

## **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 Note 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<sup>1</sup> 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.

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.

<sup>1</sup> Per processo di accreditamento si intende l'insieme delle fasi necessarie per la creazione dell'identità digitale

## 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 Catania

Nome e cognome di chi compila il questionario: Concetta Mirabella

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")? 1

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

- (1). Dipendenti dell'Ateneo;

#### 1.1 INFORMAZIONE SUL PROCESSO DI ACCREDITAMENTO

##### 1.1 Categoria di utenti: (1). Dipendenti dell'Ateneo

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

La categoria "dipendenti dell'Ateneo" si riferisce: al personale tecnico-amministrativo a tempo determinato e indeterminato; ai collaboratori tecnico-amministrativi; al personale docente di ruolo e a contratto; ai ricercatori e collaboratori alla didattica.

**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?**

a.	Si, esiste una/delle persone designate che sono le uniche incaricate ad effettuare gli accreditamenti.	<b>X</b>
b.	No, ognuno si auto-accredita.	
c.	L'accredimento 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.	
d.	Ogni utente accreditato può effettuare l'accredimento di altre persone (es. in caso di visitatore).	
e.	Altro.	

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

a.	la persona è stata identificata de visu attraverso un documento di identità personale.	
b.	la persona è stata identificata sulla base dell'acquisizione dei dati di una carta di credito o di una SIM card.	
c.	senza alcun tipo di identificazione.	
d.	Altro.	<b>X</b>

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

a.	si	<b>X</b>
b.	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
<b>X</b>	Sn	LDAPv3 rfc4519	Cognome	raccomandato
<b>X</b>	givenName	LDAPv3 rfc4519	Nome	raccomandato
<b>X</b>	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

	<b>schacPersonalTitle</b>	schac	Titolo usato per salutare il soggetto. Es: Sig., Sig.ra, Dott., Prof.	opzionale
	<b>schacPersonalPosition</b>	LDAPv3 rfc4519	Il codice rappresentativo dell'inquadramento della persona all'interno dell'organizzazione	opzionale
	<b>Nome LDAP</b>	<b>Origine</b>	<b>Descrizione</b>	<b>Stato</b>
<b>X</b>	<b>mail</b>	Cosine rfc4524	Indirizzo eMail	raccomandato
<b>X</b>	<b>telephoneNumber</b>	LDAPv3 rfc4519	Recapito telefonico	opzionale
	<b>mobile</b>	Cosine rfc4524	Recapito cellulare	opzionale
	<b>facsimileTelephoneNumber</b>	LDAPv3 rfc4519	Recapito fax	opzionale
	<b>schacUserPresenceID</b>	schac	Recapiti relativi a diversi protocolli di rete	opzionale
	<b>eduPersonOrgDN</b>	eduPerson	Il Distinguished Name (DN) della entry che rappresenta l'organizzazione di appartenenza alla quale la persona è associata	opzionale
	<b>eduPersonOrgUnitDN</b>	eduPerson	Il Distinguished Name (DN) della entry che rappresenta l'unità organizzativa di appartenenza alla quale la persona è associata (ad esempio Dipartimento)	opzionale
	<b>Nome LDAP</b>	<b>Origine</b>	<b>Descrizione</b>	<b>Stato</b>
<b>X</b>	<b>eduPersonScopedAffiliation</b>	eduPerson	Affiliazione secondo le convenzioni descritte nell'Appendice A del Documento: Specifiche Tecniche per la compilazione e l'uso degli attributi.	obbligatorio
<b>X</b>	<b>eduPersonTargetedID</b>	eduPerson	Identificativi anonimi persistenti per l'utente relativi ai diversi Servizi	obbligatorio
<b>X</b>	<b>eduPersonPrincipalName</b>	eduPerson	Identificativo unico persistente dell'utente	raccomandato
	<b>eduPersonEntitlement</b>	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)?**

