UNIVERSITÀ DI SALERNO

IDEM DOPAU UNISA

DOCUMENTO DESCRITTIVO DEL PROCESSO DI ACCREDITAMENTO DEGLI UTENTI DELL'ORGANIZZAZIONE UNISA

Alfonso Sparano

24/05/2012

DOCUMENTO DESCRITTIVO DEL PROCESSO DI ACCREDITAMENTO DEGLI UTENTI DELL'ORGANIZZAZIONE UNISA

Le informazioni fornite in questo documento sono accurate alla data del 24/05/2012

REVISIONI

Data	Versione	Descrizione modifica	Autore
09/12/2011	0.1	Bozza	Alfonso Sparano
12/12/2011	0.2	Bozza	Salvatore Ferrandino
21/12/2011	0.3	Bozza	Alfonso Sparano
24/05/2012	1.0	Definitivo	Alfonso Sparano

INDICE

NOTA INTRODUTTIVA

La partecipazione alla Federazione IDEM ("Federazione") abilita l'organizzazione partecipante ("l'Università degli studi di Salerno") ad utilizzare la tecnologia di Shibboleth di condivisione degli attributi relativi alle identità per gestire l'accesso alle risorse on-line che possono essere rese disponibili all'interno della comunità IDEM. Un obiettivo della Federazione è quello di sviluppare, nel tempo, degli standard per le organizzazioni al fine di assicurare che le asserzioni sugli attributi che vengono scambiate siano sufficientemente robuste e fidate per gestire l'accesso ad importanti risorse protette. Con la crescita della fiducia interna, la Federazione spera che ciascun partecipante possa fidarsi dei sistemi di Identity Management e dei sistemi di gestione di accesso alle risorse degli altri membri della federazione come si fidano dei propri.

Fondamentalmente ci si aspetta dai partecipanti che essi forniscano agli altri membri asserzioni sugli attributi autorevoli e accurate e che ciascuno riceva asserzioni sugli attributi protette e nel rispetto dei vincoli di privacy imposti dalla Federazione o dalla fonte delle informazioni. Per raggiungere tale obiettivo IDEM richiede che ogni partecipante renda disponibile agli altri partecipanti certe informazioni di base riguardanti il proprio sistema di Identity Management, in particolare riguardo gli attributi che vengono utilizzati per la Federazione.

I due criteri per garantire che gli Identity Provider forniscano asserzioni di attributi fidate sono:

- che il sistema di gestione delle identità ricada sotto la supervisione degli organismi che hanno responsabilità direttive e gestionali nell'Organizzazione;
- il sistema che emette le credenziali per gli utenti finali sia dotato di appropriate misure di gestione del rischio

Questo Documento è il DOPAU dell'Università di Salerno (UniSa) e contiene le informazioni necessarie per l'accreditamento alla federazione IDEM.

Qualsiasi modifica futura verrà inserita in questo documento che sarà quindi prontamente aggiornato e trasmesso in copia alla Federazione.

GESTORE DELL'ACCREDITAMENTO

L'accreditamento in UniSa è gestito dalle seguenti strutture competenti:

- **Segreterie Studenti**, per gli studenti;
- **Ufficio Post Laurea**, per gli assegnisti di ricerca, i dottorandi e per i borsisti;
- **Ufficio Coordinamento Personale Tecnico-Amministrativo**, per il personale TA;
- **Ufficio Contratti e Supplenze**, per docenti esterni o a contratto;
- **Ufficio Carriere e Stato Giuridico**, per il personale docente e ricercatore, assistenti ordinari e dei professori incaricati.

L'ufficio Sistemi Tecnologici e l'ufficio Coordinamento Servizi Informatici, gestiscono le procedure di filtraggio e armonizzazione dei dati trattati dai diversi uffici sopra riportati.

UTENTI GESTITI

PERSONALE DIPENDENTE

Sono gli utenti i cui dati provengono **dall'Ufficio Coordinamento Personale Tecnico-Amministrativo, Ufficio Carriere e Stato Giuridico, Ufficio Contratti** e **Supplenze** e **Ufficio Post Laurea** e sono:

- Assistente universitario;
- Dirigente;
- Dirigente a contratto;
- Personale docente;
- Personale docente supplente;
- Personale tecnico amministrativo;
- Ricercatore universitario.

