

The New IDP of Politecnico di Torino

[ITA](#) | [ENG](#)



Politecnico di Torino

@Poli Cert CIE SPID

To sign-in, use the username or email address provided by Politecnico di Torino and the associated password.

Username

Password

Do **not** remember login (?)

Login

or

Login with Passkey

- [Forgot your password?](#)
- [Need Help?](#)
- [Manage MFA/mobile](#)

Summary

Summary	1
What is an IDP and What is it Used For.....	2
Features of the New IDP	3
Credential Management	5
Login Operations on the IDP	7
Multi-Factor Authentication Management	16
Password Recovery	20
Password Change	22
For Further Information.....	23

What is an IDP and What is it Used For

The Identity Provider (IDP) is a system that manages user authentication, allowing users to access multiple applications and services using a single digital identity.

The new IDP of the Politecnico di Torino represents a significant step forward in digital identity management. This system not only retains all the functionalities of the previous version but also introduces a series of improvements that enhance its efficiency and security.

Integrated with the IDEM and eduGAIN networks, the new IDP enables users to authenticate and access federated services both nationally and internationally. This is particularly useful for students and staff who need to access resources and services provided by other institutions within these networks. Additionally, the system is configured to support **MyAcademicID**, an initiative that allows students to access Erasmus+ services using their university credentials.

Among the key features of the new IDP is support for unified Single Sign-On (SSO) and Single Log-Out (SLO), enabling users to log in and out of online services with a single credential. This simplifies the user experience, reducing the need to remember multiple passwords. Moreover, the new IDP supports various authentication methods, including passwords, CIE (Electronic Identity Card), SPID (Public Digital Identity System), Digital Certificates, and Passkeys. To further enhance security, multi-factor authentication (MFA) is also available, requiring an additional verification step beyond the password.

In summary, the new IDP of the Politecnico di Torino provides a modern and secure solution for digital identity management, facilitating access to a wide range of services and resources both nationally and internationally.

Features of the New IDP

The new IDP of Politecnico di Torino retains, where possible, all the features of the previous system, but with significant improvements:

1. Federated Identities

Allow users to access external services using credentials provided by Politecnico di Torino.

IDEM Federation

IDEM is the Italian Federation of Authentication and Authorization Infrastructures (AAI), designed to facilitate access to online services and content provided by various organizations for the national scientific and academic community.

eduGAIN Access

eduGAIN is the inter-federation service that connects and enables cooperation among identity federations worldwide. It allows users to access international services using their institutional credentials, promoting collaboration and access to global resources[1].

MyAcademicID

MyAcademicID is a project funded by the Connecting Europe Facility program. It enables students to authenticate for studies abroad using their home institution accounts. The project integrates academic identities with personal ones via eIDAS national nodes, reducing administrative burden for both staff and students[3].

2. Unified Single Sign-On and Single Logout

The unified Single Sign-On and Single Logout system allows long-term authentication session storage across all university systems. For trusted devices, this enables users to remain authenticated for up to 90 days from the initial login. When accessing from an untrusted device, it is advisable to select the checkbox below the credential input fields to prevent long-term session storage.

Do **not** remember login (?)

3. Authentication Methods

The authentication methods provided by the new University IDP are:

- *Password*: requires users to enter a secret combination of characters known only to them to verify their identity.
- *CIE* (Electronic Identity Card): allows users to verify their identity using their electronic identity card, which contains personal information and a digital certificate for secure access
- *SPID* (Public Digital Identity System): enables users to access online services of Public Administration and affiliated private entities using a single verified digital identity, ensuring secure and simplified access.
- *Certificato Digitale*(*Digital Certificate*): allows users to verify their identity using a digital certificate containing encrypted, unique information for secure access.

- *Passkey*: Enables users to access online services using a unique cryptographic key, eliminating the need to input a username or remember a password, offering enhanced security.
- *Multi-Factor Authentication (MFA)*: To enhance security, the system may require an additional factor (e.g., Passkey, OTP from an authentication app, or SMS) after username and password login. This reduces the risk of unauthorized access to sensitive data or critical user operations in a unified way, without delegating implementation to individual applications.
- *Biometric Authentication Systems*: By leveraging Passkeys, users can utilize biometric systems on their devices (fingerprint, facial recognition, etc.) for secure access to university services.

The new IDP integrates advanced procedures for password management (renewal, change, and recovery) and MFA system management (addition, modification, and removal of methods). These features allow users to keep their credentials up-to-date and secure, reducing the risk of unauthorized access. The system guides users through intuitive processes for periodic credential updates, recovery in case of loss, and renewal when needed, ensuring efficient and secure management.

MFA will become the sole method for accessing all online services.

