Documento descrittivo del processo di accreditamento degli utenti dell'Organizzazione Consortium GARR

Le informazioni fornite in questo documento sono accurate alla data del 19/04/2010

Abbreviazioni

UP Ufficio del Personale
RS Reparto Sistemistico
ID Identità Digitale

Gestore dell'accreditamento

Direzione: autorizza la creazione dell'identità digitale, la sua assegnazione ai gruppi e i suoi privilegi.
Ufficio del personale: attiva la procedura di creazione/modifica/disattivazione/cancellazione dell'identità digitale, comunicando al servizio tecnico le operazioni da svolgere; controlla l'esecuzione della procedura e ne accerta il compimento
Servizio tecnico: esegue le operazioni impartite dall'ufficio del personale e ne comunica allo stesso l'avvenuta esecuzione.

Utenti gestiti

Relativamente alla Federazione IDEM possono essere individuate 2 diverse categorie di utenze :
staff (member): dipendenti della direzione e assimilati
affiliate: ospiti, convegnisti, responsabili tecnici punti di accesso rete GARR presso Enti afferenti (Access Port Manager). Questi attualmente non vengono attivati sull'LDAP centralizzato e di conseguenza non sono nemmeno presenti nell'Identity Provider della Federazione IDEM.

Staff	**Affiliate**
Personale tecnico/amministrativo (determinato/indeterminato)	Visitatori
Dirigenti (contratto, ricerca, tecnologo)	Convegnisti
Membri CDA/CTS	Partecipanti seminari/riunioni esterni direzione GARR
Borsisti	APM GARR
Stagisti	APA GARR
Collaboratori coordinati e continuativi/occasionali/interinali	
Dottorandi	
Master	
Laureati di un qualunque corso di studi/ dottorato/ master	
Dipendente altro ente di ricerca	

Mappatura degli utenti sulle affiliazioni IDEM

Staff	***Affiliate***
eduPersonAffiliation: staff, member	eduPersonAffiliation: affiliate
eduPersonScopedAffiliation: $eduPersonAffiliation@garr.it	eduPersonScopedAffiliation: $eduPersonAffiliation@garr.it

Visione di insieme del processo di accreditamento degli utenti

1. UFFICIO del PERSONALE (UP) identifica la persona
2. UP stabilisce se la persona è Staff o Affiliate
3. UP stabilisce l'appartenenza della persona ai gruppi, se la persona rientra in staff
4. UP richiede al Reparto Sistemistico (RS) la creazione/modifica/cancellazione dell'identità digitale (ID)
   - € se staff: sul sistema di autenticazione centralizzato e su tutti gli altri sistemi locali su cui la persona dovrà accedere; richiede l'assegnazione ai gruppi e la creazione dei necessari privilegi.
   - € se affiliate: sul sistema di gestione dell'accesso Wi-Fi (Radius)
5. RS esegue le operazioni richieste
6. RS comunica a UP l'avvenuta la creazione/modifica/cancellazione dell'ID

Il processo di accreditamento per la categoria di utenti Staff

Il processo

Il processo di accreditamento di un nuovo utente appartenente alla categoria staff nel contesto aziendale si articola nelle seguenti fasi:

- riconoscimento dell'identità del nuovo utente e raccolta degli attributi significativi a determinarne univocamente l'identità digitale: si svolge presso UP
- inserimento dell'identità digitale del nuovo utente nel catalogo LDAP centralizzato (sistema di autenticazione centralizzato): a cura della RS
- configurazione delle risorse di accesso per l'utente: a cura del RS
- configurazione dei privilegi di accesso alle risorse (profili di autorizzazione nelle varie applicazioni): a cura degli amministratori delle varie applicazioni

Modalità di riconoscimento della persona

Il processo di accreditamento del nuovo utente staff avviene sempre presso l'UPe la convalida della sua identità è sempre subordinata alla presentazione di documento di identità in corso di validità. Pertanto ogni successivo trattamento dei dati personali del nuovo utente da parte della struttura IT dell'azienda avviene sempre previa comunicazione degli attributi distintivi dell'identità digitale da parte dell'UP.

