UNIVERSITÀ di VERONA

MFA – GUIDA OPERATIVA - ANDROID

DIREZIONE SISTEMI INFORMATIVI E TECNOLOGIE
AREA SISTEMI DI CALCOLO

Sommario

Android

MFA - Autenticazione a Fattori Multipli presso l'Università degli Studi di Verona

L'obiettivo della MFA[1] è quello di tenere al sicuro i propri account e ridurre al minimo i rischi per la sicurezza: rendere più difficile per una persona non autorizzata accedere a risorse protette.

L'autenticazione a più fattori (MFA) è un sistema di sicurezza che utilizza più metodi di autenticazione per verificare l'identità dell'utente che desidera accedere.

L'Università degli Studi di Verona per l'accesso ad Office 365 implementa una MFA a 2 fattori:

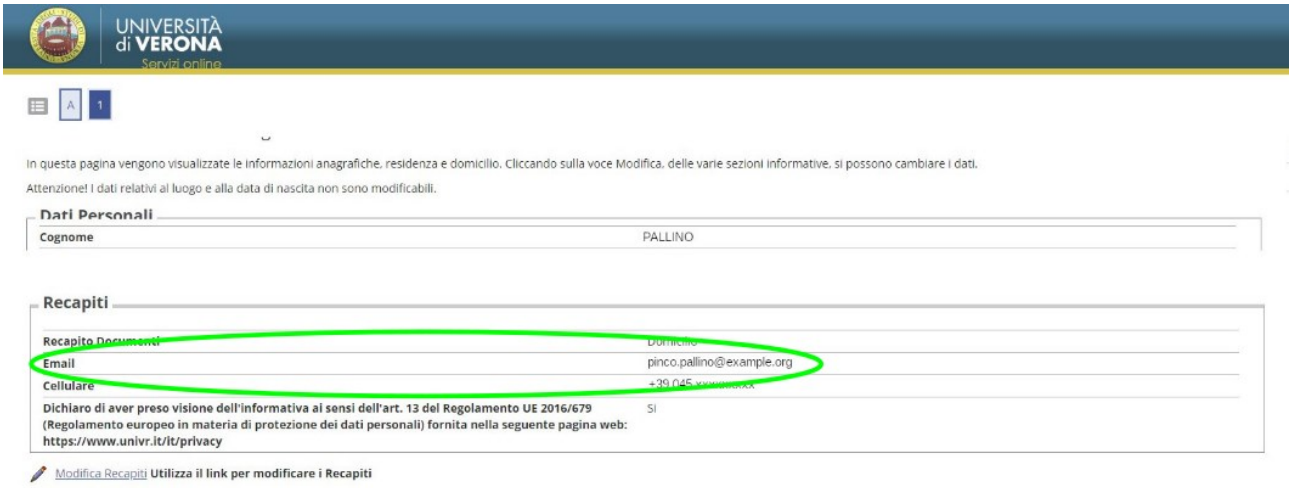
- 1° fattore di autenticazione: **login/password GIA**
- 2° fattore di autenticazione: **Token[2] di Accesso Temporaneo**

Il token può essere fornito con due modalità:

- **OTP** (One Time Password) comunicazione del codice di sicurezza all'*email privata* registrata in GIA
- **TOTP** (Time-Based One Time Password) comunicazione del codice di sicurezza utilizzando *Applicazioni Mobile* (Microsoft Authenticator, Google Authenticator, 2FA, …) o A*pplicativi Desktop* in grado di supportare lo standard (es. KeepassXC).

La prima modalità (OTP) funziona senza alcuna configurazione dell'utente che deve controllare la correttezza della propria email privata fornita all'università. Tale controllo è possibile accedendo al proprio profilo in ESSE3 carriere studenti (per gli studenti) o a DBERW (per il personale TA/docenti)**:**

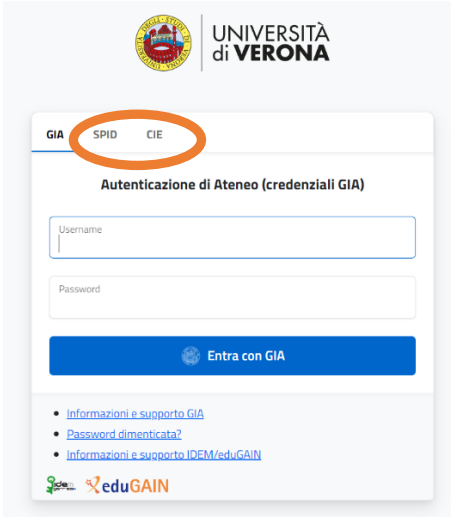
- ✓ ESSE3 – Studenti



[1] MFA = Multi Factor Authentication
[2] TOKEN = Termine informatico, individua un oggetto fisico o logico necessario per l'MFA
(E' tipicamente un codice numerico)