Credential Management

Username and **password** are unique access information assigned to each user to ensure security and authentication in IT systems. Credentials are provided for the first time during the user's registration in the system, allowing initial access to the available services and resources

Username

The username provided to employees is generally in the format:

firstname.lastname@polito.it e.g., mario.rossi@polito.it

The username provided to students is in the format:

Smatricola@studenti.polito.it e.g., S123456@studenti.polito.it

Password

The University's IDP requires passwords to meet the following minimum requirements:

1. Minimum length of 14 characters.
2. Maximum length of 20 characters.
3. Contain at least one lowercase letter from a to z.
4. Contain at least one uppercase letter from A to Z.
5. Do not contain accented letters.
6. Contain at least one number from 0 to 9.
7. Contain at least one special character (non-alphanumeric) from the following set:
@#?.,<>!%&\+_-/=; ()^|`.
8. Be different from the last five passwords used.

This type of password increases complexity and makes it more difficult for attackers to guess or brute force access, ensuring greater protection of personal information and sensitive data.

CIE (Electronic Identity Card)

To obtain CIE credentials, it is necessary to request the card from the municipality of residence. Once issued, the CIE contains a digital certificate that enables secure authentication to online services.

During the issuance process, instructions for activating and using the card will be provided, including the PIN and PUK codes required for access.¹

SPID (Public Digital Identity System)

To request SPID credentials, several steps must be followed. First, choose one of the authorized identity providers, which offer different levels of security and access methods. Registration can be done online, via webcam recognition, in person at the provider's offices, or using a CIE (Electronic Identity Card) or CNS (National Service Card). During registration, some personal data, a valid identity document, and the tax code will be required. Once the procedure is completed, SPID credentials will be issued.

Digital Certificate

The digital certificate is a `.p12` file issued by the Certification Authority of Politecnico di Torino. It contains personal information needed to identify the user to whom it is issued.

It can be used for authentication on websites (e.g., the Didactic Portal), to digitally sign documents and emails, and to securely encrypt data and email messages. The electronic signature made with this certificate does not have legal value and is recognized only by Politecnico di Torino and other entities that consider it reliable.

Passkey

It is possible to set up one or more Passkeys for each account held at Politecnico di Torino. The Passkey is registered like any other multi-factor authentication method at <https://idp.polito.it/tokens> or following the instructions in the MFA Management section. Unlike other authentication factors, once registered, it can also be used as the primary (and only) authentication factor, being inherently more secure than the traditional username/password combination.

It is important to note that the entire Passkey ecosystem is heavily dependent on the user's device, browser, and/or operating system.

Sono state testate le seguenti configurazioni:

The following configurations have been tested:

- Microsoft Windows Environment – browser-dependent:
 - Google Chrome
 - Microsoft Edge
 - Mozilla Firefox

- Android Environment – system credential manager-dependent:
 - Google Password Manager
 - Samsung Pass

- Apple Environment – browser-dependent
 - Google Chrome
 - Mozilla Firefox
 - Safari
 - Password App (iOS 18 and later)

In any case, the correct functioning of Passkeys is also tied to the hardware responsible for securely storing the associated certificates.

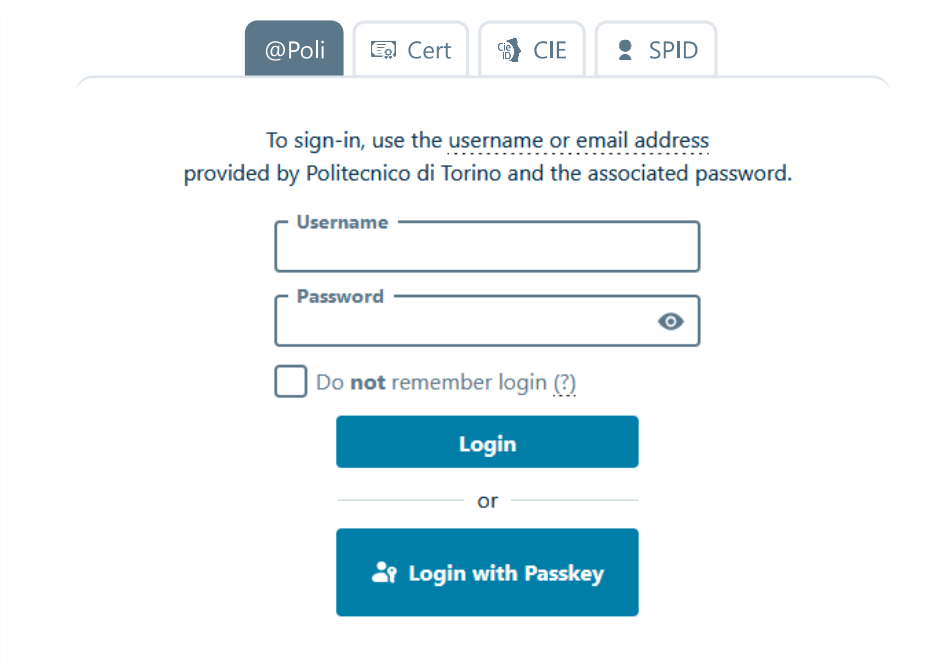
Other systems or contexts may work without issues, but given the high number of combinations, it is not possible to provide documentation for each one.