Caratteristiche dell'identità digitale

Alcuni attributi associati all'identità digitale di un utente della categoria staff sono:

```
dn: cn=Nome Cognome,ou=Voip,ou=Groups,dc=dir,dc=garr,dc=it
objectClass: top
objectClass: person
objectClass: posixAccount
objectClass: shadowAccount
objectClass: inetOrgPerson
objectClass: pkiUser
objectClass: extensibleObject
objectClass: eduPerson
objectClass: schacEmployeeInfo
objectClass: schacUserEntitlements
objectClass: garrPerson
uid: cognome
uidNumber:
gidNumber:
```

eduPersonOrgDN: dc=garr,dc=it
eduPersonOrgUnitDN: dc=dir,dc=garr,dc=it
sn: Cognome
cn: Nome Cognome
eduPersonEntitlement: urn:mace:garr.it:idem:dir:testapp1
eduPersonEntitlement: urn:mace:garr.it:idem:dir:testapp2
givenName: Nome
schacPersonalPosition: -- reserved for future IDEM implem. --
eduPersonAffiliation: member
eduPersonAffiliation: staff
schacPersonalTitle: Dott.
schacMotherTongue: it
facsimileTelephoneNumber:: KzM5IA==
telephoneNumber:: KzM5IA==
mobile:: KzM5IA==
mail: nome.cognome@garr.it
schacUserPresenceID: skype:?
preferredLanguage: it-en

Per configurazione del catalogo LDAP gli attributi di ciascun utente ritenuti sensibili non sono accessibili alle applicazioni in modalità anonima (ovvero senza username e password) ma il binding e conseguente recupero delle credenziali/attributi utente può essere effettuato solo tramite autenticazione lato applicativo con utente privilegiato .

Gli attributi della objectClass inetOrgPerson considerati sensibili e pertanto protetti da ACL (non accessibili da applicazioni con utente anonimo ma solo specificando un utente di servizio per il binding) sono:

userpassword, userpkcs12, usersmimecertificate, userCertificate

Gli attributi relativi a Shibboleth considerati sensibili (non accessibili da applicazioni con utente anonimo ma solo specificando un utente di servizio per il binding) sono:

edupersonorgdn, edupersonorgunitdn, edupersonscopedaffiliation, edupersonaffiliation, edupersontargetedid, edupersonprincipalname, edupersonentitlement

Gestione del ciclo di vita

La gestione del ciclo di vita dell'identità digitale dell'utente appartenente alla categoria staff prevede le seguenti fasi:

- cambio ufficio (corrispondente ad un cambio di mansioni): l'ufficio del personale comunica alla struttura sistemistica ed ai maintainer delle applicazioni interessate dallo spostamento la relativa variazione di ruolo (es. passaggio personale da reparto Segreteria a reparto Amministrazione e Contabilità), in modo che possano essere aggiornate sia le informazioni di autenticazione nel catalogo globale LDAP sia quelle locali alle applicazioni.)
- uscita dell'utente dalla struttura: l'ufficio del personale comunica alla struttura sistemistica ed ai maintainer delle applicazioni interessate la necessità di cancellare(disattivare) l'identità digitale

Formato e regole delle credenziali

userID/password (LDAP SSHA, UNIX MD5). Non vengono imposte regole sulla lunghezza e sulla robustezza della password. La password non scade.

PKI user certificate X509 (per utenti con accesso wireless EduROAM). Il certificato personale scade dopo 1 anno e può essere rinnovato prima della scadenza.

Eventuale presenza di credenziali multiple per la stessa persona

Credenziali diverse per l'utente staff rispetto a quelle centralmente gestite nel catalogo globale LDAP vengono rilasciate solo ed esclusivamente per garantire l'accesso a quelle applicazioni il cui sistema di autenticazione e autorizzazione non è ancora integrato sotto LDAP (vedi paragrafo precedente).

Modalità di consegna delle credenziali

Il reparto sistemistico provvede ad inviare comunicazione via mail all'utente su tutte le credenziali configurate ed i relativi accessi alle distinte applicazioni.

Modalità di recupero delle credenziali smarrite

La procedura di riconsegna password non è prevista.

Qualora l'utente smarrisca o non ricordi la propria potrà accedere all'interfaccia utente di LDAP ed avviare la procedura di recovery come da istruzioni riportate nella casella di testo.