a.	username/password.	<b>X</b>
b.	SmartCard	
c.	SmartCardPKI (si viene autenticati attraverso una smartcard con inclusa una chiave privata e un PIN)	
d.	Kerberos	
e.	InternetProtocol (si viene autenticati attraverso l'utilizzo di un indirizzo IP)	
f.	InternetProtocolPassword (si viene autenticati attraverso l'utilizzo di un indirizzo IP + una username/pwd)	

g.	PGP (si viene autenticati tramite un firma digitale dove la chiave è validata come parte di un PGP Public Key Infrastructure)	
h.	TimeSyncToken (si viene autenticati attraverso un token a tempo)	
i.	TLSCient (si è autenticati mediante un certificato lato client utilizzando un trasporto sicuro SSL/TLS)	
l.	X.509 (si viene autenticati mediante una firma digitale con una chiave validata come parte in un X.509 Public Key Infrastructured)	
m.	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...)?**

a.	si	
b.	no	<b>X</b>

**1.1.8 Come avviene la consegna delle credenziali?**

a.	vengono consegnate all'utente a mano/a voce dall'ufficio/persona preposta all'accreditamento	
b.	vengono consegnate all'utente attraverso l'invio di una email dalla persona/ufficio preposto all'accreditamento	
c.	vengono inviate all'utente per posta in busta chiusa	
d.	Altro	<b>X</b>

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

Per gestire la categoria dei *dipendenti dell'Ateneo*, il sistema applicativo utilizza il Servizio Centralizzato di Autenticazione (C.A.S.) per l'accesso ai servizi online erogati dall'ateneo.

L'utente ottiene il rilascio delle credenziali (UserID e password) a conclusione della procedura web di seguito descritta:

- 1) L'utente compila il modulo preposto con i propri dati personali. Contestualmente provvede all'inserimento di un codice PUK (Personal Unblocking Key) che sarà utilizzato come password per il primo accesso.
- 2) A seguito dell'inserimento e successiva conferma dei dati inseriti, verrà generato il modulo da stampare, che andrà firmato e consegnato personalmente ad un incaricato preposto per l'identificazione, insieme ad una copia di un valido documento di riconoscimento.
- 3) A conclusione della procedura, le credenziali saranno abilitate.

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

Nessuna nota aggiuntiva.

## 1.2 LA GESTIONE DELL'IDENTITÀ

**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):**

a.	al primo accesso l'utente è obbligato a cambiare la password	<b>X</b>
b.	un algoritmo, all'atto della sua impostazione, controlla il livello di robustezza della password, segnalandolo all'utente	
c.	all'atto del cambiamento della password, la nuova non può essere uguale alla vecchia	<b>X</b>
d.	blocco delle credenziali in caso di ripetuto inserimento di password non corretta	
e.	Altro	<b>X</b>

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

a.	si	<b>X</b>
b.	no	

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

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

**1.2.4 Esiste una policy relativa alle gestione delle credenziali?**

a.	Si, è pubblicata su web	<b>X</b>
b.	Si, è fornita all'utente contestualmente all'accreditamento	
c.	Si, ma non è pubblicata	
d.	No	
e.	Altro	

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

a.	Si, automaticamente il sistema di gestione dell'identità verifica le identità digitale rispetto alle fonte autoritative	
b.	Si, manualmente da uno o più incaricati	
c.	Si, in modalità mista automatica e manuale in base alle categorie di utenti	<b>X</b>
d.	No	
e.	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?**

a.	Si, in caso di riconoscimento de visu da una RA	
b.	si, in caso di riconoscimento tramite numero cellulare	
c.	No	<b>X</b>

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

a.	Avviene al termine del rapporto di lavoro con l'Oda oppure al termine del corso di studi (perché si è laureato)	<b>X</b>
b.	Non vengono mai disabilite	
c.	Vengono disabilite 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)	
d.	Vengono disabilite a seguito di una rinuncia esplicita (per uno studente)	
e.	Vengono disabilite a seguito di una rinuncia implicita, ovvero dopo n mesi che non ha più sostenuto esami e/o non ha più pagato le tasse	
f.	Altro	