Passkey storage management is closely tied to the device/browser/operating system/credential manager used. Despite the standard providing strict security measures regarding the storage of associated certificates, the user is considered responsible for the security of the environment where the Passkeys associated with their University accounts are saved.

If Passkeys are saved in cloud environments (e.g., the user's personal Google account) and this environment is compromised, the user must promptly remove the reference to such Passkey from their management area to prevent misuse. .

Login Operations on the IDP

Access with Username and Password

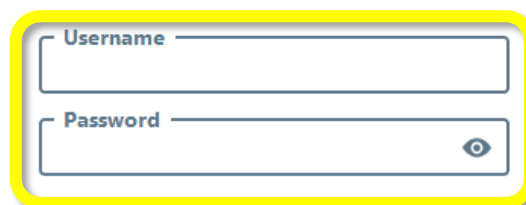


The screenshot shows the login interface with four tabs: @Poli, Cert, CIE, and SPID. The @Poli tab is selected. Below the tabs, the text reads: "To sign-in, use the username or email address provided by Politecnico di Torino and the associated password." The form contains a "Username" input field, a "Password" input field with a visibility toggle, a checkbox labeled "Do not remember login (?)", a blue "Login" button, the word "or" in the center, and a blue "Login with Passkey" button with a key icon.

Selecting the @Poli Tab

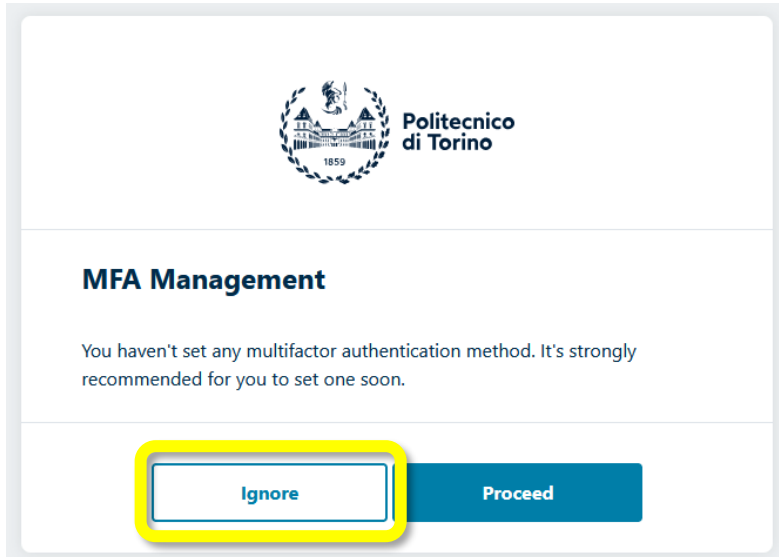


The login process uses the credentials provided and managed directly by the University. To log in with your username and password, enter your credentials in the highlighted fields.



A close-up of the login form's input fields. The "Username" and "Password" fields are highlighted with a yellow border, indicating where the user should enter their credentials.

During the first login, or if no multi-factor authentication method has been configured, you will be prompted to activate one.



If you select Ignore the authentication process ends regularly with the classic username and password method. However, the system periodically requests you to configure and use a two-factor authentication method until at least one second authentication factor is set.

The two-factor authentication procedure is strongly recommended, and once at least one second factor is configured, it will be required for every login.

If the user chooses to activate multi-factor authentication, the system proceeds with the configuration by sending an OTP via SMS as the second factor. If not already present in the system, you will be asked to enter your mobile number to receive SMS during all subsequent authentications.



MFA Management - Mobile

Setting up the mobile number allows two-factor authentication and autonomous password reset in case of password loss.

Changes of the mobile number will trigger a confirmation SMS.

The mobile number hasn't been verified. Please proceed with the verification.

Cancel

Confirm

Note: The user must have their mobile phone on hand and be in an area with good reception. If the user has already registered a mobile number on MyPoli or the Teaching Portal, the system presents it, allowing the user to change it if necessary.

The mobile number hasn't been verified. Please proceed with the verification.

To verify the mobile number, the system will send an OTP via SMS. The user must enter it in the One-Time Code (OTP) field.

Note: To prevent attack procedures and account compromise, the time for completing the field is intentionally limited. It is not possible to start and finish the procedure later.



MFA Management

Please insert the OTP received through SMS to complete the enrolment. If you don't receive any message within 2 minutes, please go back to retry.

One-Time-Password

[Back](#)

Once the OTP code received via SMS is entered, on the next page, the system summarizes the multi-factor authentication systems activated. The SMS method just configured will appear.