STUDENTI

Sono gli utenti i cui dati provengono dalle **Segreterie Studenti** e dall'**Ufficio Post Laurea** e che hanno una carriera universitaria attiva:

- Assegnista di ricerca;
- Borsista post-dottorato;
- Dottorando;
- Studente.

ALUMNI

Sono gli utenti i cui dati provengono dalle **Segreterie Studenti** e dall'**Ufficio Post Laurea**. In particolare sono studenti che hanno conseguito un titolo, eventualmente anche di primo livello.

ESTERNI

Sono utenti non in organico dell'ateneo ma identificati presso le strutture periferiche:

- Rapporti assimilabili allo studente;
- Rapporti assimilabili al docente;
- Rapporti che richiedono il solo accesso alla rete.

MAPPATURA DEGLI UTENTI SULLE AFFILIAZIONI IDEM

L'affiliazione definisce la relazione che esiste tra l'Utente e la propria Organizzazione di Appartenenza. Per descrivere l'affiliazione, all'interno delle comunità scientifiche, Internet2 propone lo schema **eduPerson** [EDUPER] con gli attributi **eduPersonAffiliation** e **eduPersonPrimaryAffiliation**. A questi attributi è associabile soltanto un insieme predefinito di valori elencati: **faculty, student, staff, alum, member, affiliate, employee, library-walk-in**.

I valori elencati individuano delle classi di persone; alcune classi sono specializzazioni di altre.

Nel documento della Federazione IDEM denominato *"Specifiche tecniche per la compilazione e l'uso degli attribuiti – v. 2.1"*, vengono definiti soltanto i valori **staff, student, member, affiliate, alum** e **library-walk-in**. L'uso degli altri valori per gli scopi della federazione italiana è sconsigliato fino a che non ne venga definito un significato unanimemente condiviso.

Il valore **staff** indica tutto il personale (docenti, personale amministrativo, bibliotecario ecc.) in servizio presso l'organizzazione di appartenenza con qualunque tipo di contratto, anche a tempo determinato, oppure rientrante nei contratti cosiddetti atipici (co.co.pro., prestazioni professionali, interinali, ecc...).

Con **student** si indicano gli studenti regolarmente iscritti ad uno dei corsi dell'organizzazione di appartenenza.

Student e **staff** sono due specializzazione distinte di **member**.

Member contiene tutte le persone che hanno un rapporto istituzionale con l'organizzazione di appartenenza e ai quali viene dato un insieme base di privilegi. Comprende gli **student**, gli **staff** e tutti coloro che pur non rientrando nelle classi precedenti, hanno rapporti istituzionali con la comunità scientifica.

Affiliate si applica alle persone con le quali l'organizzazione di appartenenza ha una qualsiasi forma di rapporto ed alle quali è necessario attribuire un'identità di utente, ma alle quali non vengono estesi i privilegi derivanti dall'essere membri dell'organizzazione stessa. Potrebbero rientrare in questa categoria i fornitori di servizi o materiali delle organizzazioni, ricercatori di altre organizzazioni che collaborano con un gruppo interno, persone per le quali è necessaria l'identificazione per servizi molto particolari riservati ad esterni all'università stessa.

Alum comprende gli ex studenti che hanno completato almeno il primo livello di studi all'interno dell'Ateneo.

Library-walk-in indica i frequentatori di una biblioteca ed è pensato per semplificare la gestione di frequenti accordi contrattuali con i fornitori di risorse. Il valore è indipendente dagli altri valori indicanti l'affiliazione, ciò vuol dire che il possedere tale requisito non influisce o pregiudica l'avere un altro tipo di affiliazione e viceversa. **Questo valore non è ad oggi utilizzato nell'Università di Salerno**.