Alcuni attributi sono modificabili dall'utente in autonomia tramite l'interfaccia utente di LDAP dopo il superamento della procedura di autenticazione. Tali attributi sono:

userPassword

telephoneNumber

mobile

facsimileTelephoneNumber

mail

schacUserPresenceID

preferredLanguage

schacMotherTongue

labeledURI

x-garr-RelativePhotoURL

Modalità di gestione smarrimento smartcard/token

Al momento non vengono utilizzate credenziali che permettono strong authentication.

Durata dell'accreditamento

La durata dell'accreditamento dell'utente è definita dall'intervallo temporale fra la comunicazione iniziale effettuata dall'ufficio del personale al reparto sistemistico per l'inserimento del nuovo utente e quella inerente la richiesta di dismissione dell'identità digitale ad esso *associata.*

Disabilitazione utente

Il processo di disabilitazione di un utente si può articolare in 2 fasi:

1. disabilitazione delle credenziali di autenticazione - account sul catalogo globale LDAP (modifica del suo uid)
2. disabilitazione del suo account su tutte le applicazioni della direzione

Cancellazione definitiva utente

Il processo di dismissione di un utente si può articolare in 2 fasi:

1. cancellazione del suo account dal catalogo globale LDAP
2. cancellazione del suo account su tutte le applicazioni della direzione

Rischi specifici associati alla categoria di utenti

L'esistenza di applicazioni non ancora integrate nel sistema centralizzato LDAP pone il problema di gestire il flusso di interventi di rassegnazione di username/password in caso di smarrimento delle credenziali di accesso.
In caso di smarrimento delle credenziali, non essendo queste univocamente determinate in un solo sistema di autenticazione (non solo sul catalogo globale LDAP ma anche dislocate presso le varie applicazioni per quelle non ancora integrate in LDAP) l'utente provvederà a darne immediata comunicazione all'ufficio del personale che dovrà verificare quanto segue:

1. l'utente ha smarrito le credenziali di autenticazione per accedere ad una applicazione già integrata in LDAP: l'ufficio del personale comunica alla struttura sistemistica la necessità di effettuare una dismissione delle vecchie credenziali (username perso) o reset della password (che l'utente potrà fare in autonomia)
2. l'utente ha smarrito le credenziali di accesso ad una applicazione non ancora integrata in LDAP: l'ufficio del personale comunica agli amministratori dell'applicazione la necessità di configurare un nuovo account per l'utente (o un reset della password dell'utente) accordandosi con lo stesso per lo svolgimento di tale attività e notificandone poi la conferma

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

Attualmente gli utenti della categoria staff non utilizzano devices che consentano un livello forte di protezione delle credenziali di accesso (smartcard, security token, key fob).
La possibilità di usare i certificati digitali come metodo di autenticazione/autorizzazione è consentita dalla presenza di tutti gli attributi della objectClass pkiUser (in particolare userCertificate) anche se subordinata alla presenza di un modulo di autenticazione integrato nell'applicazione che ne consenta l'utilizzo.

Il processo di accreditamento per la categoria di utenti Affiliate

Il processo

Il processo di accreditamento di un nuovo utente della categoria affiliate si articola nelle seguenti fasi:

1. registrazione dell'utente presso la segreteria/help desk in occasione di un evento, convalida dell'identità ed assegnazione delle relative credenziali digitali preventivamente create dalla struttura sistemistica/tecnica operativa (wireless guest account di durata pari al tempo di permanenza dell'utente) per l'accesso alle risorse disponibili (rete wireless)
2. controllo della dismissione dell'account da parte della struttura sistemistica/tecnica operativa

Modalità di riconoscimento della persona

Il riconoscimento del nuovo utente avviene a cura del reparto di segreteria/ufficio del personale che dopo aver controllato il documento di identità provvede a fornire all'utente le credenziali digitali per l'accesso alle risorse stabilite per questo tipo di categoria (rete wireless SSID garr).

Caratteristiche dell'identità digitale

Per la categoria di utenti affiliate non è prevista la creazione di un account sul sistema di autenticazione centralizzato LDAP, perché si concede il solo accesso alla risorsa rete wireless. Tutti gli account che verranno creati saranno locali al database sul server RADIUS che controlla l'accesso alla rete wireless.
L'identità digitale che verrà fornita in dotazione ad un nuovo utente della categoria affiliate sarà pertanto costituita da uno username ed una password.. La durata della validità dell'account viene impostata in fase di attivazione.