[ITA](#) | [ENG](#)



MFA Management



SMS: **PISM00223F37**

Certified mobile

Last usage: never

Add authentication method ▼

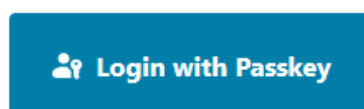
[Complete authentication](#)

By selecting “Complete Authentication,” the access procedure is completed, and you are redirected to the requested service.

From subsequent login requests, the portal will always ask for the second authentication factor.

It is recommended to configure additional MFA systems in addition to the SMS method. Please refer to the complete guide for further details.

By selecting the button,



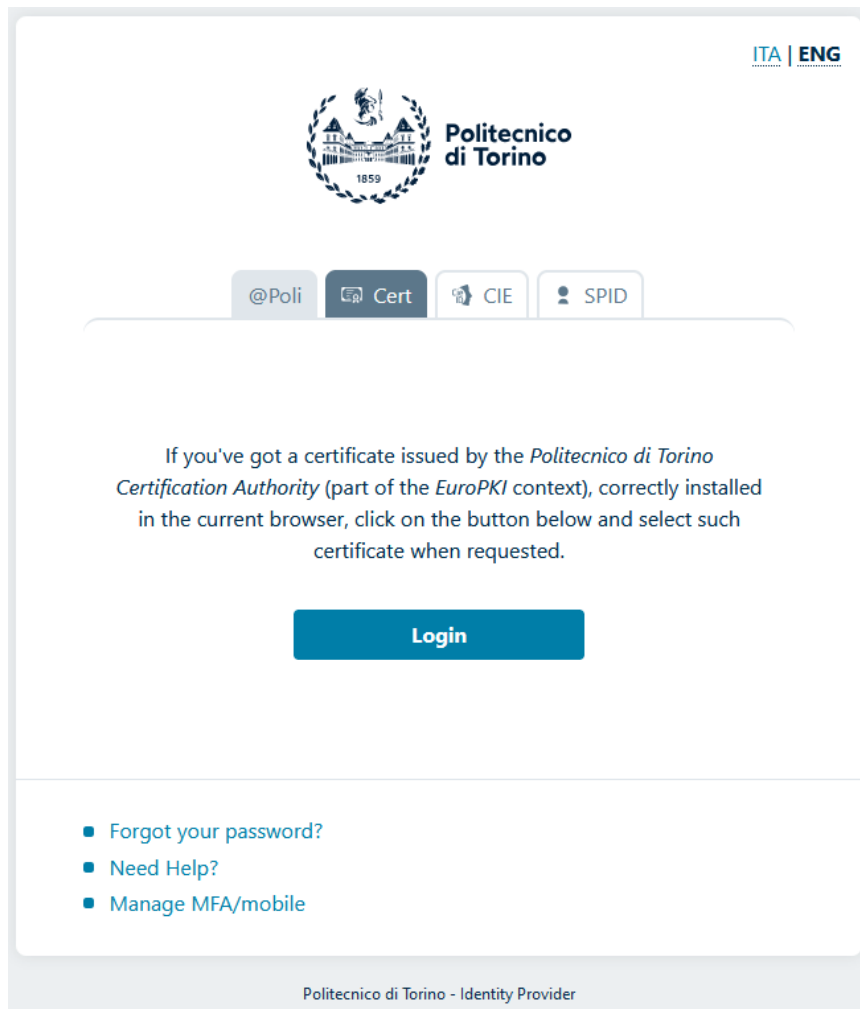
the login procedure using a Paskey will begin. This process depends on the operating system and/or browser being used.

To authenticate, at least one Paskey system must have been configured.

The Paskey authentication system is equivalent to two-factor authentication, as it typically requires two different devices to complete the process.

Refer to the links at the end of this document for more information on the most common Paskey managers.

