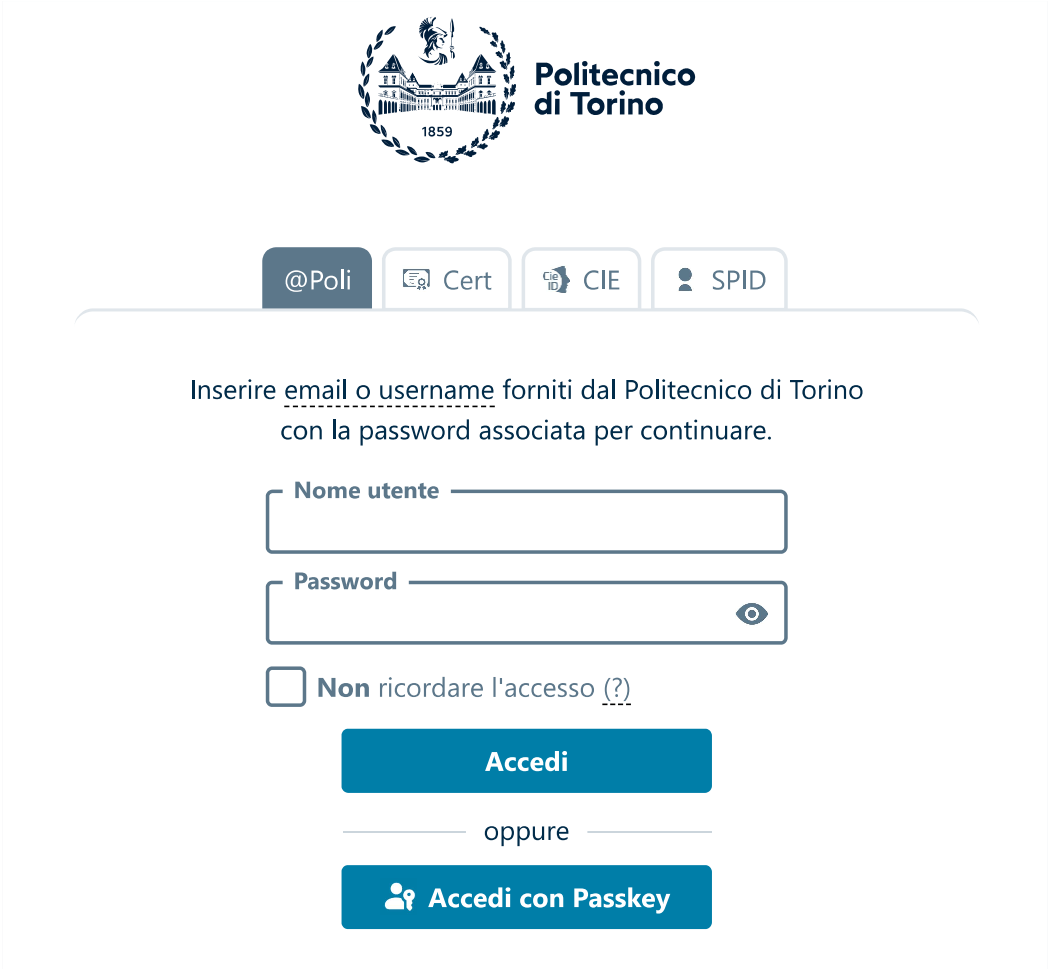
Il Nuovo IDP del Politecnico di Torino



Sommario

Cos'è un IDP e a cosa serve

L'Identity Provider (IDP) è un sistema che gestisce l'autenticazione degli utenti, permettendo loro di accedere a diverse applicazioni e servizi utilizzando un'unica identità digitale.

Il nuovo IDP del Politecnico di Torino rappresenta un significativo passo avanti nella gestione delle identità digitali, questo sistema non solo mantiene tutte le funzionalità del precedente, ma introduce una serie di miglioramenti che ne aumentano l'efficacia e la sicurezza.

Proiettato sulle reti **IDEM** e **eduGAIN**, il nuovo IDP consente agli utenti di autenticarsi e accedere a servizi federati sia a livello nazionale che internazionale[2]. Questo è particolarmente utile per gli studenti e il personale che necessitino di accedere a risorse e servizi offerti da altre istituzioni aderenti a queste reti. Inoltre, il sistema è configurato per supportare **MyAcademicID**, un'iniziativa che permette agli studenti di accedere ai servizi Erasmus+ con le proprie credenziali universitarie[3].

Tra le principali caratteristiche del nuovo IDP c'è il supporto per il **Single-Sign-On** (SSO) ed il **Single-Log-Out** (SLO) unificato, che permette agli utenti di accedere e uscire dai servizi online utilizzando un'unica credenziale[4]. l'esperienza utente risulta semplificata, riducendo la necessità di ricordare multiple password. Inoltre, il nuovo IDP supporta vari metodi di autenticazione, tra cui **password, CIE, SPID, Certificato Digitale e Passkey**[5]. Per aumentare ulteriormente la sicurezza, è prevista l'**autenticazione multi-fattore** (MFA), che richiede un ulteriore livello di verifica oltre alla password[6].

In sintesi, il nuovo IDP del Politecnico di Torino offre una soluzione moderna e sicura per la gestione delle identità digitali, facilitando l'accesso a una vasta gamma di servizi e risorse a livello nazionale ed internazionale.

Caratteristiche del Nuovo IDP

Il nuovo IDP del Politecnico di Torino mantiene, dove possibile, tutte le prerogative del vecchio sistema, ma con miglioramenti significativi:

1. **Identità federate**
   Permettono agli utenti di accedere a servizi esterni utilizzando le credenziali fornite dal Politecnico di Torino

   Federazione IDEM

   IDEM è la Federazione italiana di infrastrutture di Autenticazione e Autorizzazione (AAI), ha lo scopo di consentire agli utenti della comunità scientifica e accademica nazionale di accedere più facilmente a servizi e contenuti in rete messi a disposizione da diverse organizzazioni.

   Accesso eduGAIN

   eduGAIN è il servizio di inter-federazione che connette e permette la cooperazione tra le federazioni di identità di ogni parte del mondo, permettendo agli utenti di accedere a servizi internazionali utilizzando le proprie credenziali istituzionali, favorendo la collaborazione e l'accesso a risorse globali[1].

