Università degli Studi di Palermo

DOPAU 2.0

Introduzione

La partecipazione alla Federazione IDEM abilita l'organizzazione partecipante a condividere le risorse on-line rese disponibili all'interno della comunità IDEM.
Al fine di assicurare che le asserzioni inviate dagli Identity Provider ai Service Provider siano sufficientemente robuste e fidate per garantire l'accesso alle risorse protette, si richiede all'organizzazione partecipante di compilare il DOPAU (DOcumento descrittivo del Processo di Accreditamento degli Utenti dell'Organizzazione).

Il DOPAU è un questionario che deve essere compilato da ogni organizzazione partecipante. Esso intende raccogliere informazioni riguardanti il sistema di Identity Management dell'ente. Le informazioni che verranno rilasciate saranno riservate alla Federazione IDEM e verranno trattate secondo quanto indicato nelle Nome di Partecipazione della Federazione IDEM La federazione si riserva la possibilità di utilizzare i dati in forma anonima e/o in maniera aggregata ai fini statistici.

Modalità di compilazione

Il questionario si suddivide in due parti:

- la prima parte riguarda domande relative ad ogni processo di accreditamento[1] e gestione delle identità che genera credenziali utilizzate per l'accesso a risorse federate.
  Il questionario riguarda esclusivamente il ciclo di vita delle identità che hanno accesso alle risorse delle federazione.
  E' necessario, quindi, prima di compilare questa parte che l'organizzazione partecipante individui tutti i processi di accreditamento presenti all'interno del suo ente finalizzati al rilascio di credenziali utili per accedere alle risorse federate. Per ogni processo individuato verranno poste delle domande volte a comprendere il funzionamento dello stesso. Esse saranno suddivise in due sezioni: *Informazioni sul processo di accreditamento, La gestione delle Identità*

- la seconda parte riguarda in generale il sistema di Identity Management dell'organizzazione e l'informazione all'utente e il consenso in relazione ai servizi accessibili con autenticazione federata

Tutte le domande sono obbligatorie. Quasi tutte le domande sono a risposta chiusa. Qualora la risposta ad una domanda non rientrasse tra quelle indicate si richiede di esplicitarla nelle note compilabili in fondo a ciascuna sezione.

Si sottolinea che le domande non trattano gli aspetti già previsti per legge ai sensi del Codice in materia di protezione dei dati personali il relazione all'Allegato B "Disciplinare tecnico in materia di misure minime di sicurezza" in quanto essi devono essere rispettati come obbligo di legge.

Compito dell'organizzazione sarà quello di una revisione periodica del DOPAU. Inoltre l'organizzazione ha il compito di modificare tempestivamente il contenuto del DOPAU qualora ci siano degli aggiornamenti sul sistema di Identity Management e sui processi di accreditamento indicati.

[1]Per processo di accreditamento si intende l'insieme delle fasi necessarie per la creazione dell'identità digitale

La Federazione Idem si riserva di effettuare, in accordo con l'organizzazione partecipante, dei controlli sulla veridicità delle risposte.

L'organizzazione partecipante (nella figura del Referente Organizzativo) assume la piena responsabilità di quanto indicato nel DOPAU.

Si ricorda infine che la compilazione del questionario può essere interrotta e salvata.

La compilazione del questionario richiede circa 30 minuti.

Glossario

DOPAU: DOcumento descrittivo del Processo di Accreditamento degli Utenti dell'Organizzazione
IdP: Identity Provider
OdA: Organizzazione di Appartenenza
pwd: password
RA: Registration Authority
SP: Service Provider

Questionario

Organizzazione/Ente: **Università degli Studi di Palermo**

Nome e cognome di chi compila il questionario: **Pietro Brignola**

Parte I – I processi di accreditamento
- Informazione sul processo di accreditamento
- La gestione delle Identità

Parte II – Il sistema di Identity Management
- L'informazione all'utente e il consenso
- Informazione sul sistema di Identity Management

Parte I

Quanti processi di accreditamento sono presenti nella tua Organizzazione di Appartenenza ("OdA")?

2 (due)

Elenca i processi di accreditamento individuati nella domanda n.1 qui di seguito:

1). Personale dipendente

2). Studenti

Processo di accreditamento 1)

1.1 INFORMAZIONE SUL PROCESSO DI ACCREDITAMENTO PER IL PERSONALE DIPENDENTE

1.1.1 Descrivere brevemente a quale categoria di utenza è rivolto (max 1000 parole).

Si tratta degli utenti i cui dati hanno come fonte di riferimento l'ufficio risorse umane e carriere e stipendi di Ateneo. In particolare si fa riferimento ad alcune categorie di personale:

- Docenti
- Docenti a contratto
- Supplenti docenti
- Ricercatori Universitari
- Personale T/A a tempo determinato ed a tempo indeterminato
- Titolari di assegni di ricerca
- Dottorandi
- Tutor

1.1.2 Esiste un ufficio/un referente (RA: Registration Authority) all'interno della tua OdA incaricato di effettuare gli accreditamenti per questa tipologia di utenti?