Access with Certificate Issued by Politecnico di Torino



By selecting the **Cert** tab

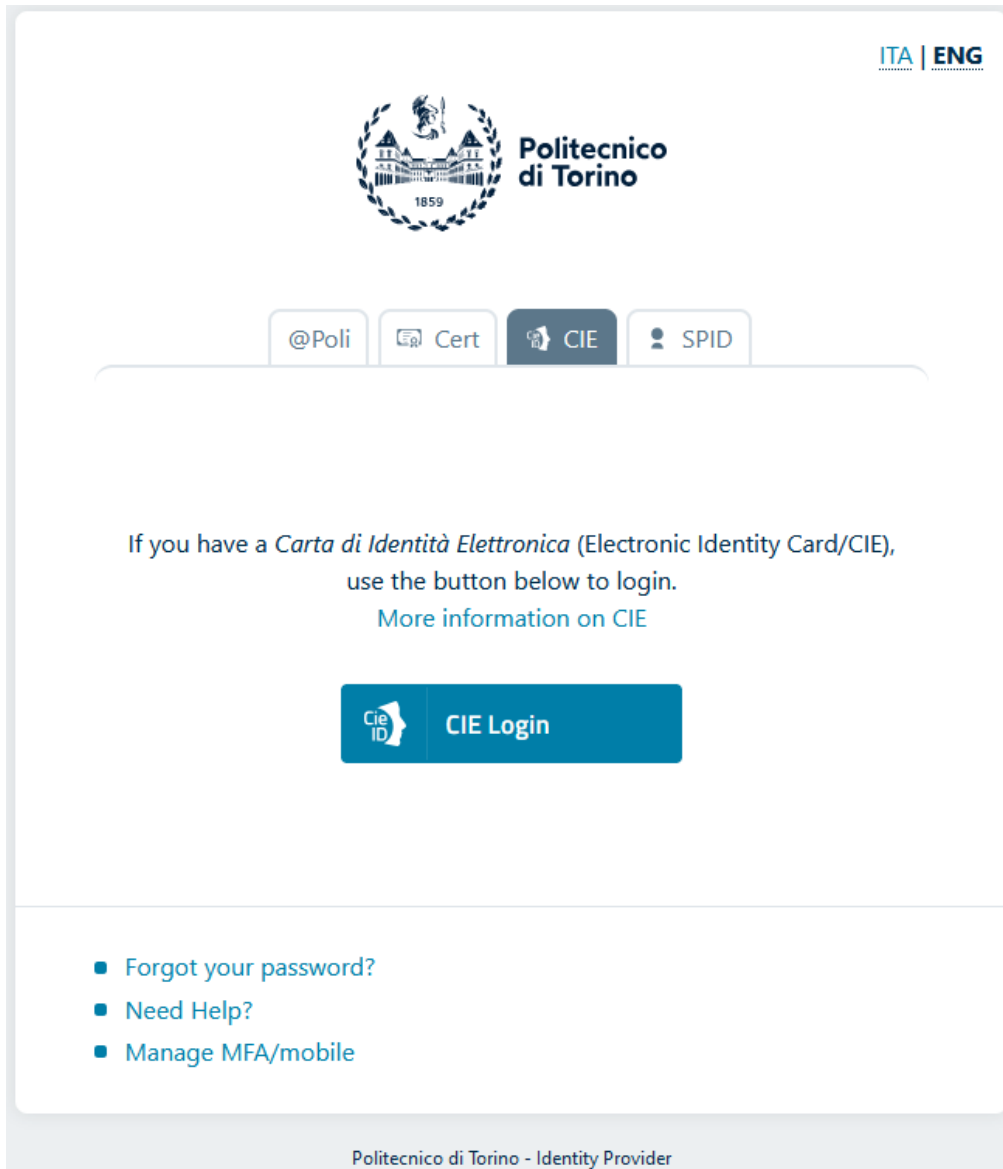


you can log in using the certificate stored in the browser being used for access.

This procedure depends on the operating system and/or browser in use.

Refer to the links at the end of this document for more information on managing certificates in the most commonly used browsers.

Access with CIE (Electronic Identity Card)