   MyAcademicID

   MyAcademicID è un progetto finanziato dal programma *Connecting Europe Facility*, che permette agli studenti di autenticarsi per gli studi all'estero utilizzando l'account studente di origine. Integra le identità accademiche con quelle personali, attraverso i nodi nazionali di eIDAS, riducendo il carico amministrativo per il personale e gli studenti[3].

2. **Single-Sign-on e Single-Logout unificato**
   Il sistema di Single-Sign-on e Single-Logout unificato consente il salvataggio a lungo termine della sessione di autenticazione su tutti i sistemi dell'ateneo. Questo permette, per i dispositivi attendibili, di rimanere autenticati fino a 90 giorni dal momento della prima autenticazione. Nel caso in cui si effettuasse l'accesso da un dispositivo non attendibile è buona norma selezionare la checkbox

   posta al di sotto dei campi di inserimento delle credenziali, in modo da impedire il salvataggio della sessione a lungo termine.

3. **Metodi di autenticazione**
   I sistemi di autenticazione previsti dal nuovo IDP di Ateneo sono:

   - *Password*: richiede che l'utente inserisca una combinazione di caratteri segreta, conosciuta solo dall'utente stesso, per verificare la propria identità;
   - *CIE* (Carta d'Identità Elettronica): permette agli utenti di verificare la propria identità utilizzando la loro carta d'identità elettronica, che contiene informazioni personali e un certificato digitale per garantire un accesso sicuro

- *SPID* (Sistema Pubblico di Identità Digitale): consente agli utenti di accedere ai servizi online della Pubblica Amministrazione e dei privati aderenti utilizzando un'unica identità digitale verificata, garantendo così un accesso sicuro e semplificato
- *Certificato Digitale*: permette agli utenti di verificare la propria identità utilizzando un certificato digitale, che contiene informazioni crittografate e univoche per garantire un accesso sicuro
- *Passkey*: consente agli utenti di accedere ai servizi online, utilizzando una chiave crittografica univoca, che elimina la necessità di inserire il nome utente e ricordare una password, offrendo un livello di sicurezza superiore;
- *Autenticazione multi-fattore*: Per aumentare il livello di sicurezza, il sistema può richiedere di autenticarsi utilizzando un fattore aggiuntivo (Passkey, OTP fornito da un'app di autenticazione o inviato via SMS) dopo l'accesso con nome utente e password. In questo modo si riducono i rischi di accesso non autorizzato a tutte le aree contenenti dati sensibili o che permettano operazioni critiche per l'utente in maniera unificata, non demandando l'implementazione ai singoli applicativi;
- *Sistemi biometrici per l'autenticazione*: grazie all'impiego delle Passkey, sarà possibile utilizzare i sistemi biometrici presenti sui propri dispositivi (impronta digitale, riconoscimento facciale, ecc.) per effettuare l'accesso sicuro ai servizi predisposti dall'Ateneo.

Il nuovo IDP del Politecnico di Torino integra una serie di procedure avanzate per la gestione delle password (tra cui il rinnovo, il cambio e il recupero delle stesse) e la gestione del sistema MFA (aggiunta, modifica e rimozione dei metodi). Queste funzionalità permettono agli utenti di mantenere le proprie credenziali sempre aggiornate e sicure, riducendo il rischio di accessi non autorizzati. Il sistema guida l'utente attraverso processi intuitivi per il cambio periodico delle credenziali, il recupero in caso di smarrimento e il rinnovo quando necessario, garantendo così una gestione efficiente e sicura delle stesse. La modalità MFA diventerà l'unica utilizzabile per accedere a tutti i servizi online.

Gestione credenziali

Username e **password** sono informazioni di accesso uniche assegnate a ciascun utente per garantire la sicurezza e l'autenticazione nei sistemi informatici. Le credenziali vengono fornite per la prima volta al momento della registrazione dell'utente nel sistema, permettendo così l'accesso iniziale ai servizi e alle risorse disponibili.

Username

La username fornita ai dipendenti è generalmente del tipo

nome.cognome@polito.it es: mario.rossi@polito.it

La username fornita agli studenti è del tipo

Smatricola@studenti.polito.it es: S123456@studenti.polito.it

Password

L'IDP di Ateneo richiede che la password soddisfi alcuni requisiti minimi:

1. lunghezza minima di 14 caratteri
2. lunghezza massima di 20 caratteri
3. contenere almeno una lettera minuscola dalla a alla z
4. contenere almeno una lettera maiuscole dalla A alla Z
5. non contiene lettere accentate
6. contenere almeno un numero da 0 a 9
7. contenere almeno un carattere speciale (non alfanumerico) dei seguenti: @#?,.<>!%&\+-_/=; ()^|
8. essere diversa dalle ultime cinque utilizzate

Questo tipo di password aumenta la complessità e rende più difficile per gli attaccanti indovinare o forzare l'accesso, garantendo una maggiore protezione delle informazioni personali e dei dati sensibili

CIE

Per ottenere le credenziali CIE (Carta d'Identità Elettronica), è necessario richiedere la Carta presso il comune di residenza. Una volta ottenuta, la CIE contiene un certificato digitale che permette di autenticarsi in modo sicuro ai servizi online.
Durante il processo di rilascio, verranno fornite le istruzioni per l'attivazione e l'utilizzo della Carta, inclusi i codici PIN e PUK necessari per l'accesso[1].

SPID

Per richiedere lo SPID (Sistema Pubblico di Identità Digitale), è necessario seguire alcuni passaggi. Innanzitutto, bisogna scegliere uno dei gestori di identità abilitati, che offrono diversi livelli di sicurezza e modalità di accesso. La registrazione può avvenire online, tramite riconoscimento via webcam, di persona presso gli uffici del gestore, o utilizzando una Carta d'Identità Elettronica (CIE) o una Carta Nazionale dei Servizi (CNS). Durante la registrazione, verranno richiesti alcuni dati personali, un documento di identità valido e il codice fiscale. Una volta completata la procedura, verranno fornite le credenziali SPID

Certificato Digitale

Il certificato digitale è un file con estensione .p12 emesso dalla *Certification Authority del Politecnico di Torino*, che contiene le informazioni personali necessarie a identificare l'utente a cui viene rilasciato.

