

Documento descrittivo del processo di accreditamento degli utenti dell'Università degli Studi di Ferrara

Le informazioni fornite in questo documento sono accurate alla data del 01/03/2010

Revisioni	1
Nota introduttiva	2
Abbreviazioni.....	2
Gestore dell'accREDITamento	3
Utenti gestiti.....	3
Staff.....	3
Student	3
Alumn.....	3
Affiliate.....	3
B2B / Servizi.....	3
Mappatura degli utenti sulle affiliazioni IDEM.....	4
Visione di insieme del processo di accREDITamento degli utenti	4
Il processo di accREDITamento per la categoria di utenti X.....	4
Il processo	4
Modalità di riconoscimento della persona	4
Caratteristiche dell'identità digitale	4
Gestione del ciclo di vita.....	4
Formato e regole delle credenziali	5
Eventuale presenza di credenziali multiple per la stessa persona.....	5
Modalità di consegna delle credenziali	5
Modalità di recupero delle credenziali smarrite.....	5
Modalità di gestione smarrimento smartcard/token.....	5
Durata dell'accREDITamento	5
Disabilitazione utente	5
Cancellazione definitiva utente.....	5
Rischi specifici associati alla categoria di utenti	5
Interoperabilità tra credenziali deboli (username+pwd) ed eventuali credenziali forti (smartcard)	5
Il sistema di autenticazione e autorizzazione interno.....	6
Partecipazione ad altre federazioni	6

Revisioni

Data	Versione	Descrizione modifica	Autore
03/04/2009	0.1	Bozza	Roberto Gaffuri
29/05/2009	0.2	Bozza	MLM
31/07/2009	0.3	Rilasciato	MLM
02/12/09	0.4	Corretta la nota introduttiva sulla pubblicità del documento	rc

Nota introduttiva

La partecipazione alla Federazione IDEM ("Federazione") abilita l'organizzazione partecipante ("Partecipante") 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 i Partecipanti alla fine possano fidarsi dei sistemi di identity management e dei sistemi di gestione di accesso alle risorse degli altri partecipanti come si fidano dei propri.

Fondamentalmente ci si aspetta dai Partecipanti che essi forniscano agli altri Partecipanti 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, incluse le informazioni relative agli attributi che vengono utilizzati per la Federazione.

I due criteri per garantire che gli Identity Provider forniscano asserzioni di attributi fidate sono: (1) che il sistema di gestione delle identità ricada sotto la supervisione degli organismi che hanno responsabilità direttive e gestionali nell'Organizzazione e che (2) il sistema che emette le credenziali per gli utenti finali (e.g., PKI certificates, userids/passwords, Kerberos principals, etc.) sia dotato di appropriate misure di gestione del rischio (e.g., authentication and authorization standards, security practices, risk assessment, change management controls, audit trails, etc.)

Il Documento DOPAU prodotto dal Partecipante DEVE contenere le informazioni elencate nel presente modello.

In caso di modifica delle procedure o informazioni descritte nel documento, esso DEVE essere prontamente aggiornato e ne deve essere data comunicazione alla Federazione.

Abbreviazioni

Si definiscono, per gli scopi del presente documento, i seguenti soggetti:

- **Ateneo:** l'Ateneo di Ferrara.
- **Utente:** soggetto con diritto di accesso ai servizi informatici.
- **Utenti strutturati:** docenti e personale tecnico-amministrativo.
- **Utenti non strutturati:** soggetti esterni con rapporti di collaborazione, di docenza e di ricerca con l'Ateneo comunque preventivamente identificati e autorizzati.
- **Studenti:** soggetti regolarmente iscritti a un qualunque corso di studio erogato dall'Ateneo, oppure studenti provenienti da altri Atenei a seguito di scambi nell'ambito di programmi nazionali e internazionali.
- **Area Amministrativa:** comprende gli uffici che organizzano e gestiscono le risorse umane, la ripartizione economica e giuridica di Ateneo.

- **Area Informatica:** è l'Area che progetta, implementa e gestisce tutti i servizi, i server, i sistemi e le reti dell'Ateneo.
- **ESSE3:** è il sistema informatico implementato dal Consorzio Interuniversitario "CINECA" per la gestione della segreteria studenti e dei servizi agli studenti.
- **CSA:** sistema informatico "Carriere e Stipendi di Ateneo" sviluppato dal CINECA dedicato alla gestione giuridica ed economica del personale universitario.