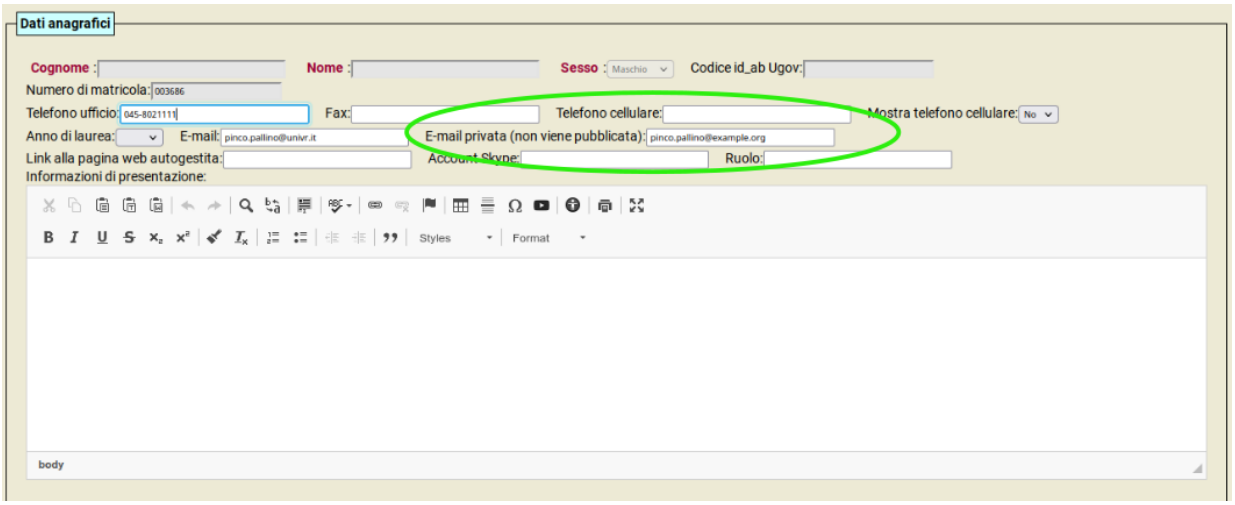
✓ Dberw – Personale

Accedere a Dberw con **SPID** o **CIE**:



Scegliere la prima opzione “Selezionare l’Utenza GIA XXXXX”:

Selezionare “Dati personali”, poi selezionare il proprio nome e cliccare su “Modifica”:



Inserire la mail desiderata nel campo “E-mail privata (non viene pubblicata)”.

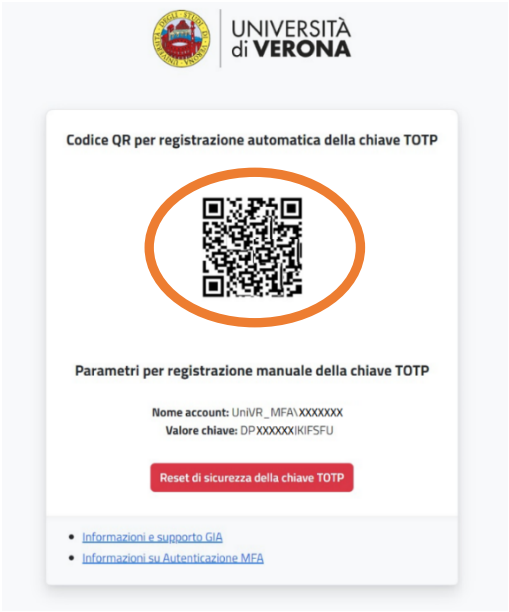
La seconda modalità (TOTP) permette la generazione del token anche in assenza di connettività di rete.

