UNIMORE
UNIVERSITÀ DEGLI STUDI DI MODENA E REGGIO EMILIA

Politica di Ateneo per l'identità digitale

xx.xx.2023

Approvato dal Consiglio di Amministrazione

Politica di Ateneo per l'identità digitale

Scopo

Questo documento ha l'obiettivo di informare riguardo le politiche e le procedure di rilascio e di gestione dell'identità digitale di UNIMORE, oltre che illustrare le procedure che ne garantiscono la sicurezza e le precauzioni che occorre mantenere per evitare rischi.

A cosa serve l'identità digitale

La gestione delle identità in UNIMORE è un processo in atto dal 2002, che si è via via consolidato ed arricchito nel tempo, nonché modificato per rimanere in linea con lo stato dell'arte tecnologico.

L'identità digitale in UNIMORE è stata unificata per garantire un maggiore controllo degli accessi che vengono effettuati dagli utenti autorizzati e una maggiore sicurezza nel processo di gestione delle identità stesse.

L'identità digitale serve ad identificare ogni persona che ha necessità di accedere ai servizi online e offline (onlife) di UNIMORE, ad autorizzarne l'accesso e a tracciarne l'utilizzo.

L'identità digitale di UNIMORE partecipa alla Federazione IDEM[1] e alla interfederazione eduGAIN[2] ed in questo modo permette l'accesso ai servizi messi a disposizione dagli altri partecipanti alle suddette federazioni[3]. Con l'identità digitale UNIMORE è possibile accedere ad eduroam®.

L'identità digitale UNIMORE può integrare l'identità SPID e CIE[4].

A chi è rivolto il servizio di identità digitale

Le categorie a cui UNIMORE rilascia una identità digitale sono:

- gli studenti (lauree triennali, lauree specialistiche, master, dottorati, erasmus),
- il personale contrattualizzato (docenti, ricercatori, assegnisti, personale tecnico-amministrativo, borsisti),
- i collaboratori esterni,
- i partecipanti a convegni presso Unimore.

Standard utilizzati

UNIMORE adotta tecnologie e standard internazionali ben noti ed implementati in software a codice sorgente aperto, o sviluppati dalla pubblica amministrazione, per tutto il processo di gestione delle identità digitali [Codice dell'amministrazione digitale, Decreto Legislativo 7 marzo 2005, n. 82, art. 68].

I protocolli e software utilizzati sono: SAML2/Shibboleth, OIDC, LDAP/OpenLDAP, ESB/Apache ActiveMQ.

---

[1] https://www.idem.garr.it/partecipare/partecipanti
[2] https://edugain.org/, https://technical.edugain.org/status
[3] Servizi IDEM https://www.idem.garr.it/partecipare/risorse-idem, servizi eduGAIN https://technical.edugain.org/entities
[4] https://www.spid.gov.it/

Ciclo di vita dell'identità

L'identità digitale è personale ed è assegnata ad una singola persona fisica. Essa è costituita da identificatori univoci, come lo username, e da attributi quali ad esempio il nome, il cognome, il codice fiscale, ecc…, e da almeno un metodo di autenticazione.

L'identità digitale ha un ciclo di vita composto dalle fasi: creazione, mantenimento, disattivazione (sospensione), distruzione.

Creazione

L'identità digitale viene creata sulla base di fonti autoritative che ne richiedono la creazione.

Prima della creazione è sempre necessario verificare l'identità della persona a cui verrà rilasciata l'identità digitale in modo da garantire che l'identità digitale sia personale. L'operazione di verifica dell'identità viene documentata dagli uffici preposti. La verifica dell'identità può avvenire:

- di persona tramite l'esibizione di un documento di identità valido e considerato autentico;
- da remoto tramite l'esibizione o l'invio di una copia di un documento di identità valido e considerato autentico;
- basata su altre credenziali il cui rilascio prevede un metodo di verifica dell'identità della persona compatibile o superiore rispetto ai casi precedenti (ad esempio a seguito di autenticazione con credenziali SPID).

L'ufficio preposto, dopo avere verificato l'identità della persona, la registra nel database. Alternativamente la persona compila un modulo online con i propri dati e l'ufficio preposto, dopo avere verificato l'identità della persona, ne autorizza l'inserimento nel database.

L'identità digitale viene automaticamente creata, mediante un processo software, nel momento in cui appare nei relativi database gestionali grazie all'uso della messaggistica asincrona.

Al momento della creazione all'identità digitale vengono assegnati almeno un metodo di autenticazione e una data di scadenza dell'identità digitale. La consegna delle credenziali segue procedure documentate e registrate.

Le identità sono salvate su un sistema di directory LDAP, la autenticazione avviene con i protocolli SAML2 o OIDC; i sistemi coinvolti sono disaccoppiati e comunicano tra di loro tramite messaggistica asincrona.