☐ Si, esiste una/delle persone designate che sono le uniche incaricate ad effettuare gli accreditamenti.
☐ No, ognuno si auto-accredita.
☒ L'accreditamento avviene in maniera automatica tramite il sistema di Identity Management a seguito di un'identificazione dell'utente da parte degli uffici amministrativi (Ufficio Risorse Umane, Segreteria Studenti, etc.) all'atto dell'inizio di un rapporto formale con l'OdA (es. assunzione, immatricolazione, etc.) anche se non finalizzata al rilascio delle credenziali.
☐ Ogni utente accreditato può effettuare l'accreditamento di altre persone (es. in caso di visitatore)
☐ Altro

1.1.3 La procedura di registrazione/accreditamento dell'utente avviene dopo che (più risposte possibili):

☒ La persona è stata identificata de visu attraverso un documento di identità personale.
☐ La persona è stata identificata sulla base dell'acquisizione dei dati di una carta di credito o di una SIM card.
☐ Senza alcun tipo di identificazione.
☐ Altro.

1.1.4 Esiste una policy e/o un documento descrittivo dei passi che devono essere eseguiti per effettuare l'identificazione?

☐ Si
☒ no

1.1.5 Quali tra gli attributi richiesti dalla Federazione IDEM (obbligatori, raccomandati o opzionali) vengono registrati e tenuti aggiornati nel tempo dall'OdA (più risposte possibili)?

	Nome LDAP	Origine	Descrizione	Stato
☒	**Sn**	LDAPv3 rfc4519	Cognome	raccomandato
☒	**givenName**	LDAPv3 rfc4519	Nome	raccomandato
☒	**Cn**	LDAPv3 rfc4519	Nome seguito da Cognome	raccomandato
☐	**preferredlanguage**	inetOrgPerson rfc2798	Lingua scritta o parlata preferita dal soggetto	opzionale
☐	**schacMotherTongue**	schac	Lingua madre del soggetto	opzionale
☐	**Title**	LDAPv3 rfc4519	Titolo nel contesto dell'organizzazione (es. "Direttore", "Responsabile Reparto X" ecc.)	opzionale
☐	**schacPersonalTitle**	schac	Titolo usato per salutare il soggetto. Es: Sig., Sig.ra, Dott., Prof.	opzionale
☐	**schacPersonalPosition**	LDAPv3 rfc4519	Il codice rappresentativo dell'inquadramento della persona all'interno dell'organizzazione	opzionale
	Nome LDAP	**Origine**	**Descrizione**	**Stato**
☐	**mail**	Cosine rfc4524	Indirizzo eMail	raccomandato
☒	**telephoneNumber**	LDAPv3 rfc4519	Recapito telefonico	opzionale
☐	**mobile**	Cosine rfc4524	Recapito cellulare	opzionale
☐	**facsimileTelephoneNumber**	LDAPv3 rfc4519	Recapito fax	opzionale
☐	**schacUserPresenceID**	schac	Recapiti relativi a diversi protocolli di rete	opzionale
☐	**eduPersonOrgDN**	eduPerson	Il Distinguished Name (DN) della entry che rappresenta l'organizzazione di appartenenza alla quale la persona è associata	opzionale

☐	**eduPersonOrgUnitDN**	eduPerson	Il Distinguished Name (DN) della entry che rappresenta l'unità organizzativa di appartenenza alla quale la persona è associata (ad esempio Dipartimento)	opzionale
	Nome LDAP	**Origine**	**Descrizione**	**Stato**
☒	**eduPersonScopedAffiliation**	eduPerson	Affiliazione secondo le convenzioni descritte nell'Appendice A del Documento: Specifiche Tecniche per la compilazione e l'uso degli attributi.	obbligatorio
☒	**eduPersonTargetedID**	eduPerson	Identificativi anonimi persistenti per l'utente relativi ai diversi Servizi	obbligatorio
☐	**eduPersonPrincipalName**	eduPerson	Identificativo unico persistente dell'utente	raccomandato
☐	**eduPersonEntitlement**	eduPerson	Uno o più URI (URN o URL)	concordati con il fornitore di servizi

1.1.6 Quali meccanismi di autenticazione sono implementati dall'OdA e utilizzati dall'Identity Provider (più risposte possibili)?

☒ username/password
☐ SmartCard
☐ SmartCardPKI (si viene autenticati attraverso una smartcard con inclusa una chiave privata e un PIN)
☐ Kerberos
☐ InternetProtocol (si viene autenticati attraverso l'utilizzo di un indirizzo IP)
☐ InternetProtocolPassword (si viene autenticati attraverso l'utilizzo di un indirizzo IP + una username/pwd)
☐ PGP (si viene autenticati tramite un firma digitale dove la chiave è validata come parte di un PGP Public Key Infrastructure)
☐ TimeSyncToken (si viene autenticati attraverso un token a tempo)
☐ TLSClient (si è autenticati mediante un certificato lato client utilizzando un trasporto sicuro SSL/TLS)
☐ X.509 (si viene autenticati mediante una firma digitale con una chiave validata come parte in un X.509 Public Key Infrastructured)
☐ Altro

1.1.7 Un utente può avere più identità digitali (e di conseguenza diverse credenziali) rilasciate dalla sua OdA (es. dipendente che è anche studente, ecc...)?