TABELLA DI ESEMPIO DI CORRISPONDENZE TRA UTENTI DI ATENEO E AFFILIAZIONI

UTENTE DI ATENEO	AFFILIATION
Alumni	ALUM
Assegnista di ricerca	MEMBER
Assistente (Assistenti universitari)	MEMBER, STAFF
Borsista post-dottorato	MEMBER, STUDENT
Dirigente	MEMBER, STAFF
Dirigente a contratto	MEMBER, STAFF

Dottorando	MEMBER, STUDENT
Personale docente	MEMBER, STAFF
Personale docente supplente	MEMBER
Personale tecnico amministrativo	MEMBER, STAFF
Rapporti assimilabili al docente	MEMBER
Rapporti assimilabili allo studente	STUDENT,MEMBER
Rapporti che richiedono il solo accesso alla rete	AFFILIATE
Ricercatore universitario	MEMBER, STAFF
Studente	STUDENT,MEMBER

VISIONE DI INSIEME DEL PROCESSO DI ACCREDITAMENTO DEGLI UTENTI

Le credenziali utente (nome utente e password) sono memorizzate in due repository principali:

- un cluster LDAP;
- nel database ORACLE – ESSE3.

Per quanto riguarda il cluster LDAP, esso contiene quasi esclusivamente dati provenienti da altre fonti dati autoritative, (l'unico dato gestito in locale, e quindi non proveniente da altre fonti, è la password).

Tutti gli attributi provengono da fonti dati autorevoli a secondo del profilo associato. Ad esempio, per uno studente gli attributi specifici provengono dal software di gestione delle carriere degli studenti ESSE3, per il personale docente e tecnico amministrativo dal software per la gestione delle risorse umane CSA.

Per gli utenti non incardinati nell'organigramma di Ateneo è stato sviluppato un applicativo specifico che rappresenta anche la fonte dati autorevole rispetto questa tipologia di utenti.

Tecnicamente il cluster Directory Server utilizzato è costituito da due server REDHAT DIRECTORY SERVER configurati in multi-master con sincronizzazione continua e bidirezionale, mentre il DB ORACLE è gestito da 5 nodi ORACLE RAC versione 11.

FONTI DATI AUTORITATIVE

Le fonti dati autoritative sono distinte per tipologia

- DB ESSE3;
- DB CSA;
- DB PersonalDesk del personale esterno/non incardinato (procedura sviluppata internamente e amministrata dai responsabili di struttura o dai docenti).

UTILIZZO DELLE CREDENZIALI

Gli utenti fanno uso delle credenziali centralizzate per diversi servizi:

- Autenticazione SHIBBOLETH di vari servizi web di Ateneo;
- Autenticazione alle caselle di posta mediante POP3, IMAP e SMTP;
- Autenticazione WIFI al CAPTIVE PORTAL attraverso un server RADIUS;
- Autenticazione WIFI alla rete EDUROAM attraverso un server RADIUS.

IL PROCESSO DI ACCREDITAMENTO PER LA CATEGORIA DI UTENTI "PERSONALE DIPENDENTE"

Per questa tipologia di utente si fa riferimento alla fonte dati autorevole CSA – Carriere e Stipendi di Ateneo. Gli uffici Coordinamento Personale Tecnico-Amministrativo, Carriere e Stato Giuridico e Ufficio Contratti e Supplenze, costantemente aggiornano l'applicativo CSA e conseguentemente, accedendo al

DB risulta possibile sapere in ogni istante quali sono le unità di personale attivo e quando invece sono scaduti i contratti. Attraverso delle viste Oracle, aggiornate ogni notte, la piattaforma centralizzata disattiva, attiva o aggiorna tutti i profili modificati.

Il processo

I flussi di creazione/modifica/cancellazione sono svolti, conformemente alle normative vigenti, nell'ambito dell'applicativo CSA. In sintesi, ogni modifica nell'applicativo, viene inserita solo in seguito a decreti amministrativi.

Modalità di riconoscimento della persona

Gli uffici competenti per le diverse tipologie di utenti richiedono la presenza dell'interessato con documento di identità valido durante:

- la firma del contratto;
- oppure, per alcune tipologie di utenti, durante la compilazione/inserimento dati nell'applicativo CSA.

