UNIVERSITÀ
DEGLI STUDI DI TRIESTE

Documento descrittivo del processo di accreditamento degli utenti

Universita' degli Studi di Trieste

2 Agosto 2011

Abbreviazioni

Divisione V Infrastrutture dei Servizi Informativi: Divisione ISI
Active Directory Microsfot Windows: AD
Personale Tecnico Amministrativo: Personale T/A
Processo Accreditamente e gestione del Ciclo di Vita degli account: processo ACV
Interfaccia CSA-like: iCSA
Interfaccia UGOV-like: iUGOV

Visione di insieme del processo di accreditamento degli utenti ai fini dell'affiliazione IDEM Garr

Per accreditamento intendiamo la generazione dell'identificativo utente nel Directory Service, X.500 compliant, implementato in AD. Diversi sono i database e diverse sono le strutture che alimentano AD per la creazione/modifica/aggiornamento dell'utenza in tale ambiente.

In figura 1 vediamo il flusso standard dalla persona fisica all'identità digitale per IDEM Garr. Durante ogni fase c'è un filtraggio degli attributi al fine di ottenere un provisioning consistente dei soli dati di interesse per la struttura che usufruirà dei dati..

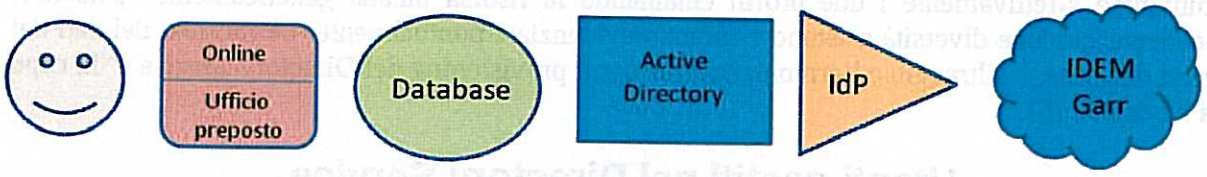

Figure 1: Flusso Stardard

Si parte dalla persona fisica che attraverso una procedura online o presso l'ufficio preposto si fa riconoscere e con questi dati viene popolato il database istituzionale al quale compete il trattamento di quella persona. Il passo successivo consiste in un provisiong per l'ambiente AD, cosa che come vedremo più avanti avviene solo a certe ben precise condizioni. Infine al momento dell'autenticazione presso il nostro Identity Provider sono ricavati gli attributi e le membership AD

associati all'utente e da questi viene estratto l'insieme di attributi minimi con cui alimentarei Service Provider di IDEM Garr. Attualmente il sistema di autenticazione autorizzazione basato su SAML e' utilizzato solo per l'ingresso nella Federazione IDEM Garr.

I nostri database istituzionali e autoritativi sono: ESSE3 per gli studenti, UGOV per il personale tecnico amministrativo e per il personale docente. In figura 2 e' rappresentato schematicamente il flusso del provisioning con maggiore dettaglio per quanto riguarda i database autoritativi e la struttura di competenza per la creazione dell'identità digitale nell'Ateneo di Trieste.