☐ Si
☒ No

1.1.8 Come avviene la consegna delle credenziali?

☐ vengono consegnate all'utente a mano/a voce dall'ufficio/persona preposta all'accreditamento

☐ vengono consegnate all'utente attraverso l'invio di una email dalla persona/ufficio preposto all'accreditamento

☐ vengono inviate all'utente per posta in busta chiusa

☒ altro. Vengono inviati un SMS ed una mail ai recapiti personali dichiarati in fase di identificazione dell'utente al fine di consentire l'attivazione delle credenziali:

- lo username viene generato automaticamente ed inviato sul recapito personale di telefonia mobile e sulla casella di posta elettronica. L'utenza, in questo momento, è sprovvista di password
- la prima impostazione della password avviene mediante procedura applicativa a partire dalla conoscenza di una One Time Password univocamente generata per l'utente e ad egli inviata mediante SMS e mail

1.1.9 E' possibile allegare un flusso che descriva il processo di accreditamento appena descritto

1.1.10 Indicare eventuali note aggiuntive che possano servire a completare le risposte sopra compilate

L'entità coinvolta nella gestione delle identità e relativa identificazione è costituita essenzialmente dall'ufficio del personale a cui è demandato il compito registrare sui sistemi informatici i dati relativi alle persone che instaurano un rapporto giuridico con l'Università per ciò che concerne quanto esposto al paragrafo 1.1.1. L'ufficio ha il compito di identificare la persona mediante un documento d'identità. A corredo dei dati anagrafici vengono acquisiti per dichiarazione spontanea dell'utente i dati circa l'indirizzo mail ed il numero di cellulare personali che vengono utilizzati successivamente dal sistema automatico di Identity Management. Nel momento in cui sul software utilizzato per la gestione dei dati (CSA) avviene una modifica, questa viene riportata sul database dell'anagrafica unica e dopo su LDAP nelle notti immediatamente successive.
In seguito alla stipula del contratto che instaura un rapporto tra l'Università e la persona, questa può connettersi ad al sito web di Ateneo che consente di eseguire gli step seguenti nell'ordine indicato:

- attivare il proprio account inserendo il codice fiscale
- ricevere via mail ed SMS (quelli personali citati sopra) lo username che è stato assegnato dal sistema
- impostare per la prima volta la password dopo avere inserito codice fiscale e username.

Normalmente lo username è costituito da una stringa composta dal nome legato al cognome mediante il carattere ".". Vengono eliminati eventuali lettere accentate, spazi e caratteri speciali. In caso di omonimia viene aggiunto un suffisso numerico progressivo in base all'ordine di attivazione dell'account.
La password può essere cambiata dopo il login sul portale di Ateneo mediante apposita funzionalità applicativa. Nel caso in cui il dipendente dimenticasse la propria password è possibile eseguire un "reset password" che consente di impostarla ex-novo; allo scopo, esiste apposita procedura applicativa che invia ai contatti personali (mail, cellulare) dell'utente le informazioni necessarie: queste hanno una validità temporale di otto ore. Sia il cambio che il reset della password hanno effetto immediato anche su LDAP.
Nel caso in cui si dimenticasse il proprio username, è possibile recuperarlo sempre tramite apposita funzionalità applicativa che fa uso, anche in questo caso, dei contatti personali dell'utente.
Le credenziali di accesso sono le medesime nel caso in cui il dipendente sia anche uno studente. Un utente non è mai cancellato dalla base di dati e/o da Ldap, ma una volta scaduti tutti i suoi incarichi e, per ciascun incarico scaduto, sono decorsi i mesi di policy di conservazione stabiliti da appositi regolamenti di Ateneo, i servizi messi a disposizione vengono disabilitati.

1.2 LA GESTIONE DELL'IDENTITA'

1.2.1 Nel caso in cui l'OdA fornisca all'utente credenziali del tipo username/password, dichiarare quali delle seguenti politiche di sicurezza sono implementate dal sistema di gestione delle identità (più risposte possibili):

☐ al primo accesso l'utente è obbligato a cambiare la password;
☒ un algoritmo, all'atto della sua impostazione, controlla il livello di robustezza della password, segnalandolo all'utente;
☒ all'atto del cambiamento della password, la nuova non può essere uguale alla vecchia
☐ blocco delle credenziali in caso di ripetuto inserimento di password non corretta
☒ Altro: al primo accesso l'utente è obbligato ad impostare la password;

1.2.2 All'utente sono fornite istruzioni relativamente alla sua responsabilità nella custodia e nel mantenimento della segretezza delle sue credenziali:

☐ Si
☒ No

1.2.3 Se si, quali misure sono adottate per rendere consapevole l'utente della riservatezza e dell'importanza delle credenziali? (più risposte possibili)

☐ Formazione per il personale neoassunto o dei nuovi iscritti
☐ L'utente firma un'assunzione di responsabilità
☐ Ci sono espliciti riferimenti in regolamento/i dell'OdA
☐ Ci sono diverse comunicazioni in occasione di specifici eventi
☐ Ci sono comunicazioni periodiche
☐ Esiste documentazione online che tratta questi argomenti
☐ Vengono svolti seminari/corsi attinenti la problematica aperti a personale e studenti
☐ Altro

1.2.4 Esiste una policy relativa alle gestione delle credenziali?

☐ si, è pubblicata su web
☐ si, è fornita all'utente contestualmente all'accreditamento
☐ si, ma non è pubblicata
☒ no
☐ altro

1.2.5 Con periodicità almeno annuale viene effettuata una verifica (audit) dell'aderenza dell'identità digitale rispetto allo stato dell'utente?

