

# Autenticazione Sicura e Moderna

## MFA e Passkey nella migrazione a Shibboleth IdP 5

Andrea Garzena | Federico Cucinella

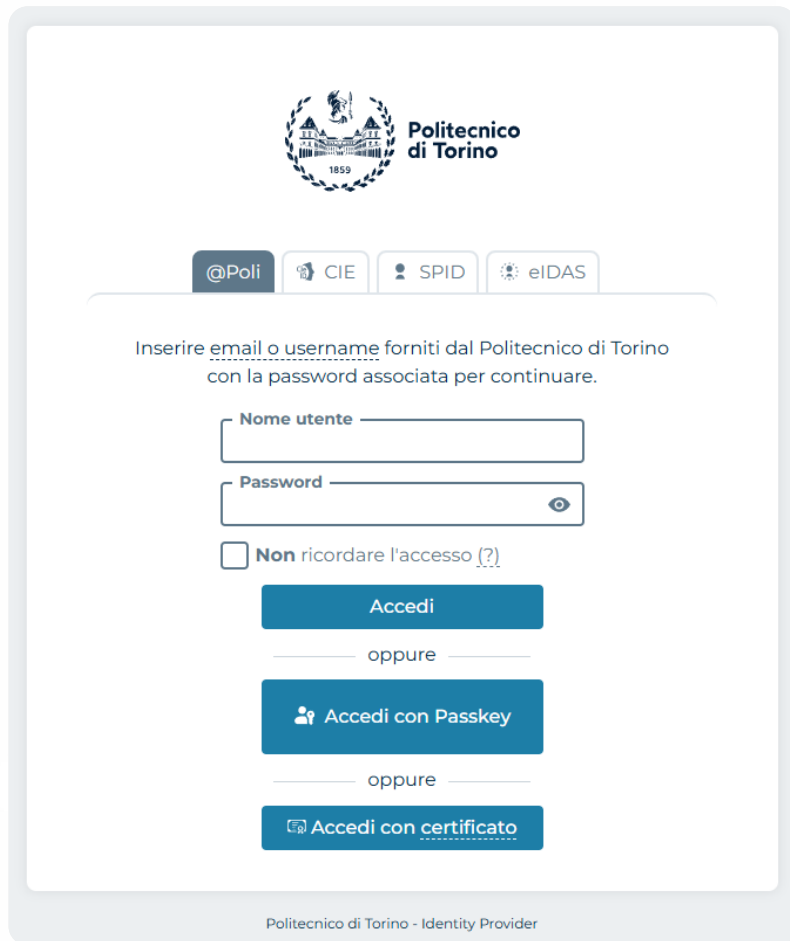
Politecnico di Torino



Politecnico  
di Torino

# Migrazione a Shibboleth IdP 5

## Un'evoluzione dell'autenticazione digitale



The screenshot shows the login page for the Politecnico di Torino Identity Provider. At the top, there is the university's logo and name. Below it, a navigation bar contains icons for '@Poli', 'CIE', 'SPID', and 'eIDAS'. The main content area features a text prompt: 'Inserire email o username forniti dal Politecnico di Torino con la password associata per continuare.' This is followed by two input fields: 'Nome utente' and 'Password' (with a toggle eye icon). A checkbox labeled 'Non ricordare l'accesso (?)' is positioned below the password field. Three blue buttons are stacked vertically: 'Accedi', 'Accedi con Passkey', and 'Accedi con certificato', separated by 'oppure' text. The footer of the page reads 'Politecnico di Torino - Identity Provider'.

- Contesto: gestione delle identità digitali al Politecnico di Torino
- Obiettivo: aggiornare l'IdP per sicurezza, efficienza e standard attuali
- Sfide: continuità del servizio, refactoring configurazioni, nuova infrastruttura

# Nuove funzionalità

## Esperienza utente e sicurezza migliorate

- Sessioni di lunga durata
- Gestione self-service delle sessioni con informazioni dettagliate
- Gestione MFA integrata
- Logout unificato (Single Log-Out)
- Cambio profilo nativo (studente ↔ staff)
- Integrazione con CIE, SPID, eIDAS
- Accesso federato IDEM/eduGAIN
- Autenticazione per Microsoft 365

The image displays two overlapping screenshots of the Politecnico di Torino's MFA management interface. The top screenshot shows the 'Gestione MFA' (MFA Management) page, which includes the university logo and the following sections:

- SMS:** PISM000009A9, Cellulare certificato, Ultimo utilizzo: 2025-03-26 08:35
- OTP:** TOTP0001DF51, authenticator, Ultimo utilizzo: 2024-12-07 19:51
- Passkey:** WAN0309B674, bwrdr, Ultimo utilizzo: 2025-05-05 15:36

Below these methods is a dropdown menu labeled 'Aggiungi metodo di autenticazio' and a blue 'Indietro' (Back) button.