By selecting the **CIE** tab,

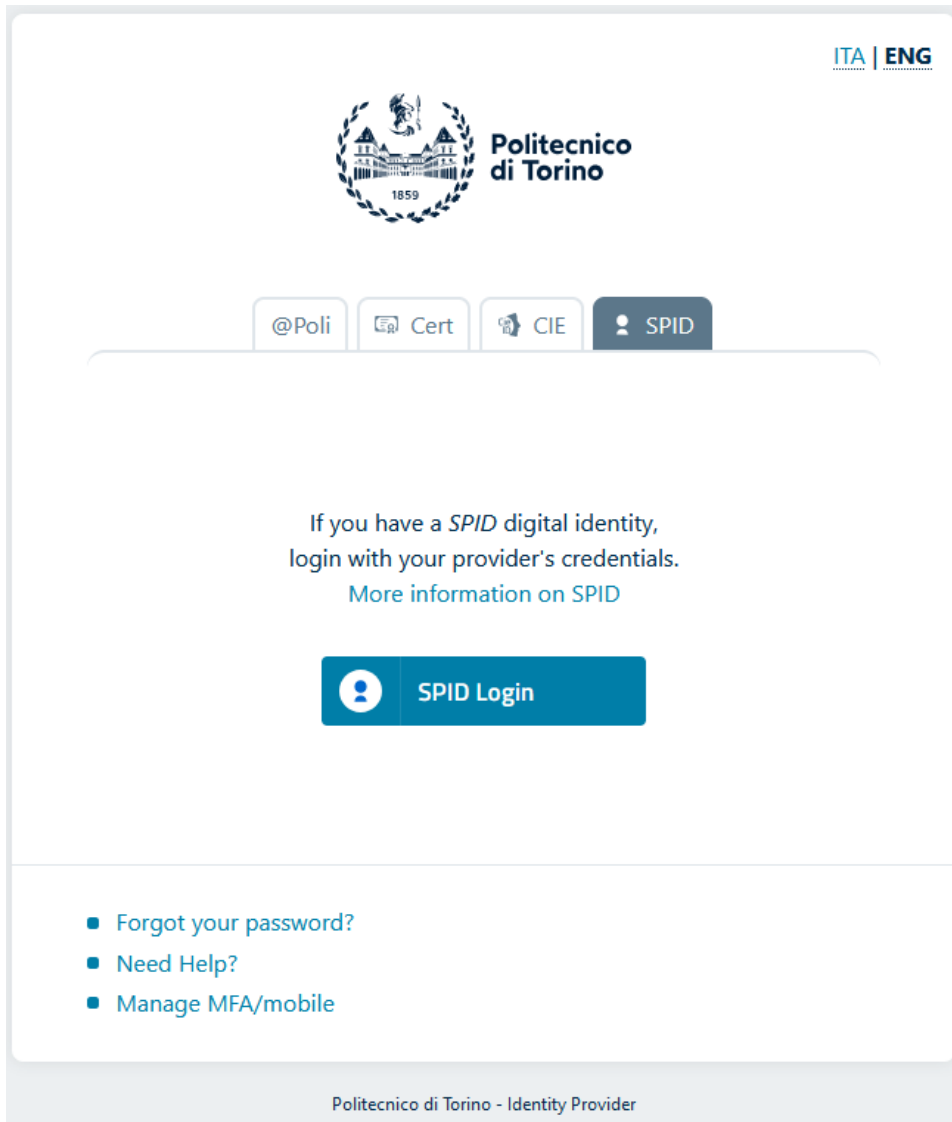


you can authenticate using your Electronic Identity Card.

Clicking on **CIE Login** redirects you to the CIE authentication portal to proceed with the login. If the process is successful, you will be returned to the authentication system, which may display a selector (if multiple profiles corresponding to the user's tax code are found in the university records, such as a student profile and an employee profile), or you will be redirected directly to the requested service if no ambiguity exists.

For more information, refer to the **More information on CIE** link available on the preceding screen.

Access with SPID (Public Digital Identity System)



By selecting the **SPID** tab,



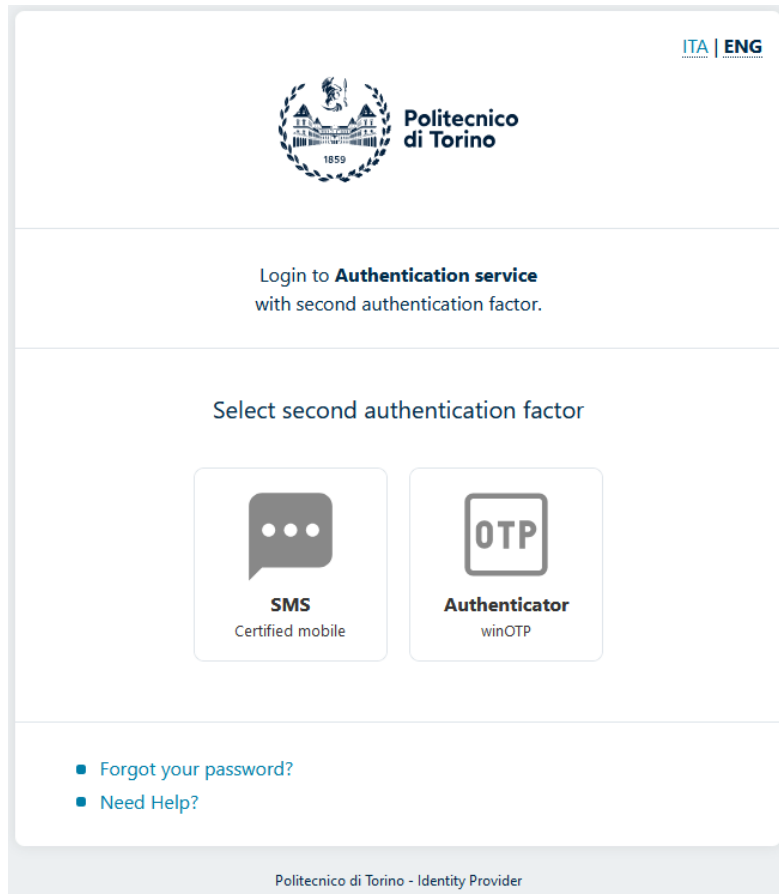
you can authenticate using the Public Digital Identity System.

Clicking on **SPID Login** displays a list of SPID providers. You must select the provider where you registered, after which you will be redirected to the authentication portal of that provider. If the login process is successful, you will be returned to the authentication system, which may display a selector (if multiple profiles corresponding to the user's tax code are found in the university records, such as a student profile and an employee profile), or you will be redirected directly to the requested service if no ambiguity exists.