☐ Si, automaticamente il sistema di gestione dell'identità verifica le identità digitale rispetto alle fonte autoritative
☐ Si, manualmente da uno o più incaricati
☐ Si, in modalità mista automatica e manuale in base alle categorie di utenti
☒ No
☐ Altro

1.2.8 Il sistema di gestione delle identità consente di discriminare gruppi di utenti in base al livello della qualità del riconoscimento effettuato all'atto del rilascio delle credenziali?

☐ Si, in caso di riconoscimento de visu da una RA
☐ si, in caso di riconoscimento tramite numero cellulare
☒ No

1.2.9 Quanto dura l'accreditamento, cioè quando avviene la disabilitazione delle credenziali?

☐ Avviene al termine del rapporto di lavoro con l'OdA oppure al termine del corso di studi (perché si è laureato)
☐ Non vengono mai disabilitate
☐ Vengono disabilitate dopo n mesi della data di cessazione del rapporto di lavoro con l'OdA o dopo n mesi dal termine del corso di studi (perché si è laureato)
☐ Vengono disabilitate a seguito di una rinuncia esplicita (per uno studente)
☐ Vengono disabilitate a seguito di una rinuncia implicita, ovvero dopo n mesi che non ha più sostenuto esami e/o non ha più pagato le tasse
☒ Altro: Le credenziali non vengono disattivate mai, ma in funzione della data di scadenza del ruolo rivestito in Ateneo vengono disabilitati i relativi servizi in riferimento ai regolamenti dell'OdA

1.2.10 L'utente viene avvisato dell'imminente scadenza/disabilitazione dell'account?
☐ Si
☒ No

1.2.11 Esiste la cancellazione definitiva dell'utente dal sistema di accreditamento?
☐ Si, in automatico a seguito della sua disattivazione/disabilitazione
☐ Si, avviene manualmente ogni tanto da un ufficio incaricato a seguito dalla sua disattivazione/disabilitazione
☒ L'utente non viene mai cancellato dal sistema di accreditamento
☐ Altro

1.2.12 Indicare eventuali note aggiuntive che possano servire a completare le risposte sopra compilate
Le informazioni relative agli utenti, come il ruolo rivestito nell'Organizzazione e le relative credenziali utente (la coppia di valori username/password), sono immagazzinati su un database che contiene solo dati che dipendono da altre fonti. I dati dalle fonti autoritative sono processati ogni notte. L'unica informazione che viene aggiornata in tempo reale è relativa al reset/cambio password per cui avviene un allineamento contestuale su LDAP.

Parte II

2.1 L'informazione all'utente e il consenso

2.1.1 L'OdA informa gli utenti della disponibilità di servizi accessibili con autenticazione federata? (più risposte possibili)

- [x] Si, mediante pagina web dedicata ai servizi di autenticazione federata
- [ ] Si, mediante la distribuzione di materiale cartaceo
- [ ] Si, mediante eventi informativi/divulgativi
- [ ] No

2.1.2 L'OdA informa gli utenti di quali siano le federazioni di identità a cui partecipa? (più risposte possibili)

- [x] Si, mediante una pagina web dedicata ai servizi di autenticazione federata
- [ ] Si, mediante la distribuzione di materiale cartaceo
- [ ] Si, mediante eventi informativi/divulgativi
- [ ] No
- [ ] Altro

2.1.3 L'OdA informa gli utenti, anche in maniera semplificata, dei meccanismi di funzionamento dei sistemi federati (ad es. rilascio degli attributi da IdP a SP, eventuali rischi connessi, ecc.)? (più risposte possibili)

- [x] Si, mediante una pagina web dedicata ai servizi di autenticazione federata
- [ ] Si, mediante la distribuzione di materiale cartaceo informativo/divulgativo
- [ ] Si, mediante eventi informativi/divulgativi
- [ ] No
- [ ] Altro

2.1.4. L'OdA informa l'utente sui dati personali che l'Identity Provider trasferirà ad uno specifico Service Provider di interesse per l'utente stesso? (più risposte possibili)

- [x] Si, mediante un' informativa disponibile su di una pagina web dedicata ai servizi di autenticazione federata
- [ ] Si, mediante un' informativa su di una pagina web dedicata raggiungibile dalla pagina di login dell'Identity Provider o direttamente disponibile su quest'ultima
- [ ] Si, in maniera dinamica all'atto del primo accesso al Service Provider, mediante l'uso di un meccanismo di visualizzazione degli attributi tipo uApprove o Consent
- [ ] Si, distribuendo agli utenti un'informativa cartacea
- [ ] No
- [ ] Altro

2.1.5. L'OdA, ove questo sia previsto dal D.Lgs. 196/2003, chiede all'utente il consenso al trasferimento dei suoi dati personali dall'Identity Provider ai Service Provider federati di interesse per l'utente stesso? (più risposte possibili)

- [ ] Si, mediante un'accettazione esplicita rilasciata on line tramite applicazione web con accesso autenticato
- [ ] Si, in maniera dinamica all'atto del primo accesso al Service Provider, mediante l'uso di un meccanismo di visualizzazione degli attributi tipo uApprove o Consent
- [ ] Si, facendo firmare agli utenti un modulo di consenso cartaceo
- [x] No
- [ ] Altro

2.1.6 Indicare eventuali note aggiuntive che possano servire a completare le risposte sopra compilate

2.2 Informazioni sul sistema di Identity Management

2.2.1 La policy dell'OdA permette di rilasciare gli attributi che i Service Provider federati dichiarano necessari al funzionamento del servizio?