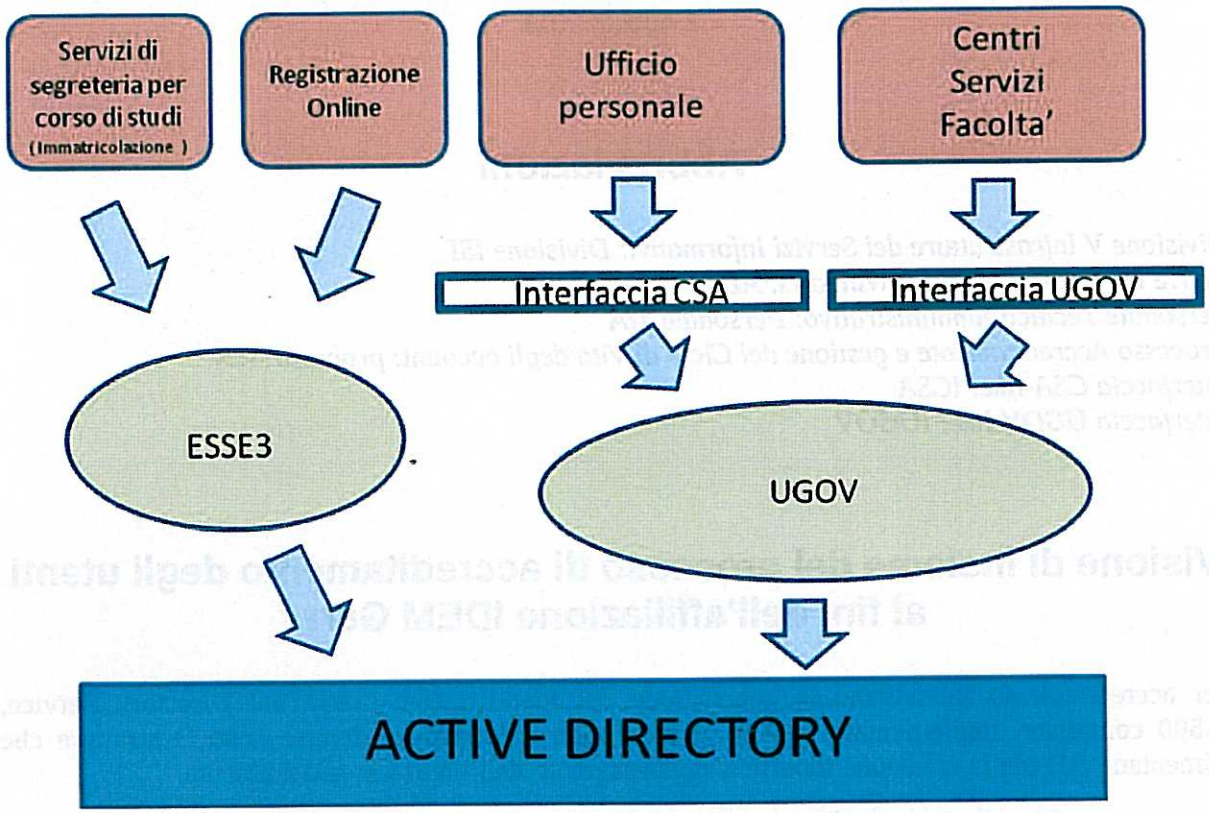

Figure 2: Flussi principali per il provisioning del directory service AD.

Poiché le identità digitali del personale tecnico amministrativo e del personale docente popolano lo stesso database e il profilo relativo alla gestione dell'identità e' molto simile si è deciso di accumunare effettivamente i due profili chiamando la risorsa umana genericamente "personale dipendente", alcune diversità esistono e saranno evidenziate puntualmente. La raccolta dei dati dai diversi database, il filtraggio e l'armonizzazione per il provisioning del Directory Service e' in capo alla Divisione ISI.

Utenti gestiti nel Directory Service

La tipologia di utenze concentrate in AD è poliedrica e complessa. In questo documento ci occuperemo solo delle tipologie di utenze di interesse per l'affiliazione IDEM Garr. Nel nostro Ateneo si è deciso, almeno in una fase iniziale, di dare accesso alle risorse federate solo alle tipologie personale e studente[1], per le quali il processo ACV, viene ampiamente descritto nel

[1] Per una spiegazione piu' esauriente di come cio' sia stato ottenuto si veda in appendice B.

seguito. Questa scelta è stata fatta poiché le altre tipologie di identità digitali in Ateneo richiedono ancora una collocazione precisa sia nel contesto federato ma soprattutto nell'infrastruttura dell'Ateneo stesso (es. personale esterno di cooperative). Se nel futuro si presenterà la necessità di aggiungere altre tipologie di utenza lo comunicheremo tempestivamente alla federazione italiana IDEM Garr per concordare la possibilità di tale cambiamento e corredando il presente documento della descrizione processo ACV della nuova tipologia.

Nel macro insieme **personale docenti** confluiscono le persone che occupano le seguenti posizioni nell'Ateneo:

- Assegnista di ricerca
- Assistente universitario
- Borsista
- Collaboratore di ricerca
- Collaboratore di ricerca - Eminente Studioso
- Collaboratore esperto linguistico
- Collaboratore esperto linguistico a tempo determinato
- Conferimento incarico di insegnamento
- Lettore di Scambio
- Prof. Emerito
- Professore a contratto
- Professore a contratto - Eminente Studioso
- Professore Associato
- Professore Ordinario
- Ricercatore a tempo determinato
- Ricercatore Universitario
- Tutor esercitazioni didattiche

Nel macro insieme **personale T/A** confluiscono le persone che occupano le seguenti posizioni nell'Ateneo:

- Contratto di collaborazione coordinata continuativa
- Dirigente
- Personale tecnico-amministrativo a tempo indeterminato
- Personale tecnico-amministrativo a tempo determinato

Nell'insieme **studenti** confluiscono le persone che occupano le seguenti posizioni nell'Ateneo:

Studenti iscritti a:

- Laurea triennali, specialistica/magistrale
- Laurea specialistica/magistrale a ciclo unico
- Master di primo e secondo livello
- Dottorato di ricerca
- Corso di specializzazione
- Corso di perfezionamento

