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.

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.

---

[1] 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 Roma TRE

Nome e cognome di chi compila il questionario: Vincenzo Praturlon

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

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

1. Accreditamento Personale
2. Accreditamento Studenti

Relativamente al processo di accreditamento 1. Accreditamento Personale rispondere alle seguenti domande:

1.1 INFORMAZIONE SUL PROCESSO DI ACCREDITAMENTO PERSONALE

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

Le utenze coinvolte sono relative al personale strutturato dell'ateneo, così come definito nelle Active Directory del dominio personale.local.

In particolare l'identità digitale viene rilasciato solo per le utenze aventi campo (LDAP) title popolato con un dei seguenti ruoli:

"personale" | "Assistente universitario" | "cultore" | "Dirigente" | "Dirigente a contratto" | "Personale non docente" | "supervisore" | "Collaboratore linguistico (rit. TESORO)" | "Lettore di madre lingua" | "Lettore di scambio" | "personale a contratto" | "Collaboratore coord. e continuativo" | "dirigente a contratto" | "interinale" | "T.A.B. a contratto" | "Assegnista di ricerca" | "Personale non docente a tempo det-Tesoro" | "non docenti a tempo det. -inps" | "Rettore" | "Direttore Generale" | "docente" | "Professore Associato" | "Professore Ordinario" | "Ricercatore universitario" | "Supplente docente interno" | "Supplente docente esterno" | "Ricercatore a tempo det-Tesoro" | "Docenti a contratto – Professionisti |"fornitore" | "ospite" | "Dottorando" | "Tutor" | "library-walk-in"

Il ruolo è sincronizzato periodicamente con il database dell'applicativo di gestione del personale (CINECA CSA), o inserito manualmente nel campo title per il personale non registrato nella anagrafica CSA.

Le informazioni del profilo utente sono fornite dall'utente stesso in un modulo online ("scheda informativa") e vengono validate dall'Area Personale prima di essere inserite in CSA.

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?

c. 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.

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

a. la persona è stata identificata de visu attraverso un documento di identità personale.

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

b. no, i passi variano a seconda della tipologia di utente (assunzione, contratto, assegno et c.)

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)?

a. username/password

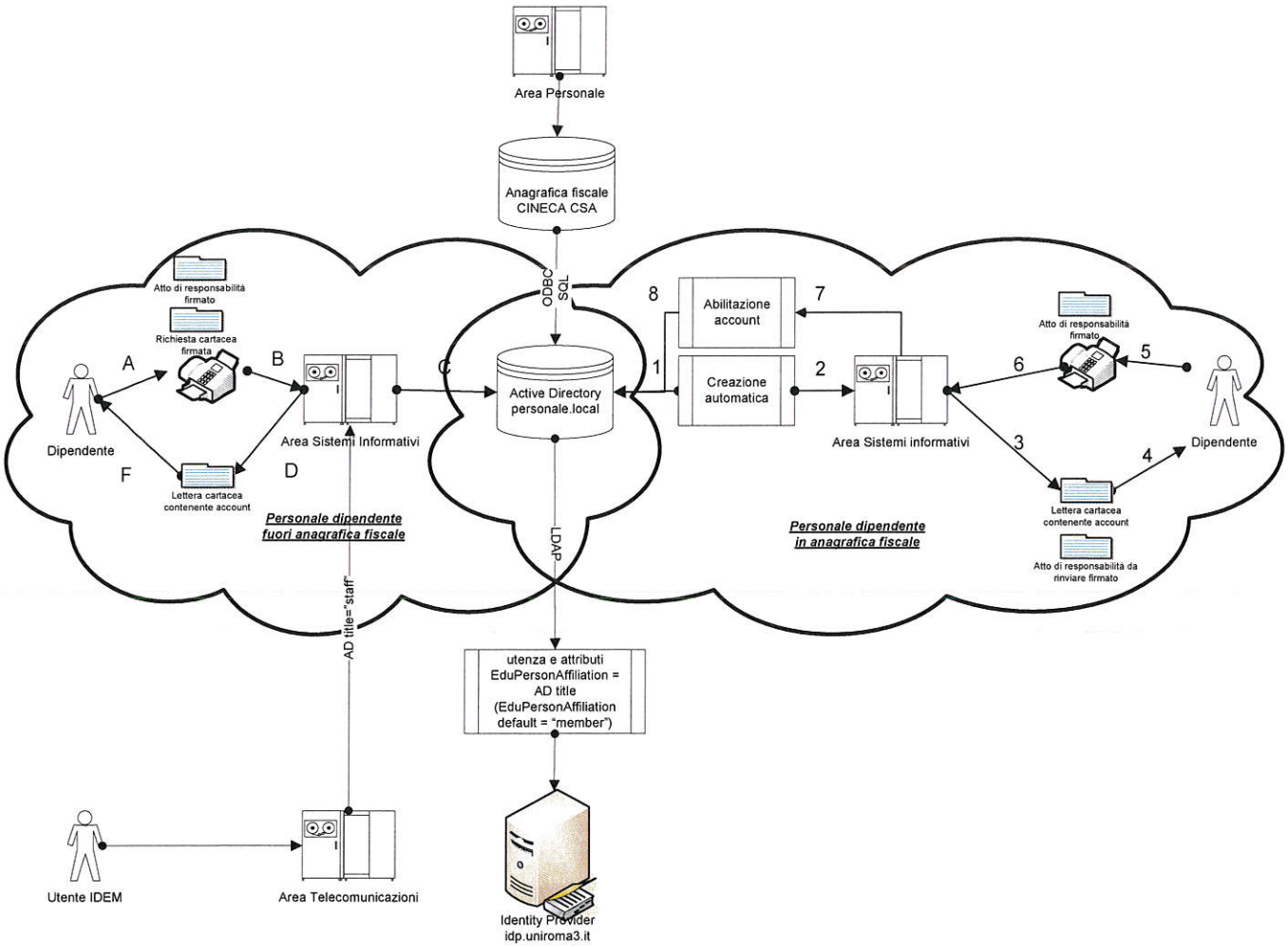
1.1.7 Un utente può avere più identità digitali (e di conseguenza diverse credenziali) rilasciate dalla sua OdA (es. dipendente che è anche studente, ecc...)?