☐ si, se il servizio viene erogato dall'Italia
☐ si, se il servizio viene erogato dall'Europa
☒ si, se il Service Provider dichiara di accettare la direttiva europea sul trattamento dei dati personali
☐ no

2.2.2 La policy dell'OdA permette di rilasciare gli attributi che i Service Provider federati dichiarano non necessari (opzionali) al funzionamento del servizio?

☐ si, se il servizio viene erogato dall'Italia
☐ si, se il servizio viene erogato dall'Europa
☒ si, se il Service Provider dichiara di accettare la direttiva europea sul trattamento dei dati personali
☐ no

2.2.3 Quali misure sono adottate per garantire la continuità del servizio del sistema di autenticazione e autorizzazione (scelte multiple)?

☐ Infrastruttura fault tolerant
☒ Piano per disaster recovery
☐ Istanze multiple dell'IdP
☐ Altro

2.2.4 Gli interventi di manutenzione che comportano interruzioni o variazioni del servizio sono pianificati e gli utenti preavvisati?

☒ Si
☐ No

2.2.5 I messaggi che restituisce l'IdP all'utente in caso di errore o malfunzionamento sono:

☒ legati al tipo di errore (es. si inserisce la pwd errata l'IdP restituisce un messaggio tipo "utenze e/o pwd errata")
☐ riportano l'indicazione di come procedere, in particolare i contatti di riferimento (es. indirizzo email, pagina web)
☐ Altro

2.2.6 Le credenziali che vengono mantenute dal sistemi di Identity Management sono sempre trasmesse in modalità sicura e crittografata?

☒ Si
☐ No, non sempre

2.2.7 Esistono applicazioni esterne all'OdA che utilizzano direttamente la directory istituzionale (ad esempio Ldap) e non l'Identity Provider?

☒ Si
☐ No

Processo di accreditamento 2

3.1 INFORMAZIONE SUL PROCESSO DI ACCREDITAMENTO PER GLI STUDENTI

3.1.1 Descrivere brevemente a quale categoria di utenza è rivolto (max 1000 parole).

Si tratta degli utenti i cui dati provengono dalle segreterie studenti di Ateneo. In particolare si fa riferimento ad alcune categorie del "mondo studenti":

- Studente di corso di studio
- Studente corso singolo
- Studente di corso di specializzazione
- Studenti di Dottorato
- Studenti stranieri incoming
- Studenti di TFA
- Studenti con titolo conseguito

3.1.2 Esiste un ufficio/un referente (RA: Registration Authority) all'interno della tua OdA incaricato di effettuare gli accreditamenti per questa tipologia di utenti?

☐ Si, esiste una/delle persone designate che sono le uniche incaricate ad effettuare gli accreditamenti.
☐ No, ognuno si auto-accredita.
☒ L'accreditamento avviene in maniera automatica tramite il sistema di Identity Management a seguito di un'identificazione dell'utente da parte degli uffici amministrativi (Ufficio Risorse Umane, Segreteria Studenti, etc.) all'atto dell'inizio di un rapporto formale con l'OdA (es. assunzione, immatricolazione, etc.) anche se non finalizzata al rilascio delle credenziali.
☐ Ogni utente accreditato può effettuare l'accreditamento di altre persone (es. in caso di visitatore)
☐ Altro

3.1.3 La procedura di registrazione/accreditamento dell'utente avviene dopo che (più risposte possibili):

☒ la persona è stata identificata de visu attraverso un documento di identità personale.
☐ la persona è stata identificata sulla base dell'acquisizione dei dati di una carta di credito o di una SIM card.
☐ senza alcun tipo di identificazione.
☐ Altro.

3.1.4 Esiste una policy e/o un documento descrittivo dei passi che devono essere eseguiti per effettuare l'identificazione?

☐ Si
☒ no

3.1.5 Quali tra gli attributi richiesti dalla Federazione IDEM (obbligatori, raccomandati o opzionali) vengono registrati e tenuti aggiornati nel tempo dall'OdA (più risposte possibili)?