Per questa modalità bisogna:

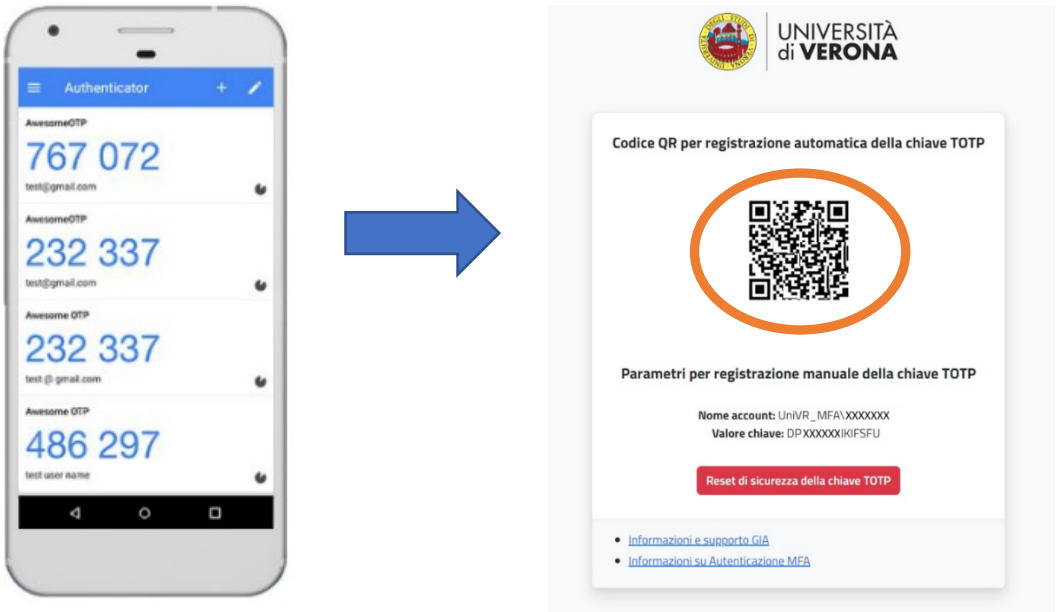
1. generare un **codice QR** per la registrazione automatica della chiave TOTP

   E' possibile farlo tramite:
   - ✓ email privata

   Oppure
   - ✓ SPID/CIE

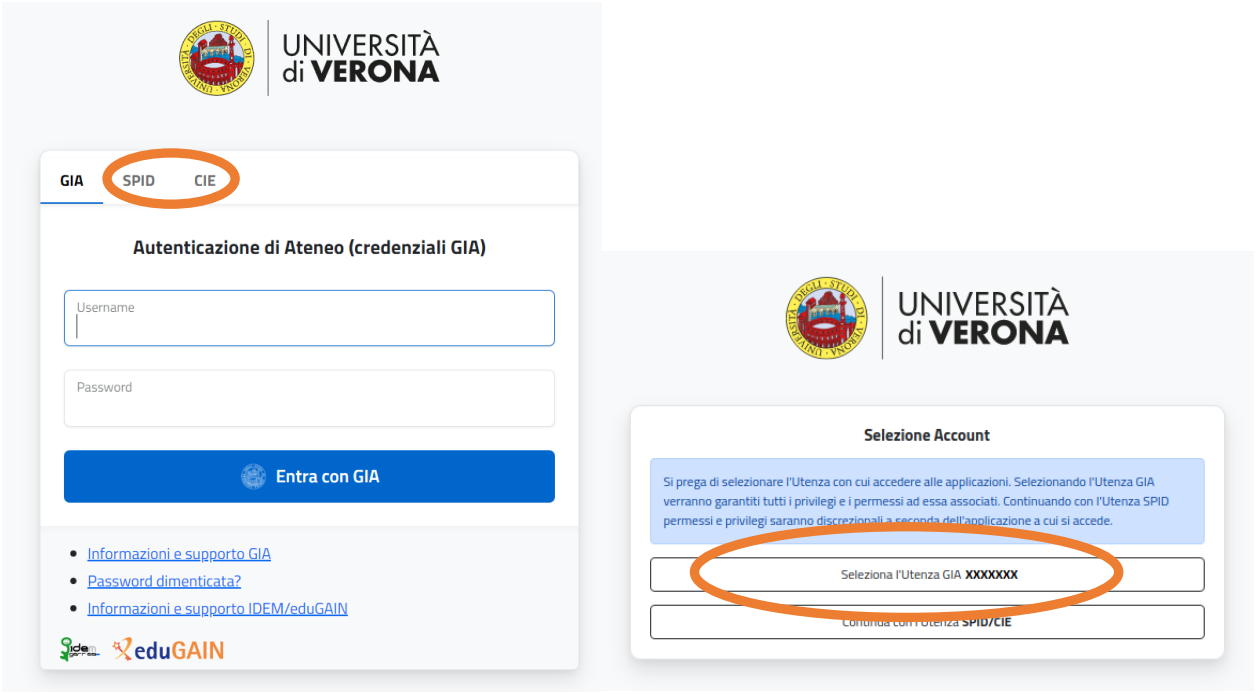


2. **configurare** associando a questo codice l'Applicazione Mobile o Applicativi Desktop scelta:



Vedere il relativo paragrafo in questa guida per configurarla.

