Identity Provider Registration Request

v1.0, 2009/07/30[1]

[X] New [ ] Change Request [ ] Removal

Organization

Name: Consiglio Nazionale delle Ricerche (CNR)

Unit name[2]: Istituto di Linguistica Computazionale "Antonio Zampolli" (ILC)

Name in DNS notation: ilc.cnr.it

Display Name[3]: CNR - ILC

Organization URL: http://www.cnr.it, http://www.ilc.cnr.it

Service URL[4]: http://www.ilc.cnr.it/viewpage.php/sez=servizi/id=116/vers=ita

Privacy Policy URL:

Metadata

EntityID: https://idem-idp.ilc.cnr.it/idp/shibboleth

CN of the Certificate: idem-idp.ilc.cnr.it

Other data

URL DOPAU:

Technical data

Operating system[5]: Linux Ubuntu 8.04.3 LTS

IdP software[6]: Shibboleth 2.1.2

Servlet Container[7]: Tomcat 5.5

Backend DB[8]: OpenLDAP/MySQL

1 Please fill in the form in Italian or in English.
It is required that the organization has previously joined the federation as a member or as a partner.
2 If applicable
3 To be displayed on WAYF server IdPs list. Could be modified by IDEM GARR AAI Service for normalization.
4 The URL of a page which describes the service, as required by "Norme di Partecipazione".
5 type/version
6 type/version
7 (if applicable) type/version
8 (e.g.LDAP/Oracle/...), type/version (if applicable)

Other information: .....

Technical contacts[9]

Name: Dr. Alessandro Enea

Position: Responsabile sistemi informativi

Address: Via G. Moruzzi, 1 - 56124 Pisa

Email: Alessandro.Enea@ilc.cnr.it

Phone: +390503152842

Support Email[10]: idem@ilc.cnr.it

The service is in compliance with the purpose of the federation.

Date: .....

Signature on behalf of the Organization[11] IL DIRIGENTE (Ing. Mario TOZZOLI) .....

9 At least one is required. If you have more Contacts copy and paste the following form section many times as needed.

10 Email address operating also during the absence of the technical contact.

11 Signature of the administrative contact person of the federation member/partner (In case of a "change request" to technical data, signature of the technical contact person is sufficient).

Procedura di accreditamento degli utenti

Istituto di Linguistica Computazionale "Antonio Zampolli"
ILC-CNR

A cura di Alessandro Enea, Riccardo Del Gratta
Servizi Informativi - ILC-CNR

1. Revisioni

Rev.	Data	Autore
1	05/03/2010	A. Enea, R. Del Gratta

Introduzione

L'Istituto di Linguistica Computazionale "Antonio Zampolli" ha da tempo un sistema di accreditamento e gestione degli utenti a cui si appoggiano i vari servizi dell'istituto. Attualmente è in corso una revisione e riprogettazione delle procedure di accreditamento e gestione degli utenti.
Il presente documento descrive le procedure attualmente in atto per la gestione degli utenti e la loro autorizzazione all'uso dei servizi informatici dell'istituto.

1. Descrizione del sistema

Il sistema di gestione degli utenti e delle identità digitali si compone di due macchine utilizzate per ospitare un server con LDAP master e una replica. Tutti gli inserimenti e modifiche sono fatte su LDAP. Inoltre è presente un server sul quale è implementato un Identity Provider usando il software Shibboleth.
L'IDP è utilizzato per l'autenticazione Single Sign-On per l'accesso ai servizi messi a disposizione dalla Federazione IDEM.