	Nome LDAP	Origine	Descrizione	Stato
☒	**Sn**	LDAPv3 rfc4519	Cognome	raccomandato

☒ **givenName**	LDAPv3 rfc4519	Nome	raccomandato
☒ **Cn**	LDAPv3 rfc4519	Nome seguito da Cognome	raccomandato
☐ **preferredlanguage**	inetOrgPerson rfc2798	Lingua scritta o parlata preferita dal soggetto	opzionale
☐ **schacMotherTongue**	schac	Lingua madre del soggetto	opzionale
☐ **Title**	LDAPv3 rfc4519	Titolo nel contesto dell'organizzazione (es. "Direttore", "Responsabile Reparto X" ecc.)	opzionale
☐ **schacPersonalTitle**	schac	Titolo usato per salutare il soggetto. Es: Sig., Sig.ra, Dott., Prof.	opzionale
☐ **schacPersonalPosition**	LDAPv3 rfc4519	Il codice rappresentativo dell'inquadramento della persona all'interno dell'organizzazione	opzionale
Nome LDAP	**Origine**	**Descrizione**	**Stato**
☐ **mail**	Cosine rfc4524	Indirizzo eMail	raccomandato
☒ **telephoneNumber**	LDAPv3 rfc4519	Recapito telefonico	opzionale
☐ **mobile**	Cosine rfc4524	Recapito cellulare	opzionale
☐ **facsimileTelephoneNumber**	LDAPv3 rfc4519	Recapito fax	opzionale
☐ **schacUserPresenceID**	schac	Recapiti relativi a diversi protocolli di rete	opzionale
☐ **eduPersonOrgDN**	eduPerson	Il Distinguished Name (DN) della entry che rappresenta l'organizzazione di appartenenza alla quale la persona è associata	opzionale
☐ **eduPersonOrgUnitDN**	eduPerson	Il Distinguished Name (DN) della entry che rappresenta l'unità organizzativa di appartenenza alla quale la persona è associata (ad esempio Dipartimento)	opzionale

	Nome LDAP	Origine	Descrizione	Stato
☒	**eduPersonScopedAffiliation**	eduPerson	Affiliazione secondo le convenzioni descritte nell'Appendice A del Documento: Specifiche Tecniche per la compilazione e l'uso degli attributi.	obbligatorio
☒	**eduPersonTargetedID**	eduPerson	Identificativi anonimi persistenti per l'utente relativi ai diversi Servizi	obbligatorio
☐	**eduPersonPrincipalName**	eduPerson	Identificativo unico persistente dell'utente	raccomandato
☐	**eduPersonEntitlement**	eduPerson	Uno o più URI (URN o URL)	concordati con il fornitore di servizi

3.1.6 Quali meccanismi di autenticazione sono implementati dall'OdA e utilizzati dall'Identity Provider (più risposte possibili)?

☒ username/password
☐ SmartCard
☐ SmartCardPKI (si viene autenticati attraverso una smartcard con inclusa una chiave privata e un PIN)
☐ Kerberos
☐ InternetProtocol (si viene autenticati attraverso l'utilizzo di un indirizzo IP)
☐ InternetProtocolPassword (si viene autenticati attraverso l'utilizzo di un indirizzo IP + una username/pwd)
☐ PGP (si viene autenticati tramite un firma digitale dove la chiave è validata come parte di un PGP Public Key Infrastructure)
☐ TimeSyncToken (si viene autenticati attraverso un token a tempo)
☐ TLSClient (si è autenticati mediante un certificato lato client utilizzando un trasporto sicuro SSL/TLS)
☐ X.509 (si viene autenticati mediante una firma digitale con una chiave validata come parte in un X.509 Public Key Infrastructured)
☐ Altro

3.1.7 Un utente può avere più identità digitali (e di conseguenza diverse credenziali) rilasciate dalla sua OdA (es. dipendente che è anche studente, ecc...)?

☐ Si
☒ No

3.1.8 Come avviene la consegna delle credenziali?

☐ vengono consegnate all'utente a mano/a voce dall'ufficio/persona preposta all'accreditamento
☐ vengono consegnate all'utente attraverso l'invio di una email dalla persona/ufficio preposto all'accreditamento
☐ vengono inviate all'utente per posta in busta chiusa

☒ altro. Viene inviata una mail al recapito personale dichiarato in fase di registrazione dell'utente al fine di consentire l'attivazione delle credenziali:

- lo username viene generato automaticamente ed inviato sul recapito personale di posta elettronica. L'utenza al momento è sprovvista di password
- la prima impostazione della password avviene mediante procedura applicativa a partire dalla conoscenza di una One Time Password univocamente generata per l'utente e ad egli inviata tramite mail

3.1.9 E' possibile allegare un flusso che descriva il processo di accreditamento appena descritto

3.1.10 Indicare eventuali note aggiuntive che possano servire a completare le risposte sopra compilate

Le entità coinvolte nella gestione delle identità e relativa identificazione sono costituite rispettivamente dal portale studenti di Ateneo e dagli uffici delle segreterie studenti.
Il processo è costituito essenzialmente dai seguenti step successivi:

- Registrazione dell'utente sul portale studenti di Ateneo (a corredo dei dati anagrafici vengono richieste le informazioni circa l'indirizzo mail ed il numero di cellulare personali che vengono utilizzati successivamente dal sistema automatico di Identity Management)
- Invio mediante mail all'indirizzo di posta di cui al punto precedente dello username generato dal sistema e link per la conferma / attivazione dell'account.
- Registrazione delle modifiche sulla base dati dell'anagrafica unica di Ateneo
- Registrazione delle modifiche su LDAP (nella notte successiva)
- Avvio on line da parte dello studente di una pratica di iscrizione presso un corso dell'Ateneo
- Pagamento delle tasse
- "Perfezionamento" pratica in segreteria studenti con contestuale identificazione de visu e mediante documento d'identità.