Nota:
In alternativa all'MFA per l'accesso ad Office 365 rimane sempre attiva l'autenticazione tramite SPID o CIE:



Generare il codice QR

Requisito

Verificare che l'orario del dispositivo su cui si installa l'App Mobile per l'autenticazione MFA sia corretto per garantire il funzionamento dei codici di sicurezza TOTP.

Procedimento

Generare il codice QR per poter registrare l'App Mobile o App Desktop per l'autenticazione MFA e ricevere i codici di verifica TOTP.

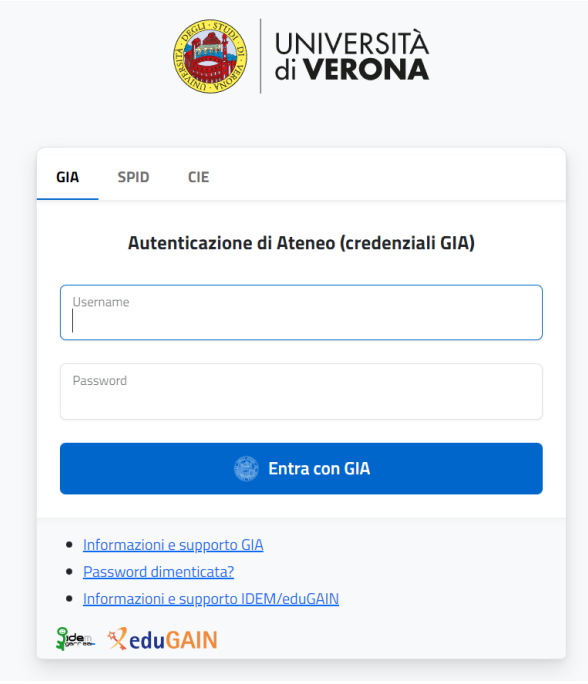
1° Metodo: utilizzare la mail privata

Requisito

Questa procedura richiede che ci sia un indirizzo email privata in ESSE3 carriere studenti (per gli studenti) o in DBERW (per il personale TA/docenti) valida ed accedibile dall'utente al momento della registrazione.

1. Accedere alla pagina web:
   https://aap.univr.it/UNIVRMfaQr/qr

2. Autenticarsi con Login/password GIA:

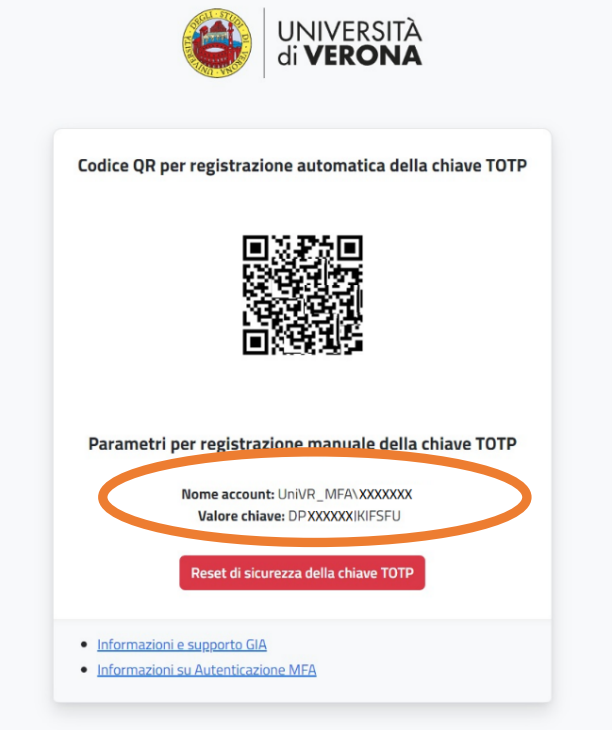


3. Inserire il codice OTP inviato all'email privata con messaggio dal contenuto simile al seguente:

   Subject: One Time Pin
   Please use 313242 as a One Time Pin to access the requested resource.

   Premere "Login"

4. Viene generato il codice QR e i parametri per la registrazione manuale utili per configurare l'App Mobile o l'App Desktop di autenticazione MFA:



Note

E’ possibile da questa schermata eseguire il **reset della chiave segreta** attraverso il pulsante “Reset di sicurezza della chiave TOTP”. Il reset della chiave TOTP determina la necessità di procedere a una nuova registrazione delle App Mobile o App Desktop di autenticazione MFA in uso (ripetere dall’inizio i passaggi).