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

a.	si	
b.	no	<b>X</b>

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

a.	Si, in automatico a seguito della sua disattivazione/disabilitazione	
b.	Si, avviene manualmente ogni tanto da un ufficio incaricato a seguito dalla sua disattivazione/disabilitazione	
c.	L'utente non viene mai cancellato dal sistema di accreditamento	<b>X</b>
d.	Altro	

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

Il codice PUK (Personal Unblocking Key) scelto dall'utente all'atto della richiesta delle credenziali sarà utilizzato come password per il primo accesso. La perdita del codice PUK, esigerà una nuova richiesta di rilascio delle credenziali.

In occasione del primo accesso e alla scadenza della password prevista ogni sei mesi, l'utente è obbligato alla modifica della password che non potrà essere uguale all'ultima in uso. In caso di smarrimento il PUK potrà essere utilizzato come codice di riattivazione.

Il codice PUK e la password di accesso sono strettamente personali. L'utente è responsabile delle credenziali ricevute e si impegna, all'atto della registrazione, a non divulgarle a terzi e ad astenersi da qualunque uso improprio delle stesse e dei servizi a cui avrà accesso.

\*\*\*\*\*

## 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)

a.	Si, mediante pagina web dedicata ai servizi di autenticazione federata	<input checked="" type="checkbox"/>
b.	Si, mediante la distribuzione di materiale cartaceo	<input type="checkbox"/>
c.	Si, mediante eventi informativi/divulgativi	<input type="checkbox"/>
d.	No	<input type="checkbox"/>

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

a.	Si, mediante una pagina web dedicata ai servizi di autenticazione federata	<input checked="" type="checkbox"/>
b.	Si, mediante la distribuzione di materiale cartaceo	<input type="checkbox"/>
c.	Si, mediante eventi informativi/divulgativi	<input type="checkbox"/>
d.	No	<input type="checkbox"/>
e.	Altro.	<input type="checkbox"/>

#### 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)

a.	Si, mediante una pagina web dedicata ai servizi di autenticazione federata	<input checked="" type="checkbox"/>
b.	Si, mediante la distribuzione di materiale cartaceo	<input type="checkbox"/>

c.	Si, mediante eventi informativi/divulgativi	
d.	No	
e.	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)**

a.	Si, mediante un' informativa disponibile su di una pagina web dedicata ai servizi di autenticazione federata	
b.	Si, mediante un' informativa su di una pagina web dedicata raggiungibile dalla pagina di login dell'Identity Provider o direttamente disponibile su quest'ultima	<b>X</b>
c.	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	
d.	Si, distribuendo agli utenti un'informativa cartacea	
e.	No	
f.	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)**

a.	Si, mediante un'accettazione esplicita rilasciata on line tramite applicazione web con accesso autenticato	
b.	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	
c.	Si, facendo firmare agli utenti un modulo di consenso cartaceo	
d.	No	
e.	Altro.	<b>X</b>

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

Richiedendo l'accesso al Service Provider federato, l'utente consente implicitamente il trasferimento degli attributi dall' IdP all'SP richiesto. L'utente è informato al momento dell'autenticazione.

**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?**

a.	si, se il servizio viene erogato dall'Italia	
b.	si, se il servizio viene erogato dall'Europa	
c.	si, se il Service Provider dichiara di accettare la direttiva europea sul trattamento dei dati personali	<b>X</b>
d.	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?**

a.	si, se il servizio viene erogato dall'Italia	
b.	si, se il servizio viene erogato dall'Europa	
c.	si, se il Service Provider dichiara di accettare la direttiva europea sul trattamento dei dati personali	
d.	no	<b>X</b>

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

a.	Infrastruttura fault tolerant	<b>X</b>
b.	Piano per disaster recovery	<b>X</b>
c.	Istanze multiple dell'IdP	
d.	Altro	

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

a.	si	<b>X</b>
b.	no	

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

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

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

a.	si	<b>X</b>
b.	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?**

a.	si	
b.	no	<b>X</b>