Esso può essere utilizzato per l'autenticazione su siti web, ad esempio il Portale della Didattica, per firmare digitalmente documenti ed e-mail, e per cifrare in modo sicuro dati e messaggi di posta elettronica. La firma elettronica effettuata con questo certificato non ha valore legale e viene riconosciuta solo dal Politecnico di Torino e dagli altri enti che vogliano ritenerla attendibile.

Passkey

È possibile impostare una o più Passkey per ogni account che si detiene presso il Politecnico di Torino. La Passkey si registra come qualsiasi altro metodo di autenticazione multi-fattore presso l'indirizzo https://idp.polito.it/tokens o comunque seguendo le indicazioni riportate sulla sezione Gestione MFA. A differenza degli altri fattori di autenticazione però, una volta registrato, potrà essere utilizzato anche come fattore primario (e unico) di autenticazione, essendo intrinsecamente più sicuro della classica combinazione nome utente/password. È doveroso notare come tutto "l'ecosistema" delle Passkey sia fortemente dipendente dal dispositivo in uso da parte dell'utente, dal browser e/o eventualmente dal sistema operativo.

Sono state testate le seguenti configurazioni:

- Ambiente Microsoft Windows – dipendenza: browser
  - Google Chrome
  - Microsoft Edge
  - Mozilla Firefox
- Ambiente Android – dipendenza: gestore credenziali di sistema
  - Google Password Manager
  - Samsung Pass
- Ambiente Apple – dipendenza: browser
  - Google Chrome
  - Mozilla Firefox
  - Safari
  - App Password (iOS 18 e successivi)

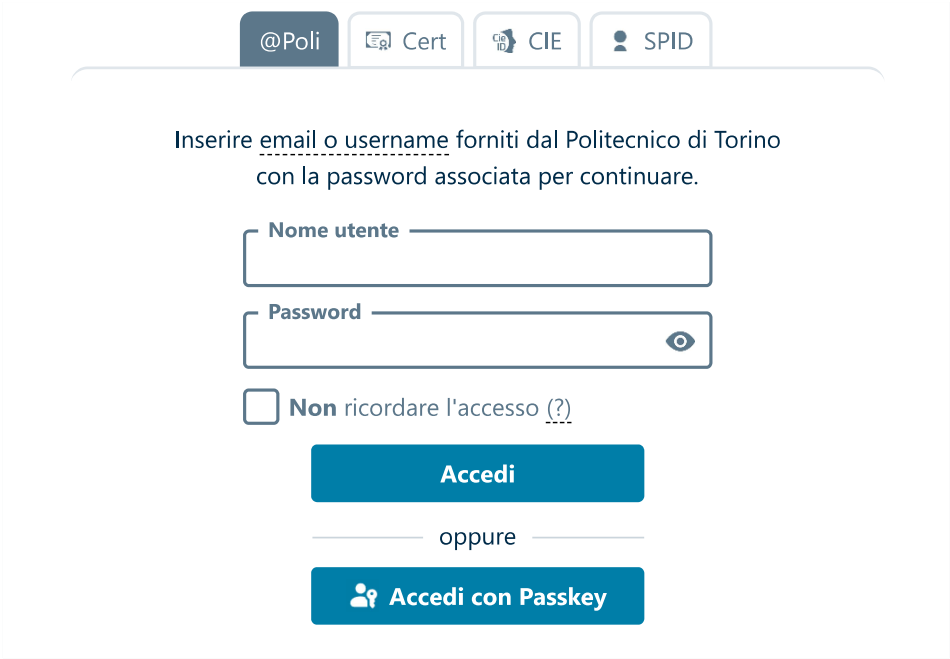
In ogni caso il corretto funzionamento delle Passkey è legato anche all'hardware demandato all'archiviazione sicura dei certificati associati.

Altri sistemi o contesti potrebbero funzionare senza problemi ma, considerato l'elevato numero di combinazioni in essere, non è possibile fornire documentazione su ognuna di esse.

La gestione della memorizzazione delle Passkey è strettamente legata al dispositivo/browser/sistema operativo/gestore credenziali utilizzate, nonostante lo standard preveda misure di sicurezza rigorose in merito alle modalità di salvataggio dei certificati associati. L'utente viene considerato responsabile della sicurezza del contesto in cui vengono salvate le Passkey associate ai propri account di Ateneo. Nel caso in cui le Passkey venissero salvate in ambienti cloud (es. sul proprio account Google personale) e questo venisse compromesso, l'utente è tenuto a rimuovere quanto prima il riferimento a tale Passkey dalla propria area di gestione in modo da evitarne l'uso improprio.

Operazioni di Login sull'IDP

Accesso con nome utente e password



Selezionando il tab **@Poli**

si opera il login utilizzando le credenziali fornite e gestite direttamente dall'Ateneo.

Per eseguire l'accesso con username e password inserire nei campi evidenziati le proprie credenziali

Durante il primo accesso o se non si è configurato nessun metodo di autenticazione multi-fattore viene richiesto di attivarne uno

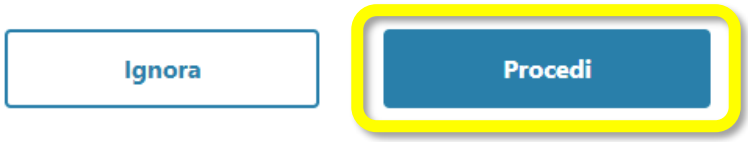
Selezionando **Ignora**

la procedura di autenticazione termina regolarmente come autenticazione classica, con nome utente e password.

La richiesta di configurare ed utilizzare un metodo di autenticazione a due fattori viene reiterata dal sistema finché non viene configurato almeno un metodo.

La procedura di autenticazione a due fattori è fortemente suggerita ed una volta configurato almeno un secondo fattore questo sarà richiesto ad ogni accesso.