In alcuni casi particolari può non essere possibile scansionare il QRCode. L’App Mobile o App Desktop di autenticazione scelta per l’MFA dovrebbe permettere di inserire manualmente il “Nome account: UNIVR\XXXXX” e la chiave segreta “Valore chiave: XXXXXXXXXX”. Fare riferimento alle guide specifiche dell’App Mobile o App Desktop di autenticazione scelta per l’MFA per le istruzioni per l’inserimento manuale della chiave segreta.

Esistono molte Applicativi Mobile (Microsoft Authenticator, Google Authenticator, 2FA, …) o Applicativi Desktop in grado di supportare lo standard (es. KeepassXC) che permettono la generazione di codici di sicurezza per l’MFA.

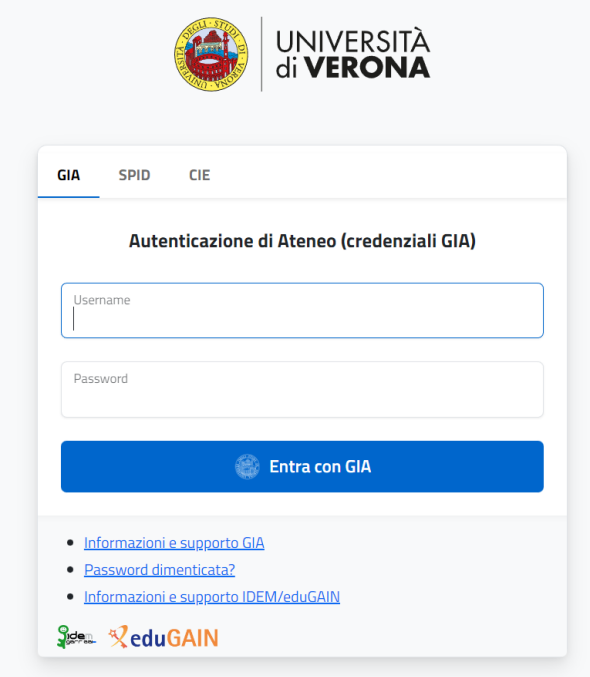
Vi illustriamo come procedere con le App Mobile:

