coordinate bancarie, della cui modifica ed esattezza è responsabile il dipendente.

Della gestione del ciclo di vita di un'identità (variazione della posizione contrattuale, risoluzione di un contratto, passaggio ad altro dipartimento o ad altro responsabile/coordinatore) è quindi responsabile l'ufficio del personale.
In occasione del cambio della categoria dell'utente viene verificato il mantenimento o meno della titolarità all'accesso a determinati servizi.

Formato e regole delle credenziali

Sebbene CINECA si serva di certificati digitali personali per l'autenticazione e l'accesso a taluni servizi, la stragrande maggioranza delle applicazioni si servono di coppie (username,password).
Le funzioni di hash della password supportati da sistemi, applicazioni web e servizi sono '{SHA}', '{CRYPT}' e '{MD5}' così come sono intesi dall'utility "slappasswd".
Per abilitare un nuovo accesso a un servizio (o a un sistema, sia esso ICT o HPC) è necessario compilare un form web. A seconda del servizio, la richiesta segue un workflow che precede l'attivazione vera e propria sul sistema.

I servizi web, l'accesso alla casella di posta e la connettività sono legati dalla "single password". Per altri servizi, come ad esempio l'accesso a sistemi ICT o HPC, la password (non banale) viene generata dallo staff preposto al provisioning e comunicato direttamente all'utente (a voce o, se noto/identificabile da parte dell'operatore, al telefono). L'account viene creato in modo che la password scada al primo login, obbligando quindi l'utente a impostarne una nuova durante il primo accesso.

Eventuale presenza di credenziali multiple per la stessa persona

Ad ogni dipendente CINECA è associata una casella di posta con dominio "cineca.it". Ai responsabili dei servizi o di unità organizzative o di gruppi di lavoro possono essere associate anche caselle di servizio (e.g. "almalaurea@cineca.it" o "ugov-info@cineca.it"). In casi come questi, il titolare viene considerato responsabile della conservazione sicura delle credenziali.

Modalità di consegna delle credenziali

La "single password" iniziale viene comunicata a voce. In fase di registrazione di un nuovo utente, a questi viene anche comunicato l'algoritmo per l'assegnazione di nuova password in caso di reset.

Modalità di recupero delle credenziali smarrite

Tutte le richieste di reset della password (a causa della sua compromissione o del suo smarrimento) passano per l'ufficio del personale.

Modalità di gestione smarrimento smartcard/token

Non sono attualmente utilizzate smart-card o altri dispositivi fisici di conservazione di credenziali di accesso.

Durata dell'accreditamento

La "single password" ha una validità massima di sei mesi e tutti i servizi web che se ne servono trattano opportunamente il caso di password scaduta redirigendo l'utente verso la funzione di cambio password e comunque negando l'accesso al servizio.
Per altri servizi il periodo di validità viene specificato in occasione dell'inserimento oppure viene derivato dalla data di validità del contratto.
L'abilitazione a servizi per utenti di tipo "affiliate" segue le politiche del servizio e non eccede in ogni caso il periodo di un anno.

Disabilitazione utente

Quando un contratto giunge a termine o comunque viene risolto, una procedura in carico all'ufficio del personale impone la rimozione di tutte le abilitazioni ai servizi web e la comunicazione di cessata validità agli staff responsabili di provisioning e de-provisioning per i restanti servizi. Ognuna di queste richieste di disabilitazione genera un ticket col quale tracciare l'espletamento di tutte le attività previste.
Per conservarne lo storico, così come non vengono rimossi gli utenti, non vengono rimosse neanche le abilitazioni: viene modificata la loro data di validità.

Cancellazione definitiva utente

Salvo esplicite richieste di utenti volte a tutelare la propria privacy, U-GOV, il programma gestionale preposto al trattamento delle identità digitali, non prevede la rimozione definitiva di un utente e, così facendo, ne gestisce lo storico.

Rischi specifici associati alla categoria di utenti

Allo scopo di minimizzare i rischi relativi all'utilizzo improprio delle credenziali di accesso o dei servizi accessibili da ciascuna categoria di utenti, sono state implementate le seguenti misure:

- tutte le categorie di utenti vengono censite dall'ufficio del personale con i medesimi criteri (identificazione personale)
- I regolamenti interni prescrivono quali servizi sono accessibili a quali categorie di utenti, e sono resi noti agli utenti stessi e ai responsabili delle autorizzazioni di accesso
- è sempre implementato un workflow di autorizzazione per l'accesso ai servizi, che verifica l'ammissibilità al servizio da parte della categoria a cui appartiene l'utente
- vengono gestiti i cambi di categoria dell'utente, applicando le regole relative

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

Attualmente in CINECA non si fa uso di credenziali forti o dispositivi fisici di autenticazione e/o autorizzazione.

Il sistema di autenticazione e autorizzazione interno

E' in fase di completamento il progetto "LDAP-confluence", volto alla razionalizzazione e centralizzazione dell'Identity Management CINECA. Obiettivo del progetto è quello di demandare completamente a U-GOV la gestione delle identità digitali e, per le applicazioni web, demandare all'Identity Provider -oggetto di questo documento e legato a quella banca dati- i processi di autenticazione e autorizzazione.
A breve tutte le applicazioni web rivolte a personale CINECA o affiliati saranno protette dal medesimo Identity Provider.

Molte delle applicazioni di interesse richiedono e consumano l'informazione relativa all'indirizzo email. Il campo "eduPersonPrincipalName" viene valorizzato con quella informazione e non viene ri-assegnato a persone fisiche diverse: al più viene ri-assegnato alla stessa persona nel caso la sua collaborazione con CINECA cessi e, in seguito, ri-inizi.

Per valorizzare il campo "eduPersonTargetedID" ci si serve di un connettore di tipo "StoredId" e del campo "eduPersonPrincipalName" (quindi statico) come attributo sorgente. Conservando su database relazionale l'identificativo si ha garanzia di valori univoci non riassegnati.

Su Identity e Service Provider sono configurati tempi di durata della sessione e tempo in idle distinti (rispettivamente due ore e trenta minuti). Sebbene per i servizi rivolti a personale CINECA sia previsto un surrogato di "Single Log Out" (definizione di una catena per la rimozione di cookie e dati di sessione da tutte le applicazioni federate e -anello finale della catena- rimozione di cookie e dati di sessione sull'IdP), al termine del logout l'utente viene comunque invitato a chiudere il browser.

Partecipazione ad altre federazioni

CINECA è di recente divenuto membro di "EduRoam". CINECA non partecipa al momento ad altre federazioni di autenticazione e autorizzazione.