Gestione del ciclo di vita

Ogni modifica delle applicazioni cui l'utente affiliate potrà accedere dovranno essere comunicate dalla segreteria/ufficio del personale ai relativi amministratori che provvederanno a configurare i relativi account con i permessi di accesso.

Formato e regole delle credenziali

userID/password (MySQL DB su host radius): durata = tempo di permanenza dell'utente nella struttura GARR (es. durata convegno)

Eventuale presenza di credenziali multiple per la stessa persona

Per sua natura un utente della categoria affiliate non può mai essere duplicato (in quanto il sistema di generazione del guest account per la rete wireless è univoco).

Modalità di consegna delle credenziali

La segreteria/ufficio del personale consegna su foglio le credenziali digitali al nuovo utente previa verifica del suo documento di identità.

Modalità di recupero delle credenziali smarrite

Per l'accesso wireless non è prevista una procedura di recovery password.
Pertanto in concomitanza del verificarsi di un evento di smarrimento password l'utente dovrà richiedere la consegna di una nuova identità digitale e la cancellazione della vecchia.

Modalità di gestione smarrimento smartcard/token

Al momento non vengono utilizzate credenziali che permettono strong authentication

Durata dell'accreditamento

La durata dell'accreditamento per un utente della categoria affiliate è pari al suo tempo di permanenza all'interno della struttura GARR (es. durata del convegno).
L'account è di durata temporale limitata, la dismissione dello stesso avviene automaticamente.
Qualora occorra un prolungamento della durata, l'utente provvederà a comunicarlo alla segreteria che a sua volta fornirà (previa creazione da parte della struttura sistemistica/tecnico operativa) un nuovo account della durata richiesta.
Qualora avvengano modifiche del profilo di accesso dell'utente (accesso ad altre applicazioni) la durata di accesso verrà stabilita con l'ufficio del personale in base alle specifiche esigenze.

Disabilitazione utente

La disabilitazione dell'account utente avviene tramite la variazione del campo username nel database locale al RADIUS server per l'autenticazione/accounting degli accessi ala rete wireless.

Cancellazione definitiva utente

La cancellazione di un utente della categoria Affiliate avviene sempre a cura del reparto sistemistico dopo aver ricevuto opportuna comunicazione dalla segreteria.
Si controlla che sia avvenuta con successo la procedura automatica di cancellazione dell'account dal database delle utenze RADIUS ed eventualmente (qualora il profilo dell'utente sia cambiato rispetto a quello di semplice guest per accedere alla rete wireless) dal sistema di autenticazione centralizzato LDAP.

Rischi specifici associati alla categoria di utenti

I rischi connessi con l'utilizzo dell'identità digitale per l'utente della categoria Affiliate risiedono nella possibilità di smarrimento/furto delle credenziali dell'utente per l'accesso alla rete wireless per gli ospiti (SSID garr).
Qualora ciò avvenga l'utente provvederà immediatamente a darne comunicazione alla segreteria in modo da attivare la procedura di cancellazione del profilo utente nel database del server RADIUS da parte del reparto sistemistico.

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

Non applicabile

Il sistema di autenticazione e autorizzazione interno

Considerazioni generali

L'eterogeneità delle applicazioni in uso presso la direzione GARR ha posto sinora il problema della gestione di credenziali multiple per una singola identità .
In tale ottica la centralizzazione del sistema di gestione delle identità su catalogo LDAP si pone come passo imprescindibile per realizzare un sistema di Single Sign On che lo utilizzi come back end (Shibboleth, Kerberos).