- Google Authenticator
- Microsoft Authenticator

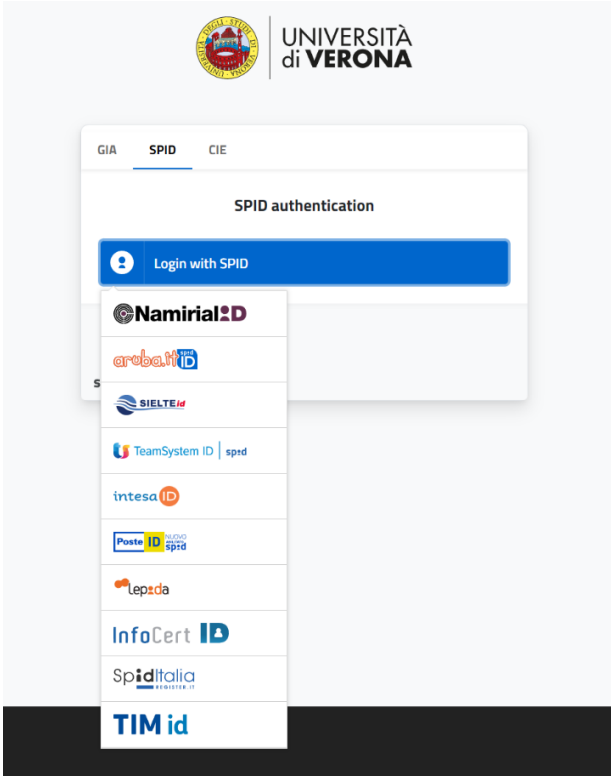
2° Metodo: utilizzare SPID

1. Accedere alla pagina web:
   https://aap.univr.it/UNIVRMfaQr/qr

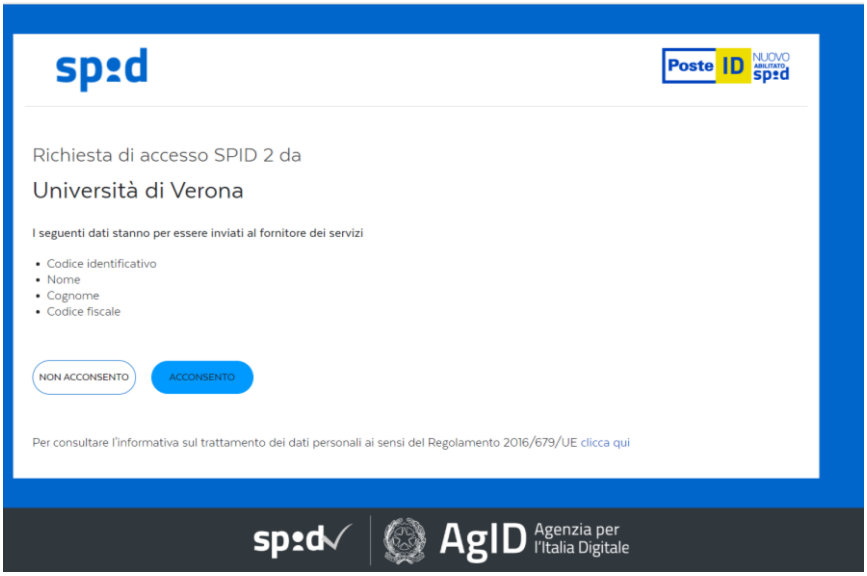
2. Autenticarsi con SPID:



3. Scegliere l'Identity Provider del tuo SPID:



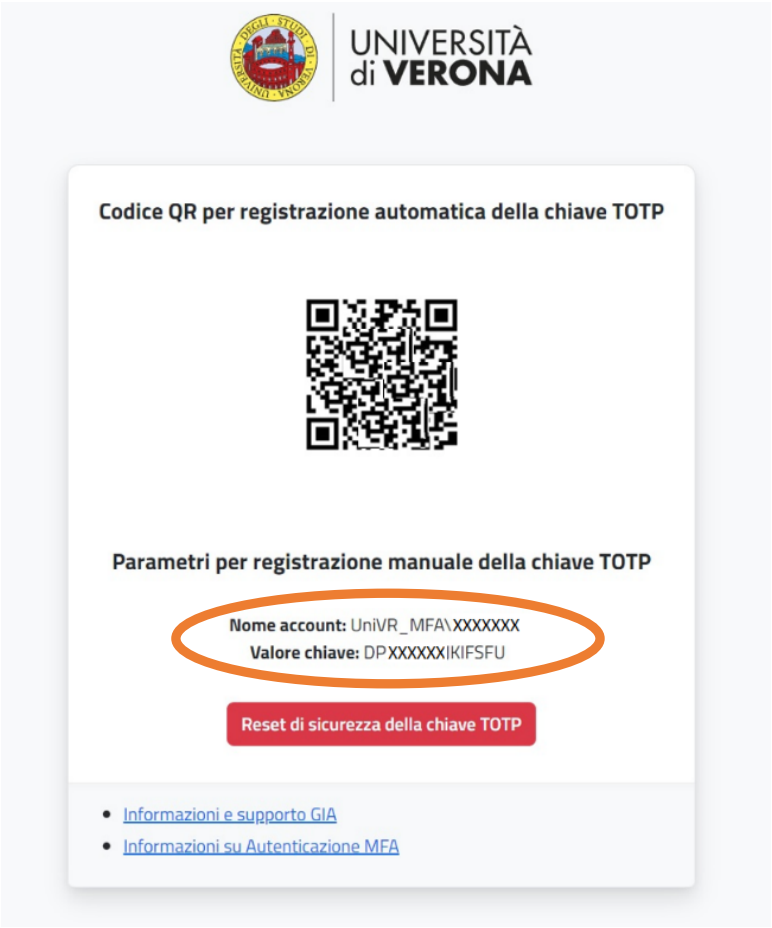
4. Scansionare il codice QR e procedere con l'autorizzazione su APP Poste ID:



Premere "Acconsento"

5. Scegliere la prima opzione “Selezionare l’Utenza GIA XXXXX”

6. Viene generato il codice QR e i parametri per la registrazione manuale utili per configurare l’App Mobile o l’App Desktop di autenticazione MFA:



Note

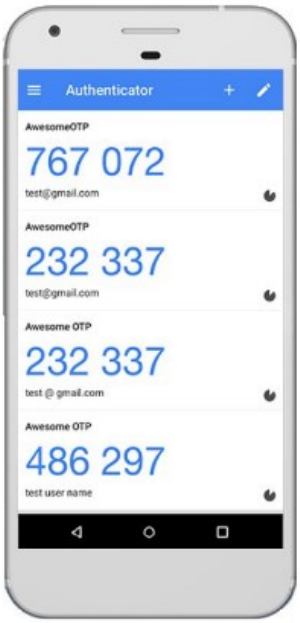
E’ possibile da questa schermata eseguire il **reset della chiave segreta** attraverso il pulsante “Reset di sicurezza della chiave TOTP”. Il reset della chiave TOTP determina la necessità di procedere a una nuova registrazione delle App Mobile o App Desktop di autenticazione MFA in uso (ripetere dall’inizio i passaggi).