Mappatura degli utenti sull'insieme di affiliazioni eduPerson necessarie per IDEM

Ai fini dell'affiliazione IDEM Garr solo quattro delle classi che compomgono l'intero spettro di attributi per l'eduPersonAffiliation sono necessarie: Staff, Student, Alum, Affiliate.
Staff e Student poi confluiscono nello stesso insieme: Member. La mappatura degli utenti AD sugli attributi necessari all'affiliazione ad IDEM è ottenuta con scripting al momento della risoluzione in sede all'IdP Shibboleth. Per chiarezza esplicitiamo che l'attributo Alum non viene assegnato a nessuno poiché non abbiamo in Ateneo nessun profilo di utenza AD che possa ricalcare questo attributo. L'attributo Affiliate , suggerito da IDEM Garr , come descrittivo degli esterni, non viene popolato da nessun profilo di utenza AD. Si deduce che gli unici profili eduPersonAffiliation che vengono forniti sono:

- **Staff** viene assegnato al gruppo Personale
- **Student** viene assegnato al gruppo Studenti
- **Member** viene assegnato a Staff e a Student

Dopo questa introduzione al processo ACV prima di entrare nel dettaglio delle singole tipologie, dobbiamo sottolineare le posizioni particolari degli studenti lavoratori, degli specializzandi e dei dottorati di ricerca. Infatti in questi casi ad una persona fisica vengano rilasciate due identità digitali distinte ed indipendenti nel contesto dell'Ateneo, quella che arriva dal flusso Esse3, come studente, e quella che arriva dal flusso Ugov come dipendente.

Il processo ACV per la categoria degli utenti: personale

Il processo

Ai fini delle credenziali AD associate all'utenza si fa riferimento al numero di matricola della risorsa umana. Il numero di matricola dei dipendenti viene generato all'atto della registrazione presso o gli Uffici del Personale o i Centri Servizi delle Facoltà di afferenza. La registrazione consiste nell'inserimento effettivo a terminale tramite iCSA o iUGOV dell'anagrafica della risorsa umana. Questa risorsa umana ora definita effettivamente dal numero di matricola verrà fatta transitare in ambiente AD soltanto se le verrà attribuito un ruolo ovvero un incarico, cioè soltanto se alla risorsa umana si associa un contratto di lavoro, flusso che passa attraverso iCSA, oppure si associa una docenza attiva, flusso che passa attraverso iUGOV.

Modalità di consegna delle credenziali

Al momento dell'attivazione dell'utenza in UGOV, sia attraverso iCSA o iUGOV e quindi della transizione verso l'ambiente AD viene inviata una mail ad un indirizzo privato, precedentemente fornito, contenente il numero di matricola, cioè lo username AD, e le istruzioni per computare la sua prima password.

Formato e regole delle credenziali

La prima password è composta da almeno 10 caratteri e non è necessario cambiarla. Questa passowrd si può cambiare sia da un computer inserito nel dominio AD sia allla pagina https://helpdesk.units.it/changepassword/index.asp.

Caratteristiche dell'identità digitale

In AD le utenze che appartengono al flusso elaborato da iCSA o iUGOV arrivano in AD corredate del seguente set di campi:

- Matricola
- Cognome
- Nome
- Telefono interno
- Mail istituzionale
- Tipo dipendente (docente o tecnico amministrativo)
- Ruolo CSA
- Recapito interno
- Afferenza organizzativa
- Facoltà
- Flag1 (inserimento iniziale, cancellazione, modifica, blocco)
- Flag2 (appartenenza amministrazione centrale)

Tutti gli attributi AD del personale sono pubblicati sul phonebook liberamente consultabile sulle pagine web dell'Ateneo.

Dopo un aggiornamento/inserimento in UGOV dell' unità di personale, lo status di inserimento, cancellazione, modifica o blocco viene reso noto ad AD tramite una sincronizzazione periodica.

Modalità di recupero delle credenziali smarrite

In caso di smarrimento della password associata al proprio numero di matricola la persona deve mandare un fax allo 040-558-3316 o lettera di richiesta di forzatura password corredati di fotocopia di un documento di identità agli uffici dell'amministrazione centrale oppure previo appuntamento chiamando lo 040-558-3333 possono presentarsi di persona.

Durata dell'accreditamento

Scadenza ore 24:00 della data più remota tra un anno solare ed il 31.08 anno successivo alla data di cessazione. Dopo tale momento, il processo di logon per l'Utente AD darà sempre esito negativo

Cancellazione definitiva utente

Non prevista.

