WORKSHOP GARR 2024

NET MAKERS

Linee guida per quality assurance: esperienza al Politecnico di Milano

Roberto Gaffuri

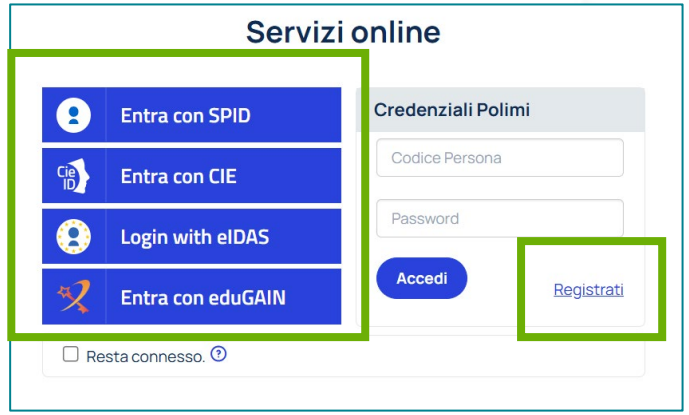
Politecnico di Milano

Registrazione

La nascita di una identità digitale avviene con **registrazione autonoma dell'utente mediante un servizio online**. L'identità viene creata in un database master -> **Anagrafica unica di Ateneo**.

Due casi:

1. Identità che proviene da un'autenticazione SPID/CIE/eIDAS
   -> Alcuni attributi vengono trasferiti dall'identità di origine (CF, nome, cognome, data nascita)
2. Identità che nasce da registrazione completa dei dati anagrafici



Consegna credenziali - primo fattore (1FA)

Alla fine della registrazione, sia nel caso di registrazione mediante identità governativa, che nel caso di auto registrazione:

- Viene chiesto all'utente di inserire un **indirizzo email personale** che deve essere confermato mediante accesso alla casella associata e link di conferma.
- Viene fornito all'utente un **Codice persona** di 8 cifre e richiesta l'impostazione di una **password** di complessità stabilita dalle nostre policy di sicurezza

Sotto casi di registrazione e consegna credenziali gestiti da uffici:

- Registrazione utente da parte di una segreteria con consegna de visu delle credenziali in busta chiusa
- Registrazione utente da parte di una segreteria + invio all'indirizzo mail dichiarato dall'utente di un link (con scadenza) per l'accesso al servizio di impostazione password.

Attivazione secondo fattore (2FA)

Al primo accesso ai Servizi Online con **credenziali 1FA Polimi** o al primo accesso con **SPID/CIE/eIDAS** dopo la registrazione, viene chiesto all'utente di attivare **un secondo fattore di autenticazione (2FA)**

Tre scenari:

1. Se **cittadino italiano** studente, laureato, candidato studente, esterno: è **obbligato ad utilizzare SPID/CIE** come modalità di autenticazione MFA
   - Eccezione: può dichiarare di non essere in grado di usare identità SPID/CIE. In questo caso è consentita l'attivazione **temporanea** di 2FA Polimi.
2. Se straniero: è **obbligato ad attivare 2FA Polimi** (solo via APP)
3. se staff Polimi: **può decidere** se utilizzare MFA esterna SPID/CIE/eIDAS oppure 2FA Polimi (via APP o SMS) o entrambe.

Identificazione

Per utenti che si sono registrati mediante SPID/CIE/eIDAS:

- **identificazione garantita da identità governativa (IDEM-P2)**

Per utenti che si sono auto registrati (tipicamente studenti stranieri):

- Per studenti che fanno il Test di ingresso Polimi: l'identificazione avviene all'ingresso del Test mediante **riconoscimento de visu + documento identità apparentemente valido (IDEM-P1)***;
- Per studenti che entrano in Ateneo attraverso altro canale di accesso (non Test di ingresso Polimi): l'identificazione avviene mediante convocazione in segreteria studenti o mediante video call **con riconoscimento de visu + documento identità apparentemente valido (IDEM-P1)***;

  **** In alcuni casi i documenti potranno essere verificati a posteriori portando l'identità a IDEM-P2***

- Per PTA/Docenti/Collaboratori/Consulenti: l'identificazione avviene in sede di attivazione del contratto mediante**: riconoscimento de visu + documento identità verificato (IDEM-P2).**

NOTA: L'accesso ad alcune funzioni dei Servizi Online **è inibita** nel caso l'utente non risulti in stato **"Riconosciuto de visu"** o **"Riconosciuto SPID/CIE/eiDAS**".

Sottoscrizione acceptable use policy (AUP)

Al primo ingresso nei Servizi Online viene chiesto all'utente di accettare le policy in materia di privacy e sicurezza.

NB: Le policy hanno una versione e possono essere rinnovate e sottoposte nuovamente all'accettazione dell'utente

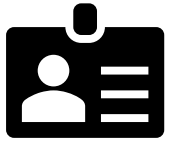
Replica identità digitali in directories slave

Alcuni attributi dell'identità digitale (Codice persone, password, nome, cognome, email, affiliazione, group membership) sono automaticamente replicati dal db master in 2 directories slave LDAP e Active Directories **dedicate ai diversi processi di autenticazioni e autorizzazione anche in contesti non web.**

Ad esempio:

- Backend IDP Shibboleth
- Sorgente sync identità per Cloud Office365 e WebEx
- Auth/Authz postazione di lavoro per PTA
- Auth/Authz VPN per docenti, ricercatori, pta, collab. esterni
- Auth/Authz storage dipartimentali per docenti/ricercatori
- Auth/Authz rete wifi mediante EAP-TTLS

Consegna Policard



- **Studenti**: la Policard viene spedito al recapito dello studente o ritirata presso la Segreteria studenti
- **Staff o esterni**: la Policard viene ritirata presso la struttura di afferenza

L'utente deve attivare la card mediante servizio online.

L'utente può chiedere, mediante servizio online, il blocco e la riemissione della card in caso di furto o smarrimento

Attivazione European Student Card (ESC)

Per studenti e dottorandi è prevista l'attivazione automatica della **European Student Card (ESC)**.

Il QR Code della ESC viene inserito in automatico nella sezione carte della App mobile di Ateneo (PolimiApp).

Recupero credenziali 1FA

Due scenari:

Modalità **autonoma** dell'utente:

1. Mediante **indirizzo email personale verificato**, con richiesta OTP per chi ha attivato 2FA Polimi
2. Mediante autenticazione SPID/CIE/eIDAS per chi ha attivato MFA esterna

Modalità **assistita** con apertura ticket da parte dell'utente ad HelpDesk.

- Nella richiesta di assistenza l'utente deve:
  - Allegare **copia documento di identità**
  - Indicare una fascia oraria in cui è disponibile per effettuare **una video call di identificazione**
- Una volta riscontrata l'identità nella video call viene inviata mail alla casella personale dell'utente con link al servizio (con scadenza) per impostare nuova password

Disattivazione temporanea 2FA

Nel caso l'utente non riesca ad autenticarsi SPID/CIE/eIDAS o sia impossibilitato ad usare Token 2FA Polimi (es. smarrimento smartphone) può **temporaneamente disattivare MFA**. Due scenari:

1. **Modalità autonoma:**
   - mediante OTP inviato a numero di cellulare personale o a indirizzo email personale verificati in fase di attivazione. Per la disattivazione l'utente dovrà inserire Credenziali 1FA Polimi + OTP
   - Mediante chiave alfanumerica rilasciata all'atto dell'attivazione MFA
2. **Modalità assistita** con richiesta di supporto ad HelpDesk via Ticket. Nella richiesta di assistenza l'utente deve:
   - Allegare documento di identità
   - Indicare una fascia oraria in cui è disponibile per effettuare una video call di riconoscimento
   - Una volta riscontrata l'identità nella video call l'operatore può disattivare MFA utente

Trascorso l'intervallo di disattivazione temporanea (72h) l'utente sarà obbligato a riattivare MFA

Q&A

Per eventuali approfondimenti scrivere a: idem@polimi.it