Mantenimento

Determinate modifiche nei dati delle fonti autoritative (database gestionali) relativamente alle persone, determinano modifiche che vengono immediatamente riprodotte nelle corrispondenti identità digitali, modificando i relativi attributi.

Sospensione

Come azione amministrativa è possibile sospendere la validità di una identità, in conseguenza di un incidente o di una sanzione.

Disattivazione / Distruzione

L'identità è automaticamente disattivata alla data di scadenza del titolo per la quale è stata rilasciata. E' prevista la possibilità di un periodo di grazia al termine del quale non è più possibile effettuare l'autenticazione. Nella tabella che segue sono indicati i periodi di grazia attivi per le diverse tipologie di utenza.

DESCRIZIONE UTENTE	Periodo di grazia in mesi	Note
STUDENTE	36	Email, Cloud Azure, Servizi bibliotecari.

		Su ESSE3 l'accesso è garantito per sempre
PROFESSORE	6	
PERSONALE TECNICO AMMINISTRATIVO	6	
PROFESSORE EMERITO	6	
TITOLARE DI BORSA DI STUDIO	6	
DIPENDENTE ALTRA UNIVERSITA	15	
DIPENDENTE ALTRO ENTE DI RICERCA	6	
COLLABORATORE DI RICERCA (A TITOLO GRATUITO)	6	
DIPENDENTE DI ALTRA AZIENDA SANITARIA	6	
INTERINALE	1	
LAUREATO FREQUENTATORE	6	
DOTTORANDO DI ALTRA UNIVERSITA	6	
PROFESSORE FUORI RUOLO ESTERNO	6	
SPECIALIZZANDI DA SEDI CAPOFILA	0	
TIROCINANTE DI DIPARTIMENTO	1	
COLLABORATORE COORDINATO CONTINUATIVO	6	
CULTORE DELLA MATERIA	6	
DOCENTE A CONTRATTO	15	
SUPERVISORE SISS	6	
TUTOR	6	
DIDATTICA INTEGRATIVA (CONFERIBILE A DOTTORANDI E ASSEGNISTI)	6	
DOCENTE IN CONVENZIONE	15	
INSEGNAMENTO IN SCUOLE DI SPECIALITA E MASTER	6	
SUPPORTO DIDATTICA LINGUE	6	
SUPPLENTE DOCENTE	6	
DOCENTE INTERATENEO	15	
SENIOR PROFESSOR	6	
TUTOR DI TIROCINIO	6	
STUDENTE DI ALTRA UNIVERSITA	6	
VISITING PROFESSOR	1	
RAPPRESENTANTE STUDENTI	0	
CONVENZIONATO (CLIENTI DELLE CONVENZIONI)	0	
OSPITE CON ACCESSO AL SERVIZIO VPN	0	
PERSONALE ARESTUD	6	
TIROCINANTE SCUOLE SUPERIORI	0	
PERSONALE MORE SERVICE	6	
PERSONALE INTERNATIONAL WELCOME DESK	6	
LAVORATORE OCCASIONALE (CONTRATTO PERSONALE SENZA PARTITA IVA)	6	
LIBERO PROFESSIONISTA (CONTRATTO PERSONALE CON PARTITA IVA)	6	
COLLABORATORE IN SPIN OFF	6	
FORNITORE (DIPENDENTE O TITOLARE DELLE DITTE FORNITRICI)	0	
COMPONENTE ORGANI COLLEGIALI	0	
MANUTENTORE	0	
OSPITE (DI SOLITO DI LUNGA DURATA)	0	

La disattivazione prevede la distruzione dal sistema di gestione delle identità salvo che per la username che, resa inattiva, è conservata indefinitamente per evitarne il riutilizzo.

