PROT. ARRIVO N. E/10601/10
DEL 19 FEB. 2010
CONSORTIUM GARR

Università degli Studi di Cagliari
Direzione per le Reti ed i Servizi Informatici

Documento descrittivo del processo di accreditamento degli utenti

Gestore dell'accreditamento

Università degli Studi di Cagliari – Direzione per le Reti ed i Servizi Informatici – Settore Reti

Utenti gestiti

Staff

Personale docente
Ricercatori
Personale tecnico ed amministrativo a tempo indeterminato
Personale tecnico ed amministrativo a tempo determinato (*)
Assegnisti di ricerca (*)
Docenti a contratto (*)
Dottorandi (*)

(*) il personale ATA a t.d., gli assegnisti, i docenti a contratto ed i dottorandi hanno account a tempo limitato con possibilità di rinnovo previa autorizzazione dei responsabili delle rispettive strutture.

Student

Al momento la categoria Student non è popolata in quanto gli studenti in regola con le tasse sono allocati su un ramo della LDAP che non ha relazioni alcune con il meccanismo di SSO; è allo studio un progetto per gestire gli studenti attraverso l'integrazione di Esse3 e LDAP che comunque non vede coinvolto il meccanismo di SSO.

Alumn

Al momento la categoria Student non è popolata né si pensa possa esserlo, almeno a

Università degli Studi di Cagliari
Direzione per le Reti ed i Servizi Informatici

Documento descrittivo del processo di accreditamento degli utenti

breve- medio termine.

Affiliate
Visiting Professors

N.B.
I convegnisti vengono gestiti, al pari degli studenti, su un ramo parallelo della LDAP senza riferimento con il SSO e per di più volatile, nel senso che a termine convegno vengono rimossi d'ufficio.

Mappatura degli utenti sulle affiliazioni IDEM

Si veda più nel dettaglio il processo di accreditamento dell'utente.

Visione di insieme del processo di accreditamento degli utenti

Il processo di accreditamento per la categoria di utenti Staff ed Affiliate

Il processo

Modalità di riconoscimento della persona

Poiché il SSO al momento è utilizzato prevalentemente per l'accesso ai servizi erogati da IDEM-GARR-AAI e non ci sono previsioni a breve di utilizzo per altri servizi, il processo di riconoscimento parte dall'ente – Dipartimento, Facoltà o Direzione Centrale – che autorizza la richiesta di indirizzo e-mail dell'utente e che richiede le credenziali in nome dell'utente via fax con apposito modulo.

Università degli Studi di Cagliari
Direzione per le Reti ed i Servizi Informatici

Documento descrittivo del processo di accreditamento degli utenti

A seconda dell'Ente che autorizza ed a seconda delle necessità dell'utente, quest'ultimo può richiedere l'account su due domini virtuali: unica.it ed amm.unica.it, corrispondenti per esigenze di rete e di procedure a due distinti rami della LDAP: rtsc ed amm2. Il solo ramo rtsc è al momento coinvolto e visibile nel processo di SSO.
Quanto segue vale dunque in particolare per il ramo rtsc della LDAP.

Al momento della creazione dell'account e-mail una serie di scripts sincronizzano il server di posta con il server LDAP inserendo nel ramo rtsc l'utente, specificando in particolare le seguenti classi ed i seguenti attributi:

top
person
inetOrgperson
ntUser
organizationalPerson

givenName
sn
cn
description
uid
userPassword
businessCategory (in genere l'ente presso cui l'utente presta servizio)
preferredLanguage
mail
telephoneNumber
facsimileTelephoneNumber

Università degli Studi di Cagliari

Direzione per le Reti ed i Servizi Informatici

Documento descrittivo del processo di accreditamento degli utenti

ePTID (generato)
mobile (**)
employeeType (docente, ATA, ...)
employeeNumber (matricola)
postalAddress (**)
postalCode (**)
roomNumber (**)
ntUserDomainId (***)
ntUserCreateNewAccount (***)
ntUserDeleteAccount (***)
pwdpolicysubentry (***)

la classe eduPerson e gli attributi

eduPersonEntitlement
eduPersonAffiliation
eduPersonScopedAffiliation
eduPersonAffiliation
eduPersonPrincipalName
vengono invece inseriti in maniera "semiautomatica" da uno script su esplicita richiesta dell'utente, autorizzata dal responsabile dell'ente di appartenenza.

Le strutture tecnico-amministrative coinvolte sono dunque la direzione e la segreteria del singolo ente autorizzante ed il settore reti della DRSI che provvede ad inserire l'utente in LDAP ed eventualmente ad aggiungere la classe eduPerson ed i relativi attributi.

(**) se dichiarati al momento della richiesta: non obbligatori (mobile solitamente è parte

Università degli Studi di Cagliari
Direzione per le Reti ed i Servizi Informatici

Documento descrittivo del processo di accreditamento degli utenti

del campo gecos nella creazione della mail)

(***) inseriti per necessità di congruenza con il sistema di Active Directory in uso nel sistema amministrativo ed in vista di una futura unificazione dei due sistemi

Caratteristiche dell'identità digitale

Nessun attributo tra quelli precedentemente elencati viene considerato pubblico e di conseguenza non viene fornito su richiesta alcunché ad alcuno, a meno di esplicita autorizzazione scritta da parte dell'utente titolare dei dati.