a. Si

1.1.8 Come avviene la consegna delle credenziali?

a. vengono consegnate all'utente a mano/a voce dall'ufficio/persona preposta all'accreditamento
d. altro (invio SMS su cellulare di servizio)

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

Le utenze rilasciate in modo automatico o manuale rimangono disabilitate fino alla ricezione del modulo firmato di assunzione responsabilità e presa visione dei regolamenti.

Relativamente al processo di accreditamento 2. Studenti rispondere alle seguenti domande:

1.2 INFORMAZIONE SUL PROCESSO DI ACCREDITAMENTO STUDENTI

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

Le utenze coinvolte sono relative agli studenti dell'ateneo, così come definito nelle Active Directory del dominio studenti.local.

In particolare l'identità digitale viene rilasciato solo per le utenze abilitate e con il campo (LDAP) title popolato con il seguenti ruolo:

"studente riconosciuto"

Il ruolo è assegnato periodicamente mediante estrazione dal database dell'applicativo di gestione degli studenti (CINECA ESSE3), filtrando le utenze che hanno associato almeno un esame (riconoscimento de visu da parte del docente).

Le informazioni del profilo utente sono fornite dall'utente stesso in un modulo online durante il processo di pre-immatricolazione e vengono validate dalle Segreterie Studenti prima di essere inserite in ESSE3.

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

c. 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.

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

a. la persona è stata identificata de visu attraverso un documento di identità personale.

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

b. no, i passi variano a seconda della tipologia di utente (immatricolandi, studenti, dottorandi et c.)

1.2.5 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)?

a. username/password

1.2.7 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

1.2.8 Come avviene la consegna delle credenziali?

a. vengono consegnate all'utente a mano/a voce dall'ufficio/persona preposta all'accreditamento
d. altro (invio SMS su cellulare)

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

Il flusso è analogo a quello del personale, salvo per il database autoritativo, che è quello di Esse3 anziché CSA.

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

Le utenze rilasciate in modo automatico o manuale rimangono disabilitate fino alla ricezione del modulo firmato di assunzione responsabilità e presa visione dei regolamenti.

1.3 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):

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
d. blocco delle credenziali in caso di ripetuto inserimento di password non corretta

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

a. Si

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

b. L'utente firma un'assunzione di responsabilità
c. Ci sono espliciti riferimenti in regolamento/i dell'OdA

1.3.4 Esiste una policy relativa alle gestione delle credenziali ?

a. si, è pubblicata su web (http://asi.uniroma3.it/download/Roma3Pass.pdf)
b. si, è fornita all'utente contestualmente all'accreditamento

1.3.5 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

1.3.8 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?

c. No

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

f. Altro: non vengono mai disabilitate, bensì private di ogni privilegio / autorizzazione salvo l'accesso ai portali del personale o dello studente.

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

b. no

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

c. L'utente non viene mai cancellato dal sistema di accreditamento

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

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

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

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

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)

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

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)

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

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?

d. no: non in modo automatico, il rilascio viene valutato caso per caso

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?

d. no: non in modo automatico, il rilascio viene valutato caso per caso

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

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

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. riportano l'indicazione di come procedere, in particolare i contatti di riferimento (es. indirizzo email, pagina web)

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

a. Si

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

a. Si