For more information, refer to the **More information on SPID** link available on the preceding screen.

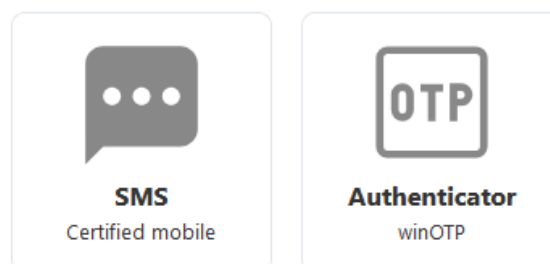
Access with Multi-Factor Authentication

If multi-factor authentication (MFA) has been enabled, after entering your credentials, you will be directed to a page for selecting the second authentication level. The available methods are those that the user has configured.



The user must select one of the available methods

Select second authentication factor



Upon selecting an authentication method, the corresponding verification process page will open. Depending on the selected method, you may be required to input a code provided by the chosen authentication method or follow the on-screen instructions.

This procedure may vary depending on the operating system and/or browser being used. Refer to the links at the end of this document for more information on managing Passkeys in commonly used browsers.

Multi-Factor Authentication Management

By selecting the relevant option

Username

Password

Do **not** remember login (?)

Login

or

Login with Passkey

- [Forgot your password?](#)
- [Need Help?](#)
- [Manage MFA/mobile](#)

you can add new second-level authentication methods.

You will be prompted to enter valid credentials to access the section.

To sign-in, use the username or email address provided by Politecnico di Torino and the associated password.

Username

Password

Do **not** remember login (?)

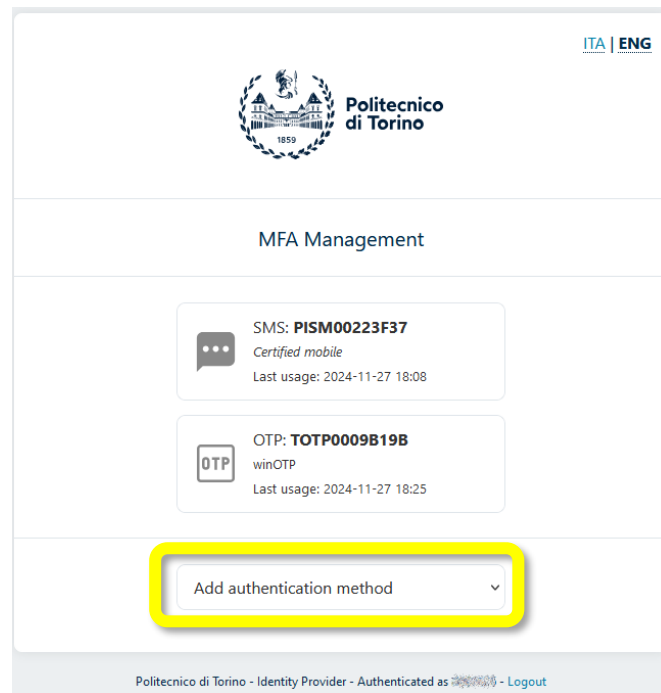
Login

or

Login with Passkey

- [Forgot your password?](#)
- [Need Help?](#)
- [Please login to manage MFA/mobile](#)

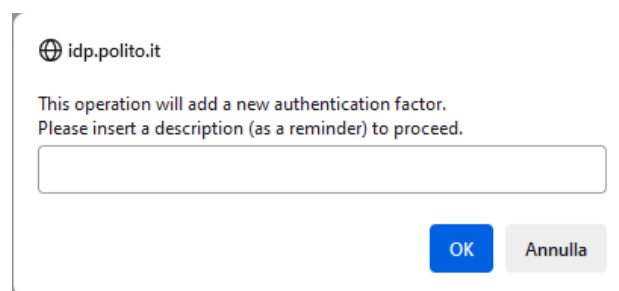
Once authorized, you can add additional authentication methods using the highlighted option.



When selecting either **OTP** or **Passkey**, you will be asked to assign a descriptive name to the chosen method (at the user's discretion), which will also be displayed during authentication.

For example:


- For OTP, you might use "Authy Motorola."
- For Passkey, you could use "Chrome Laptop," etc.



In the Next Screen, If you select **OTP**, you will be prompted to register an authenticator (e.g., Microsoft Authenticator, Authy, Google Authenticator) using a QR code:

:

MFA Management



Please scan the QR code using an authenticator app (like Google or Microsoft Authenticator).

Please insert the generated OTP to complete the enrolment.

