Consiglio Nazionale delle Ricerche
ISTITUTO DI STUDI SUI SISTEMI INTELLIGENTI PER L'AUTOMAZIONE
Via G. Amendola 122/D-I – 70126 Bari (Italy)
Tel. +39-080-5929429 Fax. +39-080-5929460

Processo Accreditamento Utenti

Area di Ricerca di Bari

Massimo Ianigro

CNR ISSIA

revisione 1.2 – 04 gennaio 2010

Introduzione

Questo documento descrive le procedure di accreditamento degli utenti dei servizi informatici erogati dall'Area di Ricerca di Bari agli Organi ad essa direttamente o indirettamente afferenti.
Nel seguito verranno indicati i criteri utilizzati per la gestione dell'utenza, le procedure seguite per l'accreditamento e la gestione delle identità digitali e l'organizzazione generale del servizio.
I servizi informatici gestiti dall'Area di Ricerca di Bari vengono erogati a favore degli utenti degli Istituti e delle Unità Organizzative di Supporto ubicati in Bari o in altre città del territorio italiano a fronte di specifiche richieste di accesso a tali servizi quali, ad esempio, Unità Organizzative di Supporto afferenti a Istituti che hanno a Bari la loro sede principale.
La lista aggiornata di tali strutture è reperibile all'indirizzo www.ba.cnr.it (Organi afferenti) e per ogni struttura è prevista la figura di un referente informatico locale che è coinvolto nelle procedure di gestione della utenza, descritte successivamente, e la responsabilità della conduzione di tali servizi afferisce al CNR ISSIA.

Sistema centralizzato di autenticazione

I servizi erogati dall'Area di Ricerca si avvalgono di un sistema unico di autenticazione, al quale accedono le varie componenti di validazione degli utenti (es. radius per le infrastrutture di rete, PAM per i processi di login, pagine web ad accesso ristretto, webmail, etc) .
Tale infrastruttura di autenticazione è inoltre disponibile, con le dovute restrizioni, anche ai singoli Istituti/Strutture, ai quali viene consentito l'accesso al proprio ramo dell'albero LDAP generale, al fine di poter riutilizzare tali credenziali anche sui sistemi afferenti alle proprie reti.
Inoltre il sistema è interfacciato a un Identity Provider per consentire l'autenticazione federata e non è previsto il riutilizzo di identificatori precedentemente assegnati ad altra utenza.

Procedura di accreditamento del personale

L'accesso ai servizi informatici (posta elettronica, web, biblioteche on-line, etc) prevede l'assegnazione per ogni utente di un identificativo univoco e personale.
E' consentito l'accesso a tali servizi sia al personale con rapporti di lavoro diretto, che alle figure cosiddette 'atipiche' quali, ad esempio, tesisti, assegnisti di ricerca, contratti d'opera, fornitori di servizi, partecipanti a progetti di ricerca.
La qualificazione degli aventi diritto avviene all'interno delle strutture alle quali essi afferiranno e viene operata tipicamente dagli uffici amministrativi che si occupano in prima analisi della verifica dei requisiti (ad esempio: sottoscrizione del contratto di assegno di ricerca, attestazione universitaria per i laureandi, etc) e provvedono alla consegna delle varie informative di prassi (sicurezza dei luoghi di lavoro, acceptable use policy, etc).
Successivamente il personale interagisce con il referente informatico locale che valutate le esigenze della persona interessata, procede alla richiesta di assegnazione di credenziali.
Tali credenziali vengono richieste mediante la compilazione di una pagina web protetta da procollo di cifratura https/ssl che racchiude gli elementi significativi dell'account e in particolare Nome,

Cognome, Struttura di afferenza, Indirizzo di posta elettronica da assegnare, oltre ad eventuali note riguardo la scadenza dell'account o altre informazioni addizionali.

La richiesta così formata viene inoltrata perviene alla gestione dei servizi informatici di Area e se non vengono ravvisati elementi ostativi quali ad esempio una richiesta duplicata, si procede alla generazione delle credenziali e alla predisposizione dei servizi richiesti.

La password assegnata inizialmente viene generata in maniera pseudocasuale e soggetta a scadenza ravvicinata (tipicamente 10 giorni); Il referente e l'utente vengono informati mediante email della necessità di procedere in tempi rapidi al cambio di password.

Il login dell'utente viene generato utilizzando uno schema del tipo IIIINCXX, dove IIII è la sigla che identifica l'Istituto di afferenza, NC rappresentano tipicamente le iniziali del nome e del cognome e XX è una parte alfanumerica variabile. La definizione dell'indirizzo di posta elettronica associato avviene invece in funzione dello schema adottato dall'Istituto, tipicamente nella forma nome.cognome@dominio, cognome@dominio oppure no.cognome@dominio .

L'attributo qualificante l'utente (Member/Staff/...) viene definito in funzione della tipologia di utente indicato dal referente all'atto della richiesta e può essere soggetto a revisione nel tempo, in funzione delle variazioni del rapporto con il CNR (es. assunzione).

Tutta la documentazione cartacea relativa all'utente, viene gestita dalle amministrazioni dei vari Organi e da essi viene custodita.

Non è consentita l'assegnazione di credenziali multiple alla stessa persona e non è prevista la custodia delle password che sono memorizzate con sistemi di codifica unidirezionali non invertibili (hashing MD5/SHA-1).

La consegna delle credenziali avviene mediante il referente locale.

Procedura di disattivazione degli utenti

La disattivazione delle utenze può avvenire in maniera automatica o su richiesta del referente. La disattivazione automatica è conseguenza della scadenza della password, la cui validità è al momento fissata in 180 giorni. Con l'approssimarsi della scadenza, l'utente viene informato via email della

necessità di procedere al cambio password e copia di queste notifiche perviene anche al referente informatico.

Il mancato cambio della password provoca il blocco dell'account e conseguentemente la cessazione dei servizi.

In alternativa, il referente può richiedere esplicitamente una disattivazione accedendo a una interfaccia web che gli consente di selezionare gli utenti afferenti alla propria struttura, nel momento in cui dovesse ravvisare che un utente non ha più i requisiti per usufruire dei servizi.

Tale richiesta viene successivamente inoltrata alla gestione dei servizi informatici di Area ed eseguita.

Prima della rimozione delle credenziali, viene effettuato un backup di tutti i dati, incluso il profilo di autenticazione e il contenuto delle sue aree di lavoro sui server di Area e viene custodito dai servizi di Area.

Gestione password

Nel caso un utente ravvisi la possibilità di un furto delle proprie credenziali di accesso, o nel caso in cui la password possa essere scaduta, i referenti hanno a disposizione una interfaccia web che consente la riassegnazione di una password temporanea con validità temporale ridotta, e conseguentemente lo sblocco dell'account.

L'operazione di generazione di una nuova password viene notificata sia ai responsabili della gestione dei servizi di Area che all'utente stesso.

Partecipazione ad altre Federazioni

L'Area di Ricerca del CNR di Bari non partecipa ad altre Federazioni.