In alcuni casi particolari può non essere possibile scansionare il QRCode. L’App Mobile o App Desktop di autenticazione scelta per l’MFA dovrebbe permettere di inserire manualmente il “Nome account: UNIVR\XXXXX” e la chiave segreta “Valore chiave: XXXXXXXXXX”. Fare riferimento alle guide specifiche dell’App Mobile o App Desktop di autenticazione scelta per l’MFA per le istruzioni per l’inserimento manuale della chiave segreta.

Esistono molte Applicativi Mobile (Microsoft Authenticator, Google Authenticator, 2FA, …) o Applicativi Desktop in grado di supportare lo standard (es. KeepassXC) che permettono la generazione di codici di sicurezza per l’MFA.

Vi illustriamo come procedere con le App Mobile:

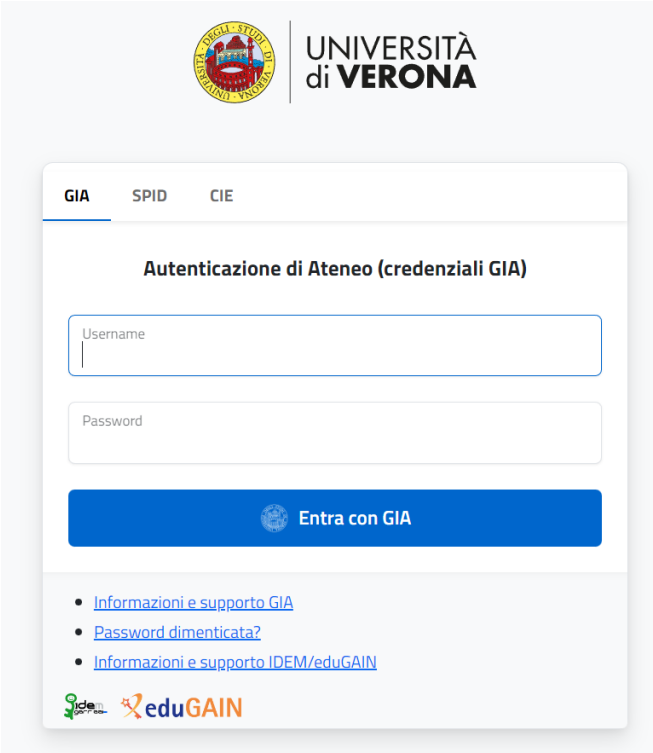
- Google Authenticator
- Microsoft Authenticator