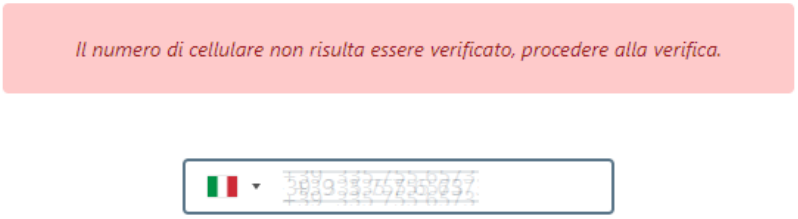
Selezionando **Procedi**



viene richiesto di configurare il sistema di accesso a due fattori tramite SMS

Per la configurazione del metodo, è necessario che l'utente abbia il cellulare che vuole utilizzare come dispositivo di ricezione dello SMS a portata di mano e che sia in una zona dove non abbia difficoltà di ricezione.

Se l'utente ha già registrato un numero di cellulare in MyPoli e/o sul Portale della Didattica, questo viene presentato all'utente che ha la possibilità di indicarne uno alternativo.



Inserito il numero di cellulare che si vuole utilizzare per ricevere il messaggio SMS contenente la OTP, procedendo con conferma verrà richiesto di inserire il codice ricevuto nel campo OTP. Si ricorda che per prevenire procedure di attacco e compromissione dell'account, i tempi per la compilazione del campo sono stretti e non è possibile iniziare la procedura a finirla in un secondo tempo.

Inserita la OTP ricevuta via SMS procedere con **Conferma**. Nella pagina seguente:

<u>è fortemente consigliato aggiungere altri metodi di autenticazione</u>.

È possibile aggiungere sia Passkey(s) che OTP. Entrambi i metodi permettono un accesso più rapido potenzialmente funzionano anche in assenza di rete sul dispositivo autenticatore.

Selezionando **Completa autenticazione** si viene indirizzati al servizio richiesto.

Selezionando il pulsante

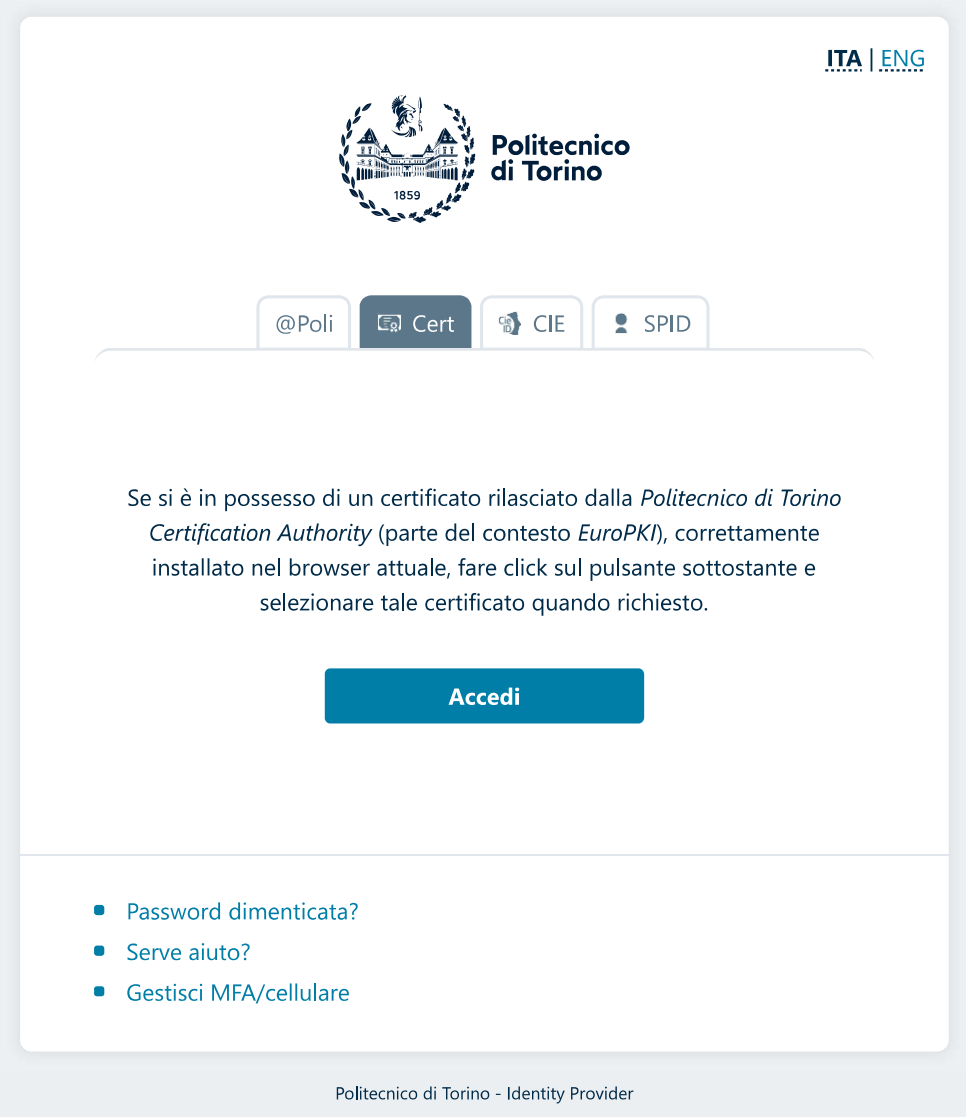
viene iniziata la procedura di login tramite Passkey. Questa procedura dipende dal sistema operativo e/o dal browser in uso.

Per autenticarsi, è necessario aver configurato almeno un sistema di Passkey.

Il sistema di autenticazione tramite Passkey è equivalente all' autenticazione a due fattori, in quanto richiede normalmente due diversi dispositivi per essere completato.

Fare riferimento ai link presenti alla fine di questo documento per ottenere maggiori informazioni per i gestori Passkey più comuni.