Normalmente lo username è costituito da una stringa composta dal nome legato al cognome mediante il carattere ".". Vengono eliminati eventuali lettere accentate, spazi e caratteri speciali. In caso di omonimia viene aggiunto un suffisso numerico progressivo in base all'ordine di registrazione.
La password può essere cambiata dopo il login sul portale studenti dell'Ateneo mediante apposita funzionalità applicativa. Nel caso in cui lo studente dimenticasse la propria password è possibile eseguire un reset password impostandola ex-novo mediante apposita procedura che invia ai contatti personali (mail, cellulare) le informazioni necessarie. Le informazioni contenute nei messaggi hanno una validità temporale di otto ore. Sia il cambio che il reset della password hanno effetto immediato anche su LDAP.
Le credenziali di accesso sono le medesime nel caso in cui lo studente sia anche un dipendente. Un utente non è mai cancellato dalla base di dati e/o da ldap, ma una volta scaduti tutti i suoi ruoli in Ateneo e, per ciascun incarico scaduto, sono decorsi i mesi di policy di conservazione stabiliti da appositi regolamenti di Ateneo, i servizi messi a disposizione vengono disabilitati.

3.2 LA GESTIONE DELL'IDENTITA'

3.2.1 Nel caso in cui l'OdA fornisca all'utente credenziali del tipo username/password, dichiarare quali delle seguenti politiche di sicurezza sono implementate dal sistema di gestione delle identità (più risposte possibili):

☐ al primo accesso l'utente è obbligato a cambiare la password;
☒ un algoritmo, all'atto della sua impostazione, controlla il livello di robustezza della password, segnalandolo all'utente;
☒ all'atto del cambiamento della password, la nuova non può essere uguale alla vecchia
☐ blocco delle credenziali in caso di ripetuto inserimento di password non corretta
☒ Altro: al primo accesso l'utente è obbligato ad impostare la password;

3.2.2 All'utente sono fornite istruzioni relativamente alla sua responsabilità nella custodia e nel mantenimento della segretezza delle sue credenziali:

☒ Si
☐ No

3.2.3 Se si, quali misure sono adottate per rendere consapevole l'utente della riservatezza e dell'importanza delle credenziali? (più risposte possibili)

☐ Formazione per il personale neoassunto o dei nuovi iscritti
☐ L'utente firma un'assunzione di responsabilità
☐ Ci sono espliciti riferimenti in regolamento/i dell'OdA
☐ Ci sono diverse comunicazioni in occasione di specifici eventi
☐ Ci sono comunicazioni periodiche
☐ Esiste documentazione online che tratta questi argomenti
☐ Vengono svolti seminari/corsi attinenti la problematica aperti a personale e studenti
☒ Altro. Costituisce parte integrante della pratica di iscrizione / immatricolazione un disclaimer informativo che l'utente accetta sottoscrivendo la pratica.

3.2.4 Esiste una policy relativa alle gestione delle credenziali?

☐ si, è pubblicata su web
☐ si, è fornita all'utente contestualmente all'accreditamento
☐ si, ma non è pubblicata
☒ no
☐ altro

3.2.5 Con periodicità almeno annuale viene effettuata una verifica (audit) dell'aderenza dell'identità digitale rispetto allo stato dell'utente?

☐ Si, automaticamente il sistema di gestione dell'identità verifica le identità digitale rispetto alle fonte autoritative
☐ Si, manualmente da uno o più incaricati
☐ Si, in modalità mista automatica e manuale in base alle categorie di utenti
☒ No
☐ Altro

3.2.8 Il sistema di gestione delle identità consente di discriminare gruppi di utenti in base al livello della qualità del riconoscimento effettuato all'atto del rilascio delle credenziali?

☐ Si, in caso di riconoscimento de visu da una RA
☐ Si, in caso di riconoscimento tramite numero cellulare
☒ No

3.2.9 Quanto dura l'accreditamento, cioè quando avviene la disabilitazione delle credenziali?

☐ Avviene al termine del rapporto di lavoro con l'OdA oppure al termine del corso di studi (perché si è laureato)
☐ Non vengono mai disabilitate
☐ Vengono disabilitate dopo n mesi della data di cessazione del rapporto di lavoro con l'OdA o dopo n mesi dal termine del corso di studi (perché si è laureato)
☐ Vengono disabilitate a seguito di una rinuncia esplicita (per uno studente)
☐ Vengono disabilitate a seguito di una rinuncia implicita, ovvero dopo n mesi che non ha più sostenuto esami e/o non ha più pagato le tasse
☒ Altro: Le credenziali non vengono disattivate mai, ma in funzione della data di scadenza del ruolo rivestito in Ateneo vengono disabilitati i relativi servizi in riferimento ai regolamenti interni.

3.2.10 L'utente viene avvisato dell'imminente scadenza/disabilitazione dell'account?

☐ Si
☒ No

3.2.11 Esiste la cancellazione definitiva dell'utente dal sistema di accreditamento?

☐ Si, in automatico a seguito della sua disattivazione/disabilitazione
☐ Si, avviene manualmente ogni tanto da un ufficio incaricato a seguito dalla sua disattivazione/disabilitazione
☒ L'utente non viene mai cancellato dal sistema di accreditamento
☐ Altro

3.2.12 Indicare eventuali note aggiuntive che possano servire a completare le risposte sopra compilate

Le informazioni relative agli utenti, come il ruolo rivestito nell'Organizzazione e le relative credenziali utente (la coppia di valori username/password), sono immagazzinati su un database che contiene solo dati che dipendono da altre fonti. I dati dalle fonti autoritative sono processati ogni notte. L'unica informazione che viene aggiornata in tempo reale è relativa al reset/cambio password per cui avviene un allineamento contestuale su LDAP.

Parte II

4.1 L'informazione all'utente e il consenso

4.1.1 L'OdA informa gli utenti della disponibilità di servizi accessibili con autenticazione federata? (più risposte possibili)

- [x] Si, mediante pagina web dedicata ai servizi di autenticazione federata
- [ ] Si, mediante la distribuzione di materiale cartaceo
- [ ] Si, mediante eventi informativi/divulgativi
- [ ] No

4.1.2 L'OdA informa gli utenti di quali siano le federazioni di identità a cui partecipa? (più risposte possibili)

- [x] Si, mediante una pagina web dedicata ai servizi di autenticazione federata
- [ ] Si, mediante la distribuzione di materiale cartaceo
- [ ] Si, mediante eventi informativi/divulgativi
- [ ] No
- [ ] Altro

4.1.3 L'OdA informa gli utenti, anche in maniera semplificata, dei meccanismi di funzionamento dei sistemi federati (ad es. rilascio degli attributi da IdP a SP, eventuali rischi connessi, ecc.)? (più risposte possibili)

- [x] Si, mediante una pagina web dedicata ai servizi di autenticazione federata
- [ ] Si, mediante la distribuzione di materiale cartaceo informativo/divulgativo
- [ ] Si, mediante eventi informativi/divulgativi
- [ ] No
- [ ] Altro

4.1.4. L'OdA informa l'utente sui dati personali che l'Identity Provider trasferirà ad uno specifico Service Provider di interesse per l'utente stesso? (più risposte possibili)

- [x] Si, mediante un' informativa disponibile su di una pagina web dedicata ai servizi di autenticazione federata
- [ ] Si, mediante un' informativa su di una pagina web dedicata raggiungibile dalla pagina di login dell'Identity Provider o direttamente disponibile su quest'ultima
- [ ] Si, in maniera dinamica all'atto del primo accesso al Service Provider, mediante l'uso di un meccanismo di visualizzazione degli attributi tipo uApprove o Consent
- [ ] Si, distribuendo agli utenti un'informativa cartacea
- [ ] No
- [ ] Altro

4.1.5. L'OdA, ove questo sia previsto dal D.Lgs. 196/2003, chiede all'utente il consenso al trasferimento dei suoi dati personali dall'Identity Provider ai Service Provider federati di interesse per l'utente stesso? (più risposte possibili)

- [ ] Si, mediante un'accettazione esplicita rilasciata on line tramite applicazione web con accesso autenticato
- [ ] Si, in maniera dinamica all'atto del primo accesso al Service Provider, mediante l'uso di un meccanismo di visualizzazione degli attributi tipo uApprove o Consent
- [ ] Si, facendo firmare agli utenti un modulo di consenso cartaceo
- [x] No
- [ ] Altro

4.1.6 Indicare eventuali note aggiuntive che possano servire a completare le risposte sopra compilate

4.2 Informazioni sul sistema di Identity Management

4.2.1 La policy dell'OdA permette di rilasciare gli attributi che i Service Provider federati dichiarano necessari al funzionamento del servizio?

- [ ] si, se il servizio viene erogato dall'Italia
- [ ] si, se il servizio viene erogato dall'Europa
- [x] si, se il Service Provider dichiara di accettare la direttiva europea sul trattamento dei dati personali
- [ ] no

4.2.2 La policy dell'OdA permette di rilasciare gli attributi che i Service Provider federati dichiarano non necessari (opzionali) al funzionamento del servizio?

- [ ] si, se il servizio viene erogato dall'Italia
- [ ] si, se il servizio viene erogato dall'Europa
- [x] si, se il Service Provider dichiara di accettare la direttiva europea sul trattamento dei dati personali
- [ ] no

4.2.3 Quali misure sono adottate per garantire la continuità del servizio del sistema di autenticazione e autorizzazione (scelte multiple)?

- [ ] Infrastruttura fault tolerant
- [x] Piano per disaster recovery
- [ ] Istanze multiple dell'IdP
- [ ] Altro

4.2.4 Gli interventi di manutenzione che comportano interruzioni o variazioni del servizio sono pianificati e gli utenti preavvisati?

- [x] Si
- [ ] No

4.2.5 I messaggi che restituisce l'IdP all'utente in caso di errore o malfunzionamento sono:

- [x] legati al tipo di errore (es. si inserisce la pwd errata l'IdP restituisce un messaggio tipo "utenze e/o pwd errata")
- [ ] riportano l'indicazione di come procedere, in particolare i contatti di riferimento (es. indirizzo email, pagina web)
- [ ] Altro

4.2.6 Le credenziali che vengono mantenute dal sistemi di Identity Management sono sempre trasmesse in modalità sicura e crittografata?

- [x] Si
- [ ] No, non sempre

4.2.7 Esistono applicazioni esterne all'OdA che utilizzano direttamente la directory istituzionale (ad esempio Ldap) e non l'Identity Provider?

- [x] Si
- [ ] No