The bottom screenshot shows the 'Sessioni attive' (Active Sessions) page, also featuring the university logo. It lists three active sessions with the following details:

- ID sessione:** 0109bcb9 [attiva]  
• IP primo login: 130.192.89.93  
• Prima autenticazione: lun 14 apr 2025 - 11:23:44  
• Scadenza: mer 14 mag 2025 - 12:04:55  
• MFA:  Passkey - WAN0005D154  
• Browser: Chrome (135) - Linux (amd64)  
• Utilizzata in: 2 servizi
- ID sessione:** c9431cbe [attiva]  
• IP primo login: 130.192.89.93  
• Prima autenticazione: ven 18 apr 2025 - 12:28:46  
• Scadenza: dom 18 mag 2025 - 12:39:31  
• MFA:  CIE  
• Browser: Chrome (135) - Linux (amd64)  
• Utilizzata in: 3 servizi
- ID sessione:** ce4fcdf [attiva]  
• IP primo login: 130.192.89.93  
• Prima autenticazione: ven 18 apr 2025 - 12:31:40  
• Scadenza: dom 18 mag 2025 - 12:41:40  
• MFA:  SPID - https://posteid.poste.it  
• Browser: Chrome (135) - Linux (amd64)  
• Utilizzata in: 1 servizio

# Una transizione senza interruzioni

## Strategie adottate



- Valutazione iniziale e pianificazione dettagliata
- Reinstallazione completa in ambiente protetto
- Test approfonditi in ambiente di staging
- Redazione di manuali e informazione agli utenti
- Supporto proattivo e monitoraggio durante la fase iniziale

# Verso un'autenticazione moderna

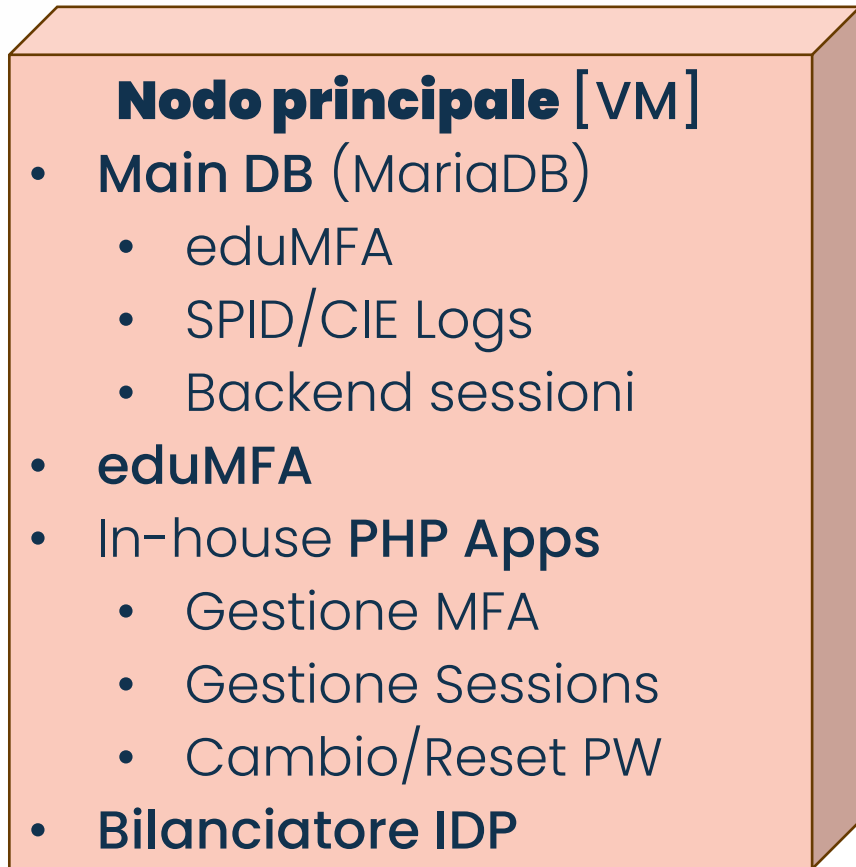
## MFA e Passkey | Implementazione

- Fudiscr & «Fudispasskeys»
  - Passkeys considerate trusted by-design
  - 2° fattore richiesto condizionalmente
- eduMFA
  - Accesso UI riservato admin
  - Gestione metodi semplificata via applicativo PHP in-house
- MFA interno non richiesto per CIE/SPID
  - Quando la risposta, validata, è almeno L2

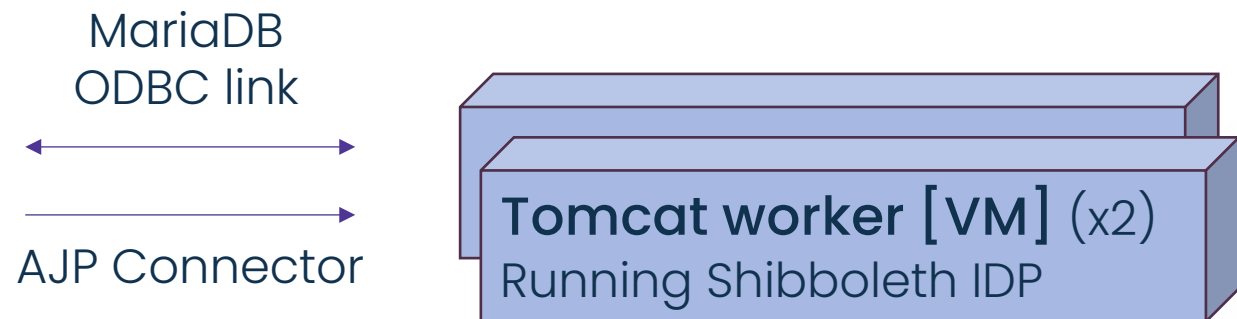


# Resilienza e scalabilità

## Cenni infrastrutturali



- Esecuzione delle 3 VM su cluster HA on-premise
- Autenticazione password su AD/LDAP interno
- Possibilità di scalare ulteriormente clusterizzando il DB e/o eduMFA



**Grazie per l'attenzione**

[andrea.garzena@polito.it](mailto:andrea.garzena@polito.it)  
[federico.cucinella@polito.it](mailto:federico.cucinella@polito.it)



**Politecnico  
di Torino**