Accesso con certificato rilasciato dal Politecnico di Torino



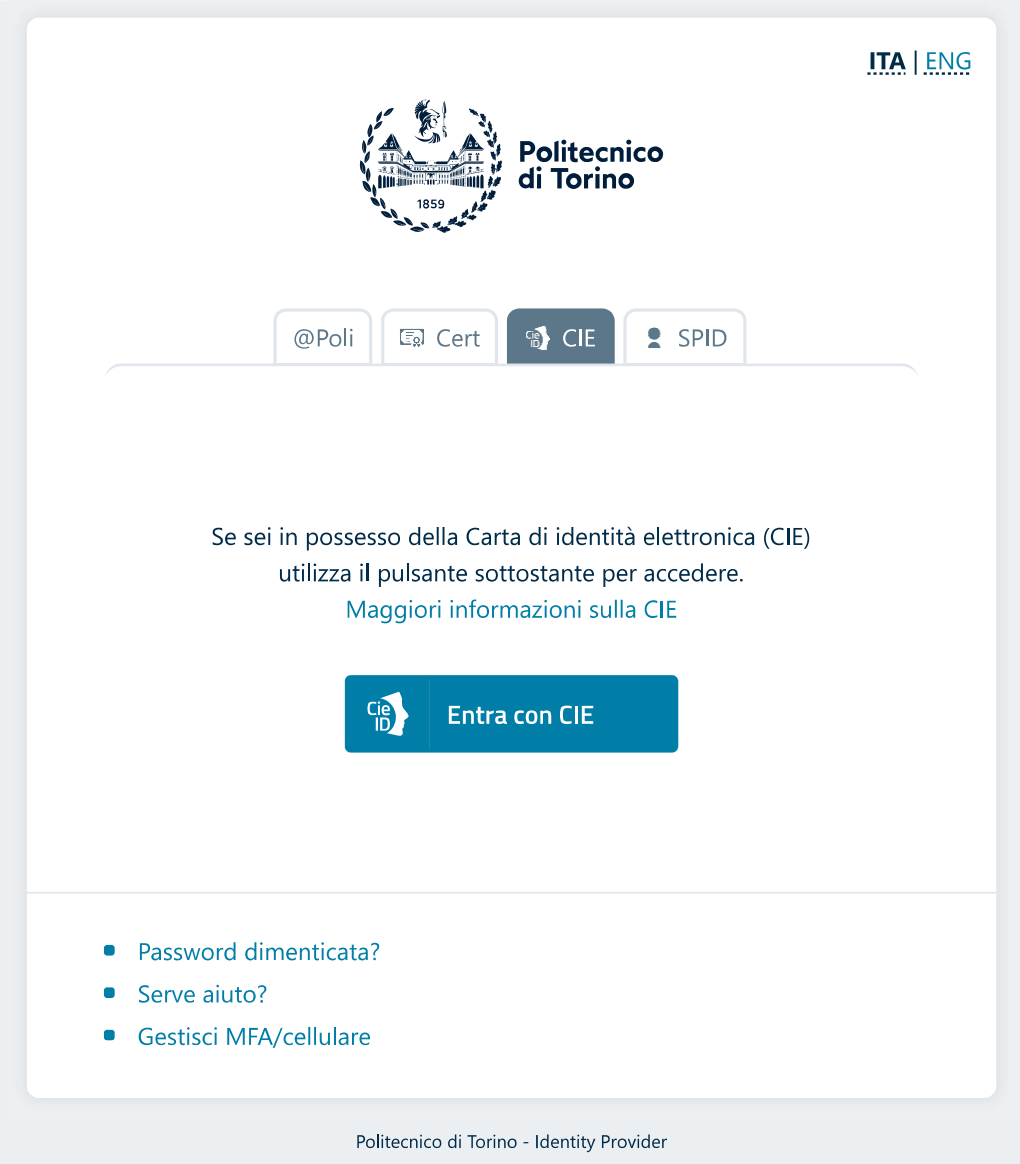
Selezionando il tab **Cert**

si esegue il login utilizzando il certificato presente nel browser utilizzato per l'accesso.

Questa procedura dipende dal sistema operativo e/o dal browser in uso.

Fare riferimento ai link presenti alla fine di questo documento per ottenere maggiori informazioni in merito alla gestione dei certificati sui browser più comuni.