Interoperabilità tra credenziali deboli e credenziali forti (solo docenti)

Nel processo descritto come verbalizzazione online, nel quale il docente usa una firma digitale per siglare l'esito degli esami e spedirlo alle segreterie studenti, c'è un uso sinergico tra credenziali deboli e credenziali forti.

Modalità di gestione smarrimento smartcard/token (solo docenti)

Il titolare può richiedere la revoca esclusivamente tramite l'Ufficio R.A. della Divisione I.S.I. presentando una richiesta scritta, accompagnata da una fotocopia di un documento di riconoscimento.

Il processo ACV per la categoria degli utenti: studenti

Il processo

Il persId , attributo che verrà poi utilizzato per creare lo username in ambiente AD degli studenti, viene generato sul database ESSE3 al momento della loro registrazione online. Solo nella fase dell'immatricolazione presso le segreterie del corso di studi, una volta identificata la persona, i record identificativi dello studente popolano AD.

Modalità di consegna delle credenziali

E' all'atto dell'immatricolazione che viene consegnata allo studente una lettera che riporta lo username AD e la password. La consegna avviene presso gli sportelli delle segreterie e cioè Segreterie studenti, Segreterie dei corsi di specializzazione, Segreteria Ripartizione Mobilità internazionale, Segreteria Dottorati di ricerca.

Caratteristiche dell'identità digitale

In AD le utenze che appartengono al flusso da ESSE3 sono create con questo insieme di attributi:

- PersID
- Status
- Cognome
- Nome
- Matricola
- Codice corso di laurea
- Codice Facoltà
- Anno di corso a cui è iscritto
- CFR in corso fuori corso ripetente
- Anno accademico di ultima iscrizione
- Sede di frequenza
- Tipologia di corso
- FINE (motivo della disabilitazione)
- Data di lettura dei Record da Esse3
- PASSWORD

Nessun attributo AD è pubblico, né ovviamente i dati personali dell'utenza in qualsiasi database si trovino. Il db Esse3 viene sincronizzato automaticamente ogni 24 ore con l'ambiente AD.

Formato e regole delle credenziali

La prima password è composta da almeno 10 caratteri e non è necessario cambiarla. Questa password si può cambiare sia da un computer inserito nel dominio AD sia allla pagina https://helpdesk.units.it/changepassword/index.asp

Modalità di recupero delle credenziali smarrite

Per forzare una nuova password , in caso di smarrimento, lo studente può recarsi presso:

- Sportello Veloce
- Segreterie studenti
- Segreterie dei corsi di specializzazione
- Segreteria Ripartizione Mobilità internazionale
- Segretaria Dottorati di ricerca

Durata dell'accreditamento

Dal giorno in cui si immatricola fino ad un evento che porti il flag Status di ESSE3 al valore "Bloccato". Le motivazioni per il blocco sono diverse, ma esenzialmente ricadono in due tipologie o Sospeso o Cessato. Dalla data di blocco l'utente ha le credenziali AD abilitate fino al 31 Maggio di due anni dopo. Dopo tale momento l'utenza AD è disabilitata. Aggiungiamo anche che da uno status Bloccato per sospensione l'utente può essere riabilitato se riattiva l'iscrizione.

Cancellazione definitiva utente

Non previsto.

Partecipazione ad altre federazioni

L'università' degli Studi di Trieste partecipa alle seguenti federazioni di interesse per le identità digitali:

- Eduroam
- Trieste Città Universitaria

APPENDICE A

Al momento dell'autenticazione il modulo JAAS, come si vede dal codice allegato, è configurato per sfogliare solo le organizational unit relative agli studenti e al personale dipendente. In questo modo si è riuscito a fare una scrematura di tutte le utenze che, come si è detto, non hanno un profilo chiaro.

```
ShibUserPassAuth {

   edu.vt.middleware.ldap.jaas.LdapLoginModule sufficient
      referral="follow"
      ldapUrl="ldap://dc1ts.ds.units.it:389"
      baseDn="ou=personale,dc=ds,dc=units,dc=it"
      ssl="true"
      subtreeSearch="true"
      bindDn=utente@ds.units.it
      bindCredential="PASSWORD"
      userFilter="sAMAccountname={0}";

   edu.vt.middleware.ldap.jaas.LdapLoginModule sufficient
      referral="follow"
      ldapUrl="ldap://dc1ts.ds.units.it:389"
```

```
        baseDn="ou=studenti,dc=ds,dc=units,dc=it"
        ssl="true"
        subtreeSearch="true"
        bindDn=utente@ds.units.it
        bindCredential="PASSWORD"
        userFilter="sAMAccountname={0}";

};
```