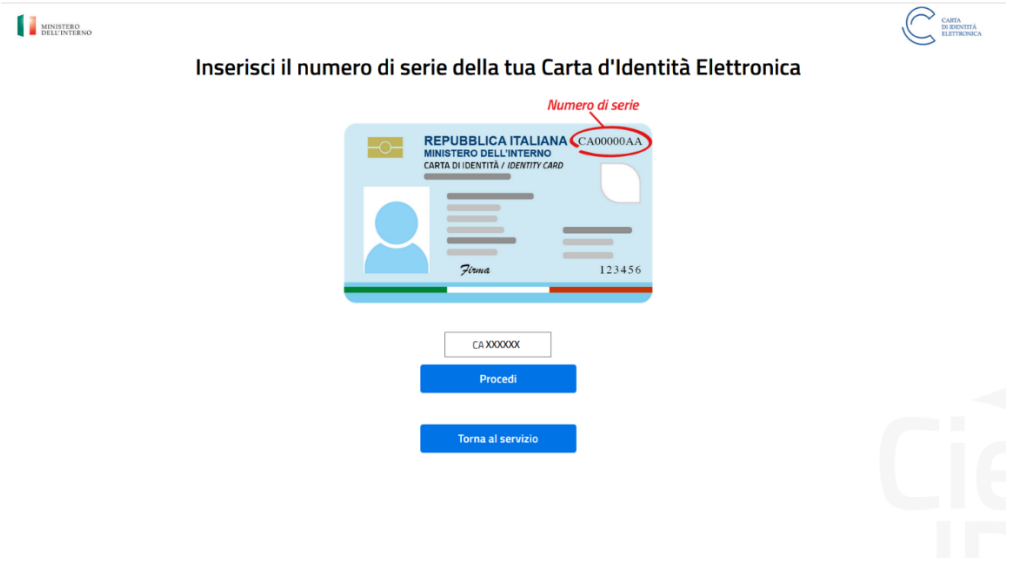
3° Metodo: utilizzare CIE

1. Accedere alla pagina web: https://aap.univr.it/UNIVRMfaQr/qr

2. Autenticarsi con CIE:



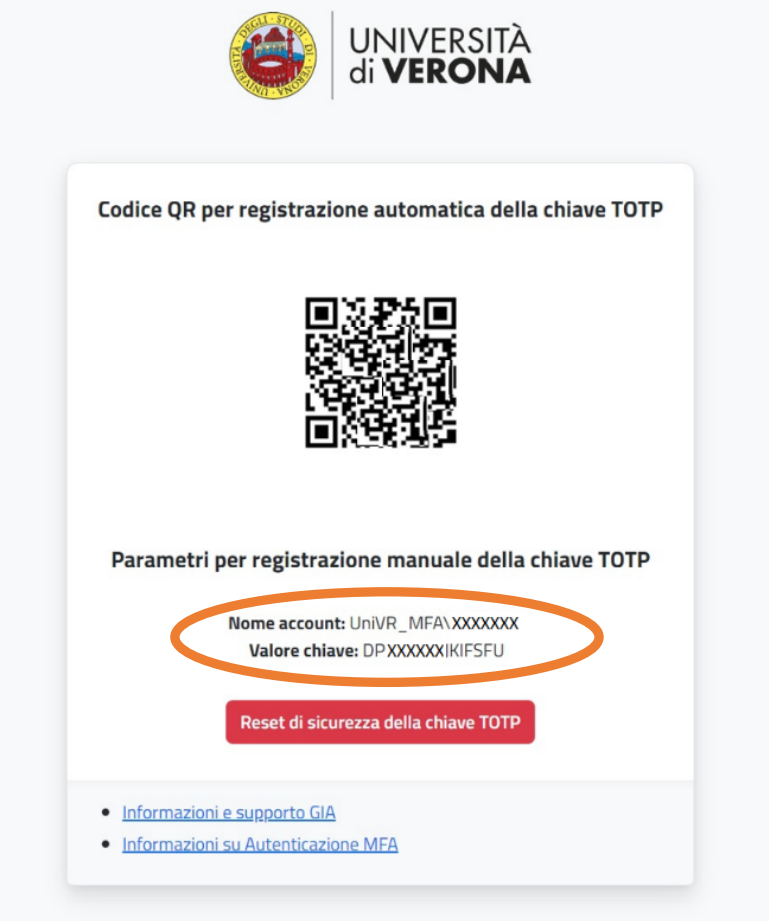
3. Inserire il numero di serie della CIE:



4. Scansionare il QR code con l'app CIE ed inserire il codice OTP ricevuto

5. Scegliere la prima opzione "Selezionare l'Utenza GIA XXXXX"

6. Viene generato il codice QR e i parametri per la registrazione manuale utili per configurare l'App Mobile o l'App Desktop di autenticazione MFA:



Note

E' possibile da questa schermata eseguire il **reset della chiave segreta** attraverso il pulsante "Reset di sicurezza della chiave TOTP". Il reset della chiave TOTP determina la necessità di procedere a una nuova registrazione delle App Mobile o App Desktop di autenticazione MFA in uso (ripetere dall'inizio i passaggi).

In alcuni casi particolari può non essere possibile scansionare il QRCode. L'App Mobile o App Desktop di autenticazione scelta per l'MFA dovrebbe permettere di inserire manualmente il "Nome account: UNIVR\XXXXX" e la chiave segreta "Valore chiave: XXXXXXXXXX". Fare riferimento alle guide specifiche dell'App Mobile o App Desktop di autenticazione scelta per l'MFA per le istruzioni per l'inserimento manuale della chiave segreta.

Esistono molte Applicativi Mobile (Microsoft Authenticator, Google Authenticator, 2FA, …) o Applicativi Desktop in grado di supportare lo standard (es. KeepassXC) che permettono la generazione di codici di sicurezza per l'MFA.

Vi illustriamo come procedere con le App Mobile:

- Google Authenticator
- Microsoft Authenticator