Accesso con CIE



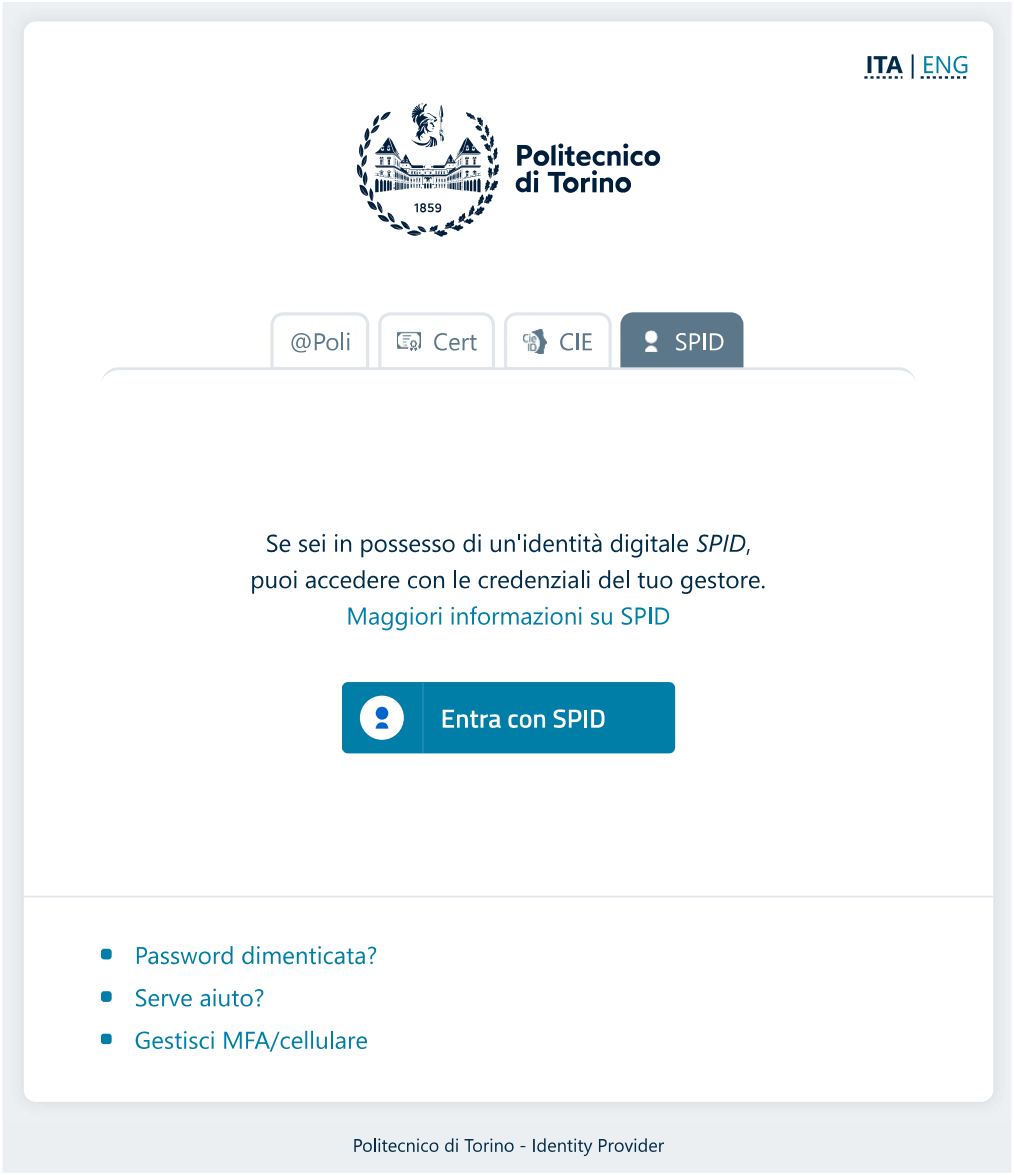
Selezionando il tab **CIE**

è possibile autenticarsi utilizzando la Carta D'identità Elettronica.

Facendo click su **Entra con CIE** si viene rediretti sul portale di autenticazione CIE per procedere all'accesso. Se eseguito correttamente, si viene riportati sul sistema di autenticazione che a questo punto può visualizzare un selettore (nel caso siano trovati nell'anagrafica di ateneo più profili corrispondenti al codice fiscale dell'utente, come ad esempio un profilo studente e uno dipendente), oppure si viene rediretti direttamente al servizio richiesto nel caso non ci sia ambiguità.

È possibile ottenere più informazioni a riguardo tramite il link **Maggiori informazioni sulla CIE** presente sulla schermata soprastante.

Accesso con SPID



Selezionando il tab **SPID**

è possibile autenticarsi utilizzando Sistema Pubblico di Identità Digitale.

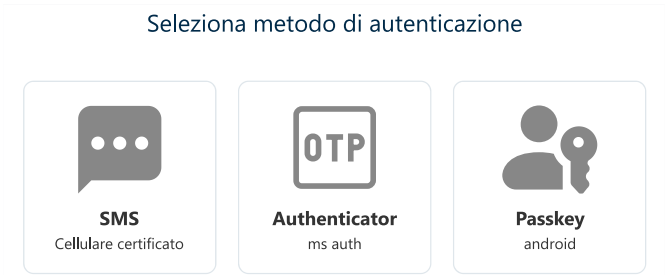
Facendo click su **Entra con SPID** è mostrato un selettore di fornitori SPID. È necessario selezionare il fornitore presso cui ci si è registrati; quindi, si verrà rediretti sul portale di autenticazione di tale fornitore. Se l'accesso viene eseguito correttamente, si viene riportati sul sistema di autenticazione che a questo punto può visualizzare un selettore (nel caso siano trovati nell'anagrafica di ateneo più profili corrispondenti al codice fiscale dell'utente, come ad esempio un profilo studente e uno dipendente), oppure si viene rediretti direttamente al servizio richiesto nel caso non ci sia ambiguità.

È possibile ottenere più informazioni a riguardo tramite il link **Maggiori informazioni su SPID** presente sulla schermata soprastante.

Accesso con secondo fattore di autenticazione

Nel caso si sia abilitato il secondo fattore di autenticazione, dopo l'inserimento delle credenziali si viene indirizzati alla pagina per la selezione del secondo livello di autenticazione. I metodi disponibili sono quelli che l'utente ha configurato.

L'utente deve selezionare uno dei metodi presenti

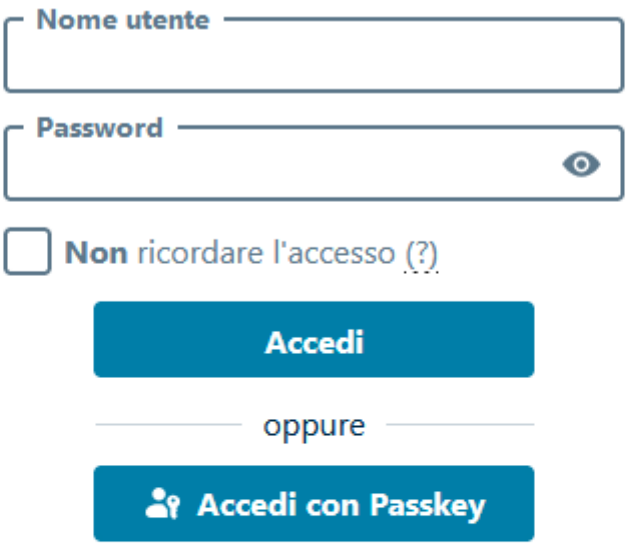


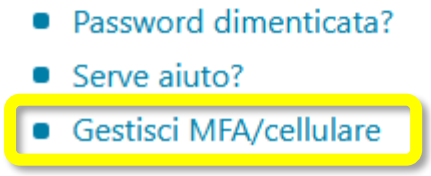
Selezionando un metodo di autenticazione si aprirà la corrisponde pagine della procedura di verifica.

A seconda del metodo selezionato può essere richiesto di inserire un codice fornito dal metodo di autenticazione selezionato oppure di seguire le informazioni a schermo. Questa procedura può dipendere dal sistema operativo e/o dal browser in uso. Fare riferimento ai link presenti alla fine di questo documento per ottenere maggiori informazioni in merito alla gestione delle Passkey sui browser più comuni.