Sistema di autenticazione ed autorizzazione interno – situazione attuale

I sistemi di autenticazione utilizzati all'interno della direzione GARR sono attualmente :

- LDAP centralizzato (OpenLDAP 2.4.19) utilizzato per la convalida dell'accesso utente alle seguenti applicazioni:
    1. posta elettronica interna (account @garr.it)
    2. sistema di monitoring dei circuiti delle rete GARR (GINS)
    3. wiki collaborativo
    4. pagine private del NOC
    5. rancid (CVS configurazioni routers e switch rete GARR)
    6. vconf (servizio videoconferenza, previa creazione del corrispondente account sul sistema di autorizzazione interno all'applicazione vconf basato su mysql database)
    7. VPN SSL Juniper (realm ldap-direzione)
    8. sistema elettronico modifica giustificativi/ritardi/permessi (cartellino.dir.garr.it): previa creazione del relativo account nel sistema interno (DB MySQL) effettuata dagli amministratori dell'applicazione di gestione sistema rilevazione presenze

- NIS database (old UNIX file server)
- Windows Active Directory (utilizzato per accesso utente a personal share folder su Windows File Server)

Attualmente il login degli utenti avviene utilizzando il tradizionale sistema username e password, senza l'utilizzo di sistemi di SSO.

Non essendo disponibile alcun meccanismo di Single Sign On, all'utente verrà chiesta l'immissione delle credenziali ogniqualvolta accederà ad una delle applicazioni della direzione.

L'utente staff utilizzerà come login name l'attributo 'uid'del catalogo globale LDAP per tutte quelle applicazioni già integrate.

Per quelle per le quali non è ancora stata realizzata l'integrazione l'utente dovrà utilizzare lo username locale definito nell'applicazione.

È stata stabilita per semplificazione degli accessi utente la convenzione che quest'ultimo sia uguale all'attributo uid configurato su LDAP.

Configurazione dei profili di autorizzazione per le applicazioni della direzione

La configurazione dell'account LDAP garantisce al nuovo utente staff che effettui l'autenticazione l'accesso alle seguenti applicazioni (con profilo di autorizzazione "Guest", ovvero con privilegi minimi fra quelli previsti dal sistema di autorizzazione locale all'applicazione) :

1. posta elettronica interna (previa creazione della mailbox dell'utente e relativa entry record su /etc/mail/userdb sul server di posta interno cyrus.dir.garr.it e del relativo alias nel file /etc/mail/aliases su frontend di posta lx1.dir.garr.it ed lx5.dir.garr.it – a cura del reparto sistemistico)
2. wiki collaborativo (previa registrazione dell'utente sul TWiki effettuata sempre dal reparto sistemistico)
3. monitoring dei circuiti rete GARR (GINS) e relativo profilo di autorizzazione (a cura degli amministratori del reparto di monitoring dei circuiti di rete, se e come stabilito dall'ufficio del personale)
4. pagine private del NOC
5. rancid (CVS configurazioni routers e switch rete GARR)
6. vconf (servizio videoconferenza, previa creazione del corrispondente account sul sistema di autorizzazione interno all'applicazione vconf basato su mysql database)
7. VPN SSL Juniper (realm ldap-direzione)
8. sistema elettronico modifica giustificativi/ritardi/permessi (cartellino.dir.garr.it): previa creazione del relativo account nel sistema interno (DB MySQL) effettuata dagli amministratori dell'applicazione di gestione sistema rilevazione presenze

Sistema di autenticazione ed autorizzazione interno – sviluppi futuri

Considerata l'eterogeneità e la molteplicità di applicazioni in uso presso la direzione la scelta del sistema di Single Sign On e' da considerarsi principalmente subordinata alla verifica dei seguenti requisiti :

- interoperabilità con altri meccanismi di SSO di terze parti
- integrazione con il sistema di gestione centralizzata delle identità degli utenti delle direzione GARR (OpenLDAP)
- conformità a standard non proprietari

- adattabilità alla tipologia di applicazioni in uso presso la direzione
- integrazione con attuale sistema in uso per l'accesso alle applicazioni della federazione IDEM

In tale ottica l'orientamento delle direzione GARR e' quello di utilizzare Shibboleth come sistema di SSO, soprattutto in considerazione di:

- già utilizzato come sistema di autenticazione ed autorizzazione per l'accesso alle applicazioni della federazione IDEM
- interoperabilità di Shibboleth con Kerberos (da utilizzarsi per le applicazioni che non supportano nativamente il protocollo HTTP)
- la maggioranza delle applicazioni in uso presso la direzione prevedono l'accesso alle informazioni tramite protocollo HTTP (web-based applications)

Partecipazione ad altre federazioni

Al momento della scrittura del presente documento non è prevista la partecipazione del Consortium GARR ad altre federazioni ad eccezione di IDEM.