Caratteristiche dell'identità digitale

Gli attributi estratti dalla fonte dati autorevole sono esclusivamente quelli di tipo obbligatori e raccomandati secondo classificazione riportata nel documento *"Specifiche tecniche per la compilazione e l'uso degli attribuiti – v. 2.1"*, ovvero:

- come attributi raccomandati: sn, givenName, cn, mail;
- come attributi obbligatori: eduPersonScopedAffiliation, eduPersonTargetedID ed eduPersonPrincipalName.

Tutti gli attributi estratti sono considerati pubblici nell'ambito della federazione IDEM ma soggetti ad approvazione mediante uApprove dal singolo utente.

Per eventuali SP esterni alla Federazione IDEM gli attributi saranno rilasciati accordandosi con i fornitori del servizio, coerentemente alla polita di fornire il minor numero di attributi possibili necessari alla corretta erogazione del servizio.

Gestione del ciclo di vita

Quando un dato viene modificato in uno dei DB autorevoli, la sincronizzazione viene propagata nel Sistema di Gestione delle Identità di Ateneo entro le 24 ore successive.

Formato e regole delle credenziali

Ciascun individuo, indipendentemente dal ruolo associato, è dotato di un'unica coppia di credenziali di autenticazione univoche (denominate CAU). La username è costruita sulla base del codice fiscale più un progressivo. Questa codifica consente di avere una unica username associata ad una persona fisica conformemente al decreto legislativo 196/2003.

Ad oggi non è previsto nessun altro sistema di autenticazione.

Modalità di consegna delle credenziali

La prima password viene assegnata tramite una procedura WEB automatica eseguita direttamente dall'utente interessato. Il proprietario accede alla procedura WEB utilizzando il suo codice fiscale e un codice OTP (codice consegnato in busta chiusa e a mano all'interessato dall'ufficio competente).

Terminata la fase di inizializzazione all'utente vengono assegnate le CAU che resteranno legate al suo codice fiscale indipendentemente dal ruolo associato.

Modalità di recupero delle credenziali smarrite

Qualora l'utente abbia fornito il suo cellulare personale, potrà ripristinare la password attraverso un sistema di SMS e OTP. Negli altri casi si procede tramite ticket HELPDESK e riconoscimento de visu.

Durata dell'accreditamento

L'accreditamento dura fino al giorno del termine del contratto. Una volta scaduto il contratto, l'utente non potrà accedere ad alcun servizio tranne che la posta elettronica. Nel caso di riattivazione di un nuovo contratto, l'utente potrà nuovamente accedere ai servizi informatici con le medesime credenziali. La disattivazione di un utente avviene durante la notte ad opera degli script di sincronizzazione che marcano il profilo come non più attivo.

Disabilitazione utente

Non sono previste procedure di disattivazione utente se non per termine.

Cancellazione definitiva utente

L'utente non viene mai cancellato ma solo disattivato in seguito alla scadenza.

Il processo di accreditamento per la categoria di utenti "STUDENTI"

Per questa tipologia di utente si fa riferimento alle fonti dati autorevoli ESSE3 – Segreteria e Servizi agli Studenti e a CSA – Carriere e Stipendi di Ateneo . Gli uffici delle Segreteria Studenti e Ufficio Post Laurea costantemente aggiornano gli applicativi ESSE3 e CSA e conseguentemente, accedendo ai DB relativi, risulta possibile sapere in ogni istante quali sono gli studenti attivi e quali invece non sono più attivi. Attraverso delle viste Oracle, aggiornate in real-time, la piattaforma centralizzata disattiva, attiva o aggiorna tutti i profili.

Il processo

Sinteticamente i flussi di creazione/modifica/cancellazione sono svolti, conformemente alle normative vigenti, nell'ambito degli applicativi ESSE3e CSA.

L'iscrizione ad ESSE3 viene svolta dall'interessato in autonomia. Dopo aver introdotto i suoi dati anagrafici, eventuale e-mail di recupero credenziali e altre informazioni personali, viene attivato un profilo utente temporaneo. Questo profilo (costituito da username e password), prevede la possibilità di accedere alla federazione IDEM solo che l'utente in questione non avrà alcun attributo di tipo Affiliation.

In pratica lo studente potrà avere tre tipologie di Affiliation:

- Student;
- (none);
- Alumn.

Lo stato Alumn viene descritto successivamente. Per quanto riguarda invece lo stato Student, questo è assegnato ad un utente ESSE3 che risulti registrato e in regola con i pagamenti, ovvero sia in grado di

sostenere esami, in attesa di discussione di tesi, o condizioni similari. Lo stato (none) invece caratterizzano un utente registrato ma non ancora, o non più, in regola con i pagamenti.

MODALITÀ DI RICONOSCIMENTO DELLA PERSONA

Le credenziali temporanee diventano definitive nel momento in cui viene completata l'iscrizione e pagata la prima rata (ovvero l'utente diventa Student).

Gli uffici competenti per le diverse tipologie di utenti richiedono la presenza dell'interessato con documenti di identità validi o equivalenti durante il riconoscimento e la convalida dei dati introdotti in autonomia.

CARATTERISTICHE DELL'IDENTITÀ DIGITALE

Gli attributi estratti dalla fonte dati autorevole sono esclusivamente quelli di tipo obbligatori e raccomandati secondo classificazione riportata nel documento *"Specifiche tecniche per la compilazione e l'uso degli attribuiti – v. 2.1"*, ovvero:

- come attributi raccomandati: sn, givenName, cn, mail;
- come attributi obbligatori: eduPersonScopedAffiliation, eduPersonTargetedID ed eduPersonPrincipalName.

Tutti gli attributi estratti sono considerati pubblici nell'ambito della federazione IDEM ma soggetti ad approvazione mediante uApprove dal singolo utente.

Per eventuali SP esterni alla Federazione IDEM gli attributi saranno rilasciati accordandosi con i fornitori del servizio, coerentemente alla polita di fornire il minor numero di attributi possibili necessari alla corretta erogazione del servizio.

GESTIONE DEL CICLO DI VITA

Quando un dato viene modificato in uno dei DB autorevoli, la sincronizzazione viene propagata nel Sistema di Gestione delle Identità di Ateneo istantaneamente.

FORMATO E REGOLE DELLE CREDENZIALI

Ciascun studente è dotato di un'unica coppia di credenziali di autenticazione univoche in cui la username è costituita sulla base del nome, cognome e un progressivo. Questa codifica consente di avere una unica username associata ad una persona fisica conformemente al decreto legislativo 196/2003.

Per utenti molto vecchi la username può coincidere con la matricola.

MODALITÀ DI CONSEGNA DELLE CREDENZIALI

La prima password viene in genere assegnata tramite una procedura WEB eseguita dallo studente nell'ambiente ESSE3 (nel momento stesso della registrazione al portale). L'attivazione del profilo avviene solo in seguito al pagamento della prima rata e di una convalida dei dati presso la segreteria competente.

MODALITÀ DI RECUPERO DELLE CREDENZIALI SMARRITE

Qualora l'utente abbia fornito un indirizzo e-mail alternativo durante la registrazione al portale ESSE3, o anche successivamente, lo studente potrà recuperare la password inserendo semplicemente il suo codice fiscale. La procedura invierà quindi un messaggio all'indirizzo mail privato con i link necessari al ripristino dell'utenza.

Durata dell'accreditamento

L'accreditamento dura fino al conseguimento del titolo di studio o fino al momento di avere contratto un "debito" amministrativo. Per conseguimento titolo, lo studente "evolve" in ALUM. Per "debito" si intende invece l'incapacità dello studente ad effettuare operazioni amministrative senza provvedere prima a mettersi in regola con i pagamenti. La modifica dello stato di un profilo avviene istantaneamente.

Disabilitazione utente

Non sono previste procedure di disattivazione utente se non per evoluzione a ALUM o a (none).

Cancellazione definitiva utente

L'utente non viene mai cancellato ma solo disabilitato in seguito condizioni descritte nel paragrafo precedente.

Il processo di accreditamento per la categoria di utenti "ALUMNI"

Per questa tipologia di utente si fa riferimento alla fonte dati autorevole ESSE3 – Segreteria e Servizi agli Studenti. Gli uffici delle Segreteria Studenti e Ufficio Post Laurea costantemente aggiornano l'applicativo ESSE3 e conseguentemente, accedendo al DB risulta possibile sapere in ogni istante quali sono gli studenti con almeno un titolo conseguito. Attraverso delle viste Oracle, aggiornate in real-time, la piattaforma centralizzata modifica e aggiorna tutti i profili.

Il processo

Sinteticamente i flussi di creazione/modifica/cancellazione sono svolti, conformemente alle normative vigenti, nell'ambito dell'applicativo ESSE3. Nel momento in cui uno STUDENTE consegue un titolo diviene ALUMN. Qualora dovesse iscriversi ad altro corso di laurea, o anche laurea di secondo livello, lo studente acquisterà entrambi gli stati di ALUMN e di STUDENT.

Modalità di riconoscimento della persona

La persona non viene riconosciuta in questa fase ma quando è ancora uno STUDENTE. Di fatto, la persona di tipo ALUMN è uno STUDENTE che ha conseguito un titolo.

Caratteristiche dell'identità digitale

Gli attributi estratti dalla fonte dati autorevole sono esclusivamente quelli di tipo obbligatori e raccomandati secondo classificazione riportata nel documento *"Specifiche tecniche per la compilazione e l'uso degli attribuiti – v. 2.1"*, ovvero:

- come attributi raccomandati: sn, givenName, cn, mail;
- come attributi obbligatori: eduPersonScopedAffiliation, eduPersonTargetedID ed eduPersonPrincipalName.

Tutti gli attributi estratti sono considerati pubblici nell'ambito della federazione IDEM ma soggetti ad approvazione mediante uApprove dal singolo utente.

Per eventuali SP esterni alla Federazione IDEM gli attributi saranno rilasciati accordandosi con i fornitori del servizio, coerentemente alla polita di fornire il minor numero di attributi possibili necessari alla corretta erogazione del servizio.

GESTIONE DEL CICLO DI VITA

Quando un dato viene modificato in uno dei DB autorevoli, la sincronizzazione viene propagata nel Sistema di Gestione delle Identità di Ateneo immediatamente.

FORMATO E REGOLE DELLE CREDENZIALI

Ciascun ALUMN è dotato di un'unica coppia di credenziali di autenticazione univoche in cui la username è costituita sulla base del nome, cognome e un progressivo. Questa codifica consente di avere una unica username associata ad una persona fisica conformemente al decreto legislativo 196/2003.

Per utenti molto vecchi la username può coincidere con la matricola.

MODALITÀ DI RECUPERO DELLE CREDENZIALI SMARRITE

Qualora l'ALUMN abbia fornito un indirizzo e-mail alternativo potrà recuperare la password inserendo semplicemente il suo codice fiscale. La procedura invierà quindi un messaggio all'indirizzo mail privato con i link necessari al ripristino dell'utenza. Negli altri casi si dovranno recare presso la Segreteria esibendo un documento di identità valido e il codice fiscale.

DURATA DELL'ACCREDITAMENTO

L'accreditamento dura a tempo indefinito.

DISABILITAZIONE UTENTE

Non sono previste procedure di disattivazione utente.

CANCELLAZIONE DEFINITIVA UTENTE

L'utente non viene mai cancellato.

IL PROCESSO DI ACCREDITAMENTO PER LA CATEGORIA DI UTENTI "ESTERNI"

Per questa tipologia di utente si fa riferimento alla fonte dati autorevole PersonalDesk. Gli utenti vengono registrati, tramite un applicativo WEB, direttamente dal personale dell'Ateneo.

IL PROCESSO

Gli esterni sono accreditati direttamente nella struttura presso cui hanno il titolo che conferisce loro l'accesso al Sistema di Gestione delle Identità di Ateneo. Ogni struttura (dipartimento, facoltà, ufficio) può identificare il personale esterno. Durante la fase di identificazione, la persona che ha il compito di riconoscere l'utente, compilerà un modulo web in cui specificherà, oltre gli estremi anagrafici, anche un profilo con cui l'utente si presenterà nell'infrastruttura di Ateneo. La tipologia di utenti ESTERNI hanno un profilo con validità temporale limitata al più a tre anni. Tale periodo è rinnovabile indefinitamente.

MODALITÀ DI RICONOSCIMENTO DELLA PERSONA

La persona viene riconosciuta tramite codice fiscale e documento di identità valido.

CARATTERISTICHE DELL'IDENTITÀ DIGITALE

Gli attributi estratti dalla fonte dati autorevole sono esclusivamente quelli di tipo obbligatori e raccomandati secondo classificazione riportata nel documento *"Specifiche tecniche per la compilazione e l'uso degli attribuiti – v. 2.1"*, ovvero:

- come attributi raccomandati: sn, givenName, cn, mail;
- come attributi obbligatori: eduPersonScopedAffiliation, eduPersonTargetedID ed eduPersonPrincipalName.

Tutti gli attributi estratti sono considerati pubblici nell'ambito della federazione IDEM ma soggetti ad approvazione mediante uApprove dal singolo utente.

Per eventuali SP esterni alla Federazione IDEM gli attributi saranno rilasciati accordandosi con i fornitori del servizio, coerentemente alla polita di fornire il minor numero di attributi possibili necessari alla corretta erogazione del servizio.

Gestione del ciclo di vita

Quando un dato viene modificato la sincronizzazione viene propagata nel Sistema di Gestione delle Identità di Ateneo istantaneamente.

Formato e regole delle credenziali

Ciascun individuo, indipendentemente dal ruolo associato, è dotato di un'unica coppia di credenziali di autenticazione univoche (denominate CAU). La username è costruita sulla base del codice fiscale più un progressivo. Questa codifica consente di avere una unica username associata ad una persona fisica conformemente al decreto legislativo 196/2003.

Ad oggi non è previsto nessun altro sistema di autenticazione.

Modalità di consegna delle credenziali

La prima password viene assegnata tramite una procedura WEB automatica eseguita direttamente dall'utente interessato. Il proprietario accede alla procedura WEB utilizzando il suo codice fiscale e un codice OTP (codice consegnato in busta chiusa e a mano all'interessato dalla persona a cui è stato richiesto l'accreditamento). Terminata la fase di inizializzazione all'utente vengono assegnate le CAU che resteranno legate al suo codice fiscale indipendentemente dal ruolo associato.

Modalità di recupero delle credenziali smarrite

Qualora l'utente abbia fornito il suo cellulare personale, potrà ripristinare la password attraverso un sistema di SMS e OTP. Negli altri casi si procede tramite ticket HELPDESK e riconoscimento de visu.

Durata dell'accreditamento

L'accreditamento dura fino al giorno della scadenza impostata in fase di attivazione. Una volta terminato il periodo di accesso, l'utente non potrà accedere ad alcun servizio tranne che la posta elettronica. Nel caso di riattivazione (anche con diversa tipologia di rapporto), l'utente potrà nuovamente accedere ai servizi informatici con le medesime credenziali. La disattivazione di un utente avviene durante la notte ad opera degli script di sincronizzazione che marcano il profilo come non più attivo.

Disabilitazione utente

Non sono previste procedure di disattivazione utente se non per termine.

Cancellazione definitiva utente

L'utente non viene mai cancellato ma solo disattivato in seguito alla scadenza.

IL SISTEMA DI AUTENTICAZIONE E AUTORIZZAZIONE INTERNO

Ad oggi è attivo in UniSa un altro sistema di autenticazione che si basa sullo stesso sistema centralizzato qui descritto. Tecnicamente è un altro server IDP non collegato alla federazione e che veicola, oltre gli attributi raccomandati e obbligatori della federazione, tutta una seria di attributi specifici per i diversi SP.

In futuro non è esclusa la possibilità di unificare i due IDP in un unico servizio.

PARTECIPAZIONE AD ALTRE FEDERAZIONI

L'università di Salerno partecipa alla federazione EDUROAM esportando solo gli utenti di tipo STUDENTI e PERSONALE DIPENDENTE.