2. Procedure e responsabilità dell'accreditamento utenti

L'accreditamento degli utenti viene effettuato dai gestori dei Servizi Informatici dello ILC. L'Ufficio Personale dell'ILC inoltra ai gestori dei Servizi Informatici le informazioni sul personale afferente, nelle diverse forme, all'ILC. Un account viene rilasciato solo a chi ha un rapporto di lavoro contrattuale con l'istituto (tempo indeterminato, tempo determinato, collaboratori scientifici, assegnisti di ricerca, contratto interinale e contratto d'opera). Non sono rilasciati account a studenti che svolgono attività di tesi o stage e visitatori.
I gestori dei Servizi Informatici inseriscono i dati relativi all'identità e all'account tramite una interfaccia web nel server LDAP. Per tutti i tipi di rapporto a tempo determinato viene inserita una data di scadenza.
Il meccanismo di autenticazione utilizzato si basa su username password. I nostri userid hanno il formato di <nome.cognome>. Inizialmente viene assegnata una password temporanea che l'utente può cambiare tramite una interfaccia web.

2.1 Utenti a tempo indeterminato

La procedura sopra descritta si applica a tutti gli utenti a tempo indeterminato per i quali non è prevista nessuna scadenza relativa all'account.

2.2 Utenti con rapporto di lavoro a scadenza

La procedura sopra descritta si applica anche a tutti gli utenti con rapporto di lavoro a tempo determinato. La validità dell'account ha una durata uguale a quella del contratto di lavoro che può essere rinnovabile senza limiti purché subordinatamente al rinnovo del contratto o di altro rapporto formale con l'Istituto.

2.3 Studenti e visitatori

Per gli studenti (tirocinanti, tesisti, dottorandi, specializzandi) e visitatori non sono rilasciati account.

3. Proroga scadenza account

Il rinnovo degli account con scadenza avviene semplicemente con una richiesta all'Ufficio del Personale. Sarà cura di quest'ultimo verificare che il richiedente ne abbia diritto in funzione della validità del proprio rapporto con ILC. In caso positivo viene inviata comunicazione in forma di posta elettronica sia al richiedente che ai gestori dei Servizi Informatici per la necessaria proroga.

4. Disabilitazione account

La disabilitazione di un account può avvenire o direttamente per iniziativa dei gestori dei Servizi Informatici nel momento in cui il rapporto con ILC viene a cessare, o su richiesta dello stesso utente o di altro utente che ne abbia diritto (es. responsabile del contratto dell'utente, responsabile di un servizio, ecc.).
La disabilitazione dell'account, avviene anche automaticamente alla scadenza del contratto.
L'operazione non rimuove effettivamente i dati relativi all'account ma lo sposta su un opportuno ramo della gerarchia LDAP in modo da conservare lo storico nel server LDAP.

5. Password

La password temporanea assegnata inizialmente (par. 2) dovrà essere cambiata dall'utente.
La password non ha scadenza. Il sistema registra la data dell'ultimo aggiornamento della stessa ed è quindi compito dell'applicazione che richiede l'autenticazione e necessita che sia prevista la scadenza delle password, verificare che l'intervallo di tempo dall'ultima modifica sia non superiore al periodo previsto per legge (D. L. 196/03, tre mesi per dati personali, sei mesi per dati sensibili) e impedire l'accesso notificando il motivo all'utente. L'utente può modificare la propria password tramite interfaccia web.

6. Tipologia di utenza

La posizione contrattuale nei confronti dell'ILC è registrata nell'attributo LDAP "EmployeeType" dell'ObjectClass "inetOrgPerson".
L'affiliazione, definita con l'attributo "primaryAffiliation" dell'ObjectClass "inetOrgPerson" richiesta da IDEM, non è salvata all'interno del database LDAP ma viene comunicata alla controparte (tramite un "mapping" dinamico eseguito da Shibboleth) rispettando le corrispondenze dei valori definiti nel documento "Specifiche tecniche per la compilazione e l'uso degli attributi" della Federazione IDEM.

7. Il sistema di autenticazione e autorizzazione interno

I servizi interni dell'istituto utilizzano le credenziali descritte in questo documento per l'autenticazione e autorizzazione. Al momento non abbiamo servizi interni che usano meccanismi di web SSO.

8. Partecipazione ad altre federazioni

L'istituto partecipa alla federazione eduroam per l'accesso alle reti wifi di enti di ricerca e accademici.