Gestione del ciclo di vita

Al momento le modifiche del ciclo di vita delle credenziali vengono fatte da questo Settore manualmente ed in seguito a comunicazione scritta da parte dell'Ufficio personale.
Fanno eccezione gli utenti titolari di account di posta elettronica a scadenza, per i quali quotidianamente uno script controlla lo stato rispetto alla data di scadenza, invia una mail di notifica 15, 7 3 ed 1 giorno prima della stessa, dopodiché se l'account non viene rinnovato, lo blocca impedendo all'utente l'accesso e contestualmente elimina il dn dal ramo rtsc della LDAP, eliminando dunque tutti i servizi di SSO ed eventuali altri servizi attivati a partire dalle credenziali dell'utente (VPN, wi-fi, ···)..
Trascorsi 30 giorni dal blocco, un altro script provvede alla rimozione definitiva dell'account dal server di posta.

Formato e regole delle credenziali

Al momento le sole credenziali coinvolte nel processo di SSO sono quelle sopra descritte.

Università degli Studi di Cagliari
Direzione per le Reti ed i Servizi Informatici

Documento descrittivo del processo di accreditamento degli utenti

Eventuale presenza di credenziali multiple per la stessa persona

Segreterie e direzioni di enti sono in possesso di ulteriori credenziali "istituzionali" che comunque non sono coinvolte nel processo di SSO

Modalità di consegna delle credenziali

Le credenziali vengono consegnate personalmente e previa esibizione di un documento di identità presso la sede amministrativa del Settore Reti; occasionalmente e solo in caso di reale e comprovata necessità possono essere consegnate via mail o via fax a seguito di una richiesta per fax recante l'indirizzo e-mail di destinazione e copia di un documento valido di identità

Modalità di recupero delle credenziali smarrite

Il meccanismo, in caso di smarrimento della password, è analogo a quello di creazione dell'utenza: l'ente notifica lo smarrimento e richiede il reset della password per fax, con le modalità descritte nel processo di creazione/rinnovo.
La password viene resettata mediante generazione di password random, quindi consegnata all'utente con i metodi descritti sopra

Durata dell'accreditamento

La durata dell'accreditamento per il personale a t.d. è stabilita dal responsabile dell'ente richiedente in fase di richiesta di creazione.
Nella sezione dedicata al ciclo di vita delle credenziali è descritto il meccanismo di scadenza; la nuova scadenza, in caso di proroga, viene implementata a mano sul server di posta.

Disabilitazione utente

Documento descrittivo del processo di accreditamento degli utenti

Non esiste la possibilità di disabilitare temporaneamente un'utenza, essendo legata la stessa all'indirizzo e-mail, se si escludono i 30 giorni di "congelamento" dell'account senza alcun servizio descritta poco sopra.
Ove si presentasse la necessità di sospensioni superiori ai 30 giorni, si preferisce per motivi di sicurezza eliminare l'account ed eventualmente ricrearlo in seguito.

Cancellazione definitiva utente

La cancellazione definitiva dell'utente, ove non avvenisse automaticamente per mancato rinnovo entro i 30 giorni dal blocco, viene fatta secondo lo stesso criterio di eliminazione dell'account di posta e di conseguente sincronizzazione tra mailserver e LDAP.

Ciò avviene per notifica dell'Ufficio Personale a seguito di pensionamento, licenziamento a qualsiasi titolo, decesso dell'utente.
Nel primo caso, il pensionato che ottenga un eventuale contratto di consulenza, può richiedere tramite la direzione dell'ente di appartenenza la trasformazione del suo account in account temporaneo, qualora non sia già stato eliminato, ovvero la creazione di un account nuovo e temporaneo nell'ipotesi che il vecchio sia già stato eliminato.

Rischi specifici associati alla categoria di utenti

La sola categoria di utenti potenzialmente foriera di rischio, anche se soltanto in linea teorica, è stata individuata nei dottorandi, in quanto ex-studenti e poco avvezzi, forse, al concetto di privacy.
Su questo piano si provvede a notificare all'utente all'atto della consegna delle credenziali i diritti ed i doveri, con particolare insistenza sugli aspetti potenzialmente penali di eventuali infrazioni alle regole. Firmando per il ritiro della password, sottoscrivono

l'impegno all'accettazione delle regole ed inoltre si precisa che può essere ritenuto corresponsabile il mallevadore che autorizza la creazione dell'utenza.
Operativamente, vengono controllati periodicamente i log di Shibboleth per verificare che non vi sia difformità di IP in collegamenti cronologicamente ravvicinati della stessa utenza.

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

Al momento non vi sono interazioni tra le credenziali "deboli" utilizzate per il SSO e le eventuali credenziali "forti" (smartcard), peraltro in uso soltanto per la convalida degli esami.

Università degli Studi di Cagliari

Direzione per le Reti ed i Servizi Informatici

Documento descrittivo del processo di accreditamento degli utenti

Il sistema di autenticazione e autorizzazione interno

Oltre alle finalità sopra descritte, al momento il sistema di autenticazione basato sulle credenziali di posta elettronica e sull'autenticazione LDAP viene utilizzato, via Radius, per l'accesso alla VPN di ateneo, al wi-fi di Ateneo, ed eventualmente al wi-fi di eduRoam.
I tre campi di applicazione sorpa citati sono indipendenti ed invisibili rispetto al processo di SSO per Shibboleth.

Gli identificatori principali di ogni utente all'interno del singolo ramo LDAP sono univoci e non possono essere riutilizzati con la sola eccezione dei casi in cui, per esempio, un utente a t.d. viene cancellato per sopraggiunta scadenza e tempo dopo richiede nuovamente l'accesso a seguito di un nuovo contratto; in tali casi la tendenza è di ricreare le vecchie credenziali.

Partecipazione ad altre federazioni

L'Università di Cagliari al momento non partecipa ad altre Federazioni.