Metodi di autenticazione

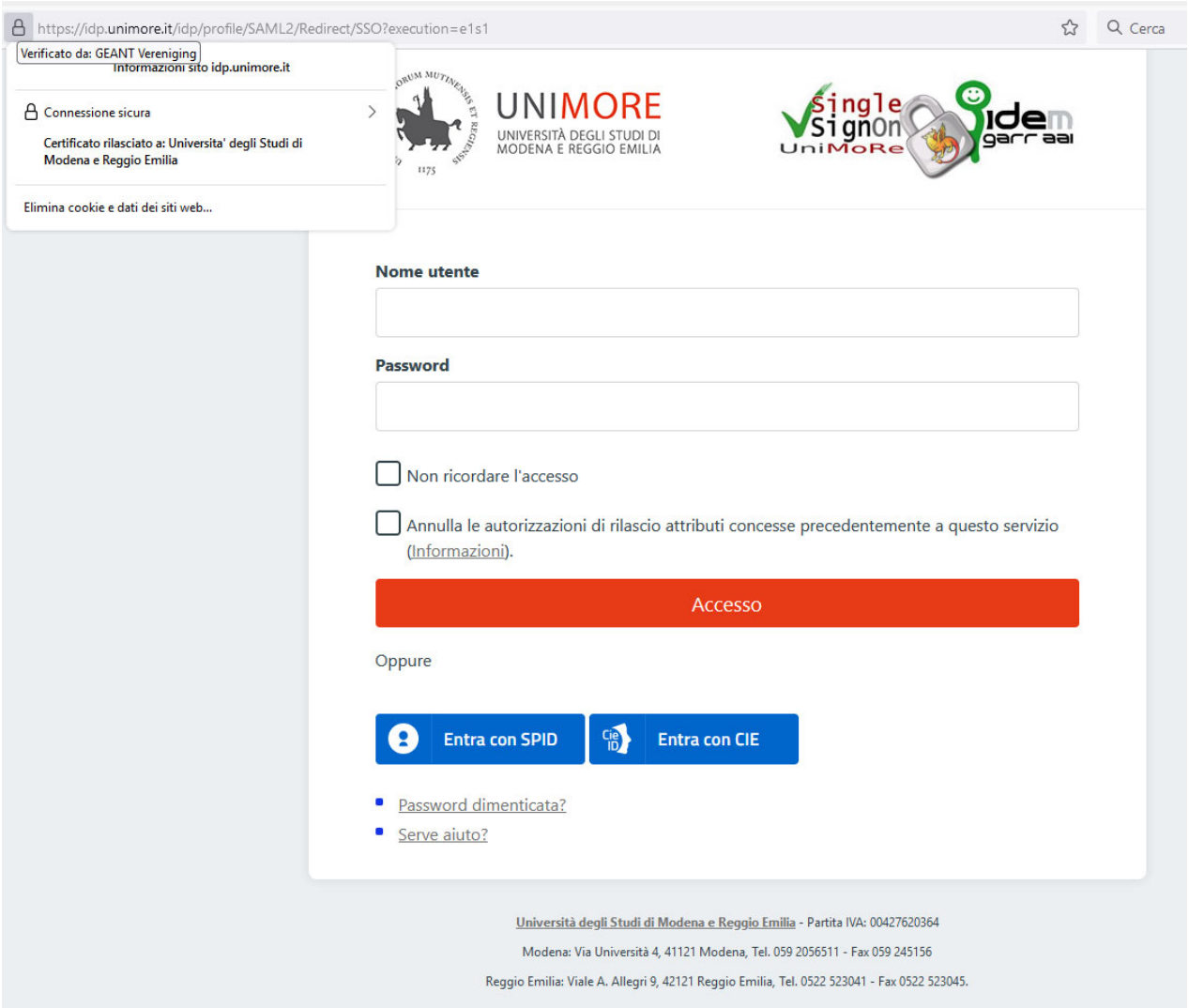
Le identità digitali di UNIMORE prevedono i seguenti metodi di autenticazione

- username/password
- badge, usato per registrare la presenza e aprire porte
- badge virtuale (QRcode)
- telecomando per apertura cancelli

Per la politica delle password si rimanda all'allegato.

Attualmente l'autenticazione a 2 fattori non è gestita centralmente, ma è demandata ai servizi che la necessitano.

Per la sicurezza delle proprie credenziali username/password, l'utente è invitato ad inserirle esclusivamente alla pagina ufficiale di autenticazione raggiungibile al seguente indirizzo, protetta da certificato valido ed illustrata in figura. https://idp.unimore.it/idp/profile/admin/hello?execution=e1s1



Per la sicurezza dei mezzi fisici di autenticazione quali badge e telecomando, l'utente è invitato a custodirli con cura e nel caso a denunciarne tempestivamente lo smarrimento agli uffici dell'Ateneo.

Accesso

L'identità digitale di UNIMORE permette l'accesso ai servizi UNIMORE, alle risorse IDEM[5] e ai servizi eduGAIN[6], oltre che l'accesso alla rete wireless mondiale eduroam®[7].

Privacy

Il trattamento di dati personali connesso alla creazione e alla gestione dell'identità digitale è improntato ai principi di correttezza, di liceità, di trasparenza ed è debitamente descritto nell'apposita informativa ai sensi dell'art. 13 del Reg. UE 2016/679 ("GDPR"), disponibile sul sito istituzionale di UNIMORE

Monitoraggio e sanzioni

Si procede alla disattivazione delle credenziali a seguito delle violazioni di …

Continuità operativa

La continuità operativa del processo di autenticazione è garantita best effort.

Revisione

Ultima revisione 15/12/2023. Si prevede aggiornamento a distanza di 12 mesi.

[5] Risorse IDEM: https://www.idem.garr.it/partecipare/risorse-idem
[6] Per chi è eduGAIN https://edugain.org/about-edugain/who-is-edugain-for/
[7] Dove puoi connetterti a eduroam https://eduroam.org/where/