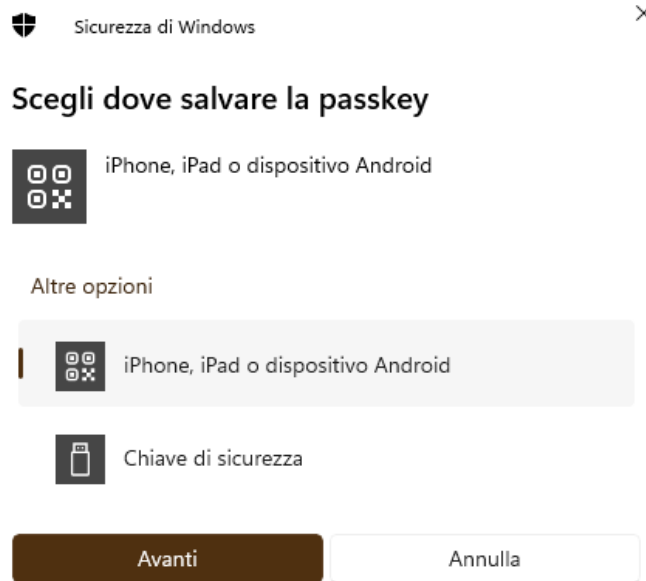
One-Time-Password

Scan the displayed QR code with the authentication app on the device you intend to use for OTP generation. This process depends on the specific authentication app being used.

Important:

- The QR code must not be stored in any way.
- It should not be saved, printed, or photographed, as a new scan would generate the same sequence of codes.
- Ensure you are in an environment or context that prevents others from viewing or saving the QR code.

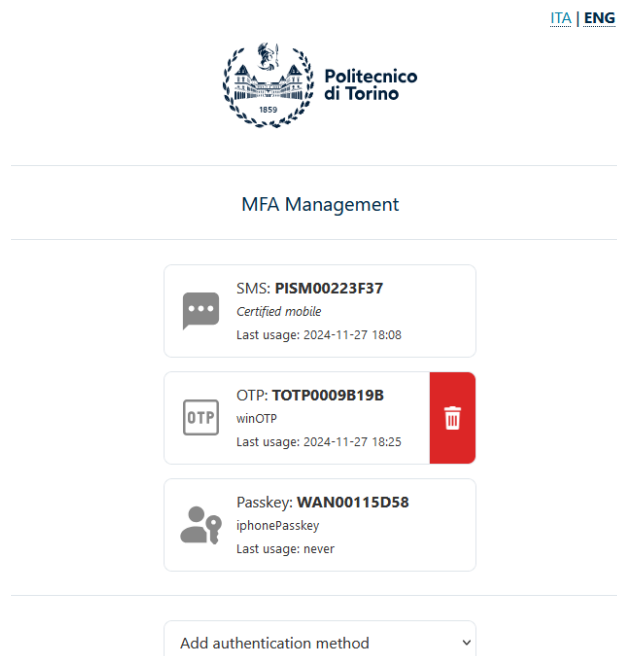
If you select **Passkey**, a saving process will begin, which depends on the device and browser in use. You will need to follow the on-screen instructions to complete the setup



This process depends on the operating system and/or browser being used. Refer to the links at the end of this document for more information on managing the most commonly used devices.

Removing an Authentication Method

Hovering the mouse (or tapping) over one of the added authentication methods (Passkey/OTP) will display a delete button next to it.



Deleting an authentication method will disable its use but will not automatically remove it from the authenticator where the credential is saved. It is the user's responsibility to remove the Passkey or OTP from the authentication app or Passkey manager being used

Password Recovery

By selecting the relevant option

- **Forgot your password?**
- Need Help?
- Manage MFA/mobile

you can request a new password in case of loss.

Enter the required information in the highlighted fields, and you will receive an SMS containing a one-time password (OTP).

[ITA](#) | [ENG](#)



Password reset

Self password reset procedure requires to be subscribed to the text message service on the teaching portal. For companies, you must be registered with the *career service*.

This procedure allows you to receive an SMS or an email with a one-time-password (OTP) you can use to reset the account password.

Email address or username

Fiscal code or VAT number

[Back](#) [Confirm](#)

After entering the received OTP and the new password

Password reset

Insert the OTP received via SMS (for those subscribed to the SMS service on the teaching portal) or via email (in case of registered companies).

One-Time-Password

New password

Confirm password

you will be able to proceed with the login process using the newly set password.

Password reset

*The password change has been completed successfully.
It is now possible to proceed logging in using the new credentials.*

Login

Password Change

By entering the required information in the highlighted fields,

Change password

Username

Current password
New password
Confirm password

you can proceed to set a new password.

Once the password change is complete, you can use the new password to access the login procedure.

Password reset

*The password change has been completed successfully.
It is now possible to proceed logging in using the new credentials.*

For Further Information

Passkey

Management on Google Chrome browser and Android systems:

<https://support.google.com/accounts/answer/13548313>

Management on Firefox browser for Windows and MacOS:

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

Management on iPhone:

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

Management on 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>