Gestione autenticazione multi-fattore

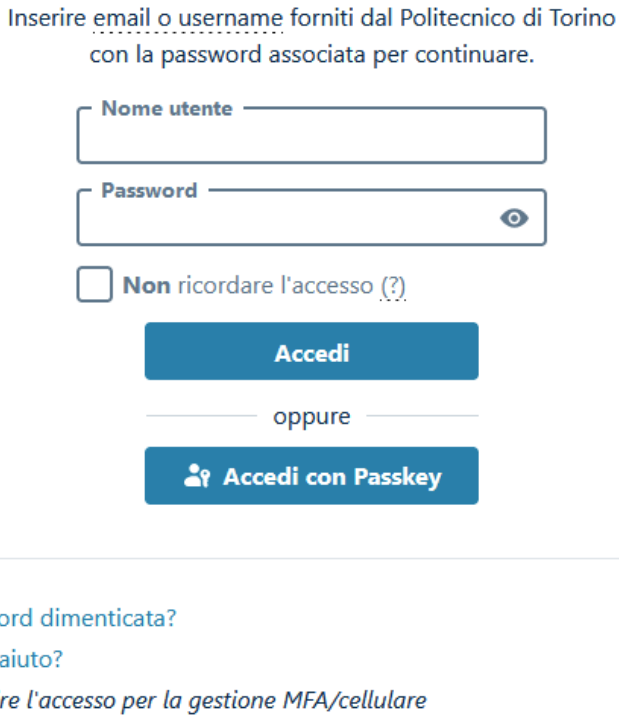
Selezionando la voce





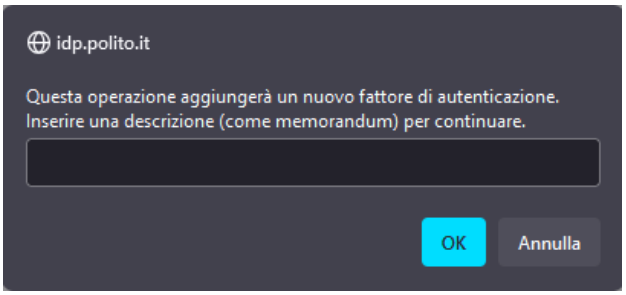
È possibile inserire nuovi metodi autenticazione di secondo livello.

Verrà richiesto di inserire delle credenziali valide per accedere alla sezione



una volta autorizzati sarà possibile aggiungere ulteriori metodi di autenticazione utilizzando la voce evidenziata

Selezionando una delle due voci OTP oppure Passkey, verrà richiesto di inserire un nome identificativo per il metodo utilizzato (a uso e discrezione dell'utente) che verrà presentato anche in fase di autenticazione. Per gli OTP, ad esempio, si potrebbe utilizzare "Authy motorola", oppure, per le Passkey "chrome laptop", etc.

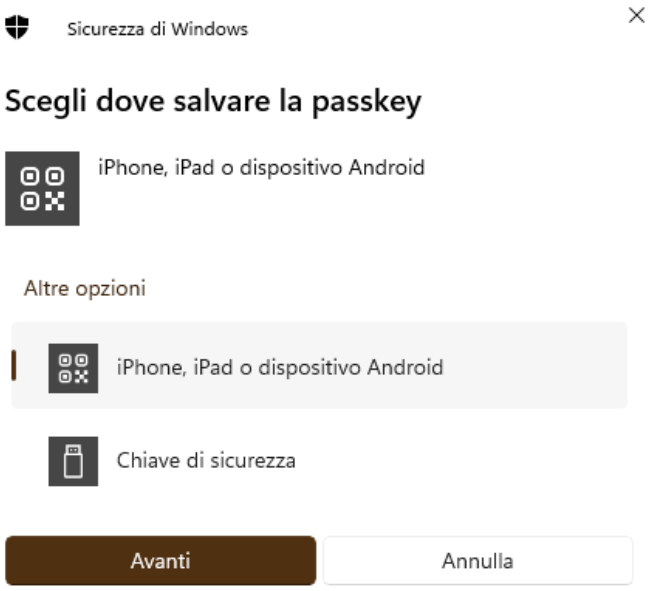


Nella schermata seguente, se si è scelto OTP, verrà richiesto di registrare un autenticatore (come ad es. Microsoft Authenticator, Authy, Google Authenticator, ecc.) tramite codice QR:

Scansionando il codice QRcode visualizzato tramite l'app di autenticazione con il dispositivo utilizzato per la generazione della OTP, sarà possibile aggiungere un nuovo metodo di autenticazione: questa procedura dipende dall'app di autenticazione utilizzata.

Attenzione: è importante che il codice QR non venga conservato in alcun modo. Non deve essere salvato, stampato o fotografato, in quanto una nuova scansione permette la generazione della stessa sequenza di codici. È anche necessario essere in un ambiente/contesto che non permetta ad altri di visualizzare o conservare il QR.

Selezionando Passkey, invece, verrà iniziata una procedura di salvataggio che dipende dal dispositivo e dal browser in uso: sarà necessario seguire la procedura a schermo.



Questa procedura dipende dal sistema operativo e/o dal browser in uso.

Occorre fare riferimento ai link presenti alla fine di questo documento per ottenere maggiori informazioni in merito alla gestione dei dispositivi più comuni.

Rimozione di un metodo di autenticazione

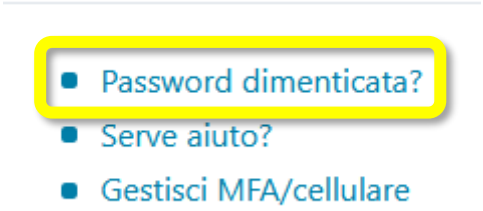
Passando il mouse (o toccando) su uno dei metodi di autenticazione aggiunti (Passkey/OTP) appare a lato il pulsante di eliminazione.

Notare che l'eliminazione di un metodo di autenticazione ne impedisce l'uso ma **non lo rimuoverà in automatico dall'autenticatore** su cui la credenziale risulta salvata. È quindi a cura

dell'utente la rimozione della Passkey o dell'OTP dall'app di autenticazione o dal gestore Passkey utilizzati.

Recupero password

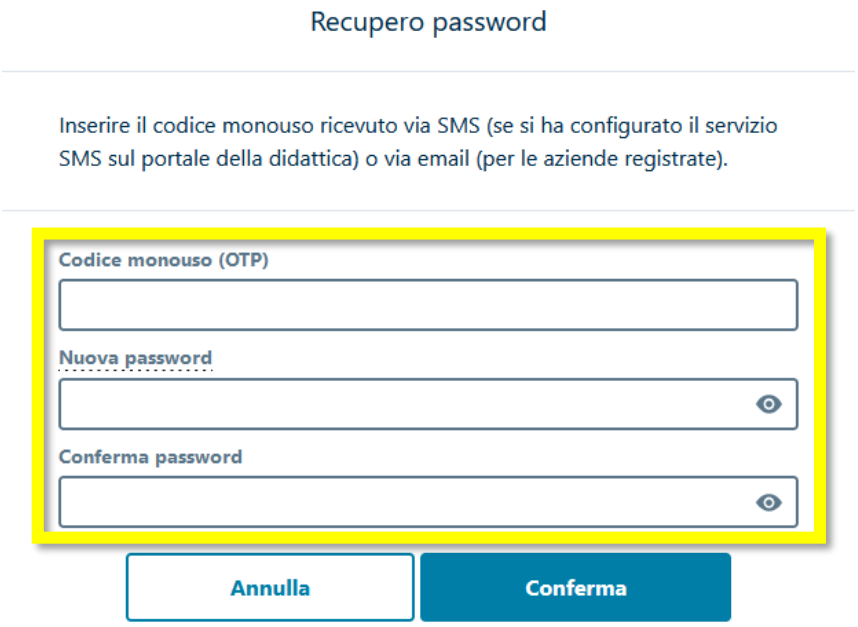
Selezionando



Sarà possibile richiedere una nuova password in caso di smarrimento.

Inserendo i dati richiesti nelle caselle evidenziate l'utente riceverà un messaggio SMS contenente una OTP

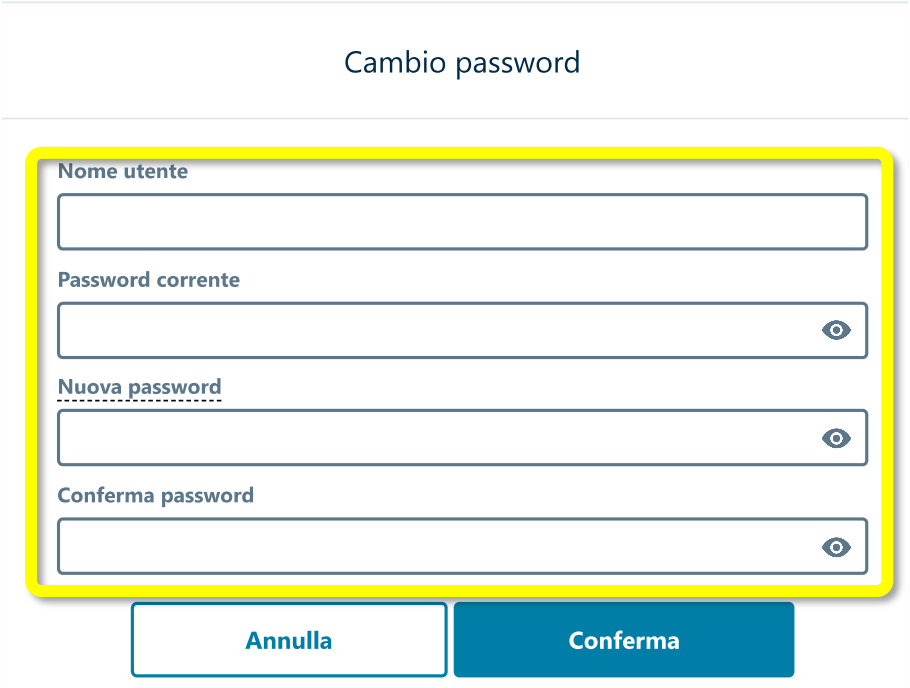
Inserendo il codice OTP ricevuto e la nuova password



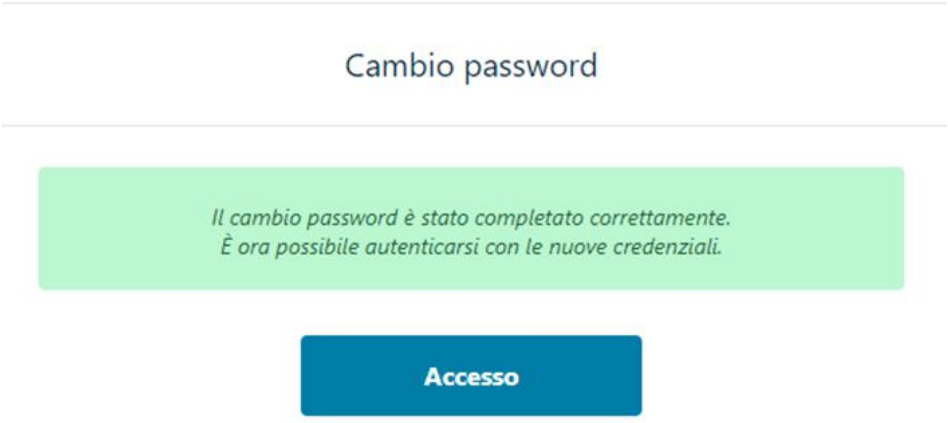
Potremo accedere alla procedura di login utilizzando la nuova password

Cambio password

Inserendo i dati richiesti nelle caselle evidenziate



Potremo accedere alla procedura di login utilizzando la nuova password



Per approfondire

Passkey

Gestione sui prodotti Google browser Chrome e sistemi Android:
https://support.google.com/accounts/answer/13548313

Gestione sul browser Firefox per Windows e MacOS:

https://support.mozilla.org/it/kb/compilazione-automatica-credenziali-firefox#w_passkey-in-firefox

Gestione su iPhone:

https://support.apple.com/it-it/guide/iphone/iphf538ea8d0/ios

Gestione su MacOS:

https://support.apple.com/it-it/guide/passwords/mchl4af65d1a/mac

Cie, SPID

https://www.cartaidentita.interno.gov.it/info-utili/identificazione-digitale

https://www.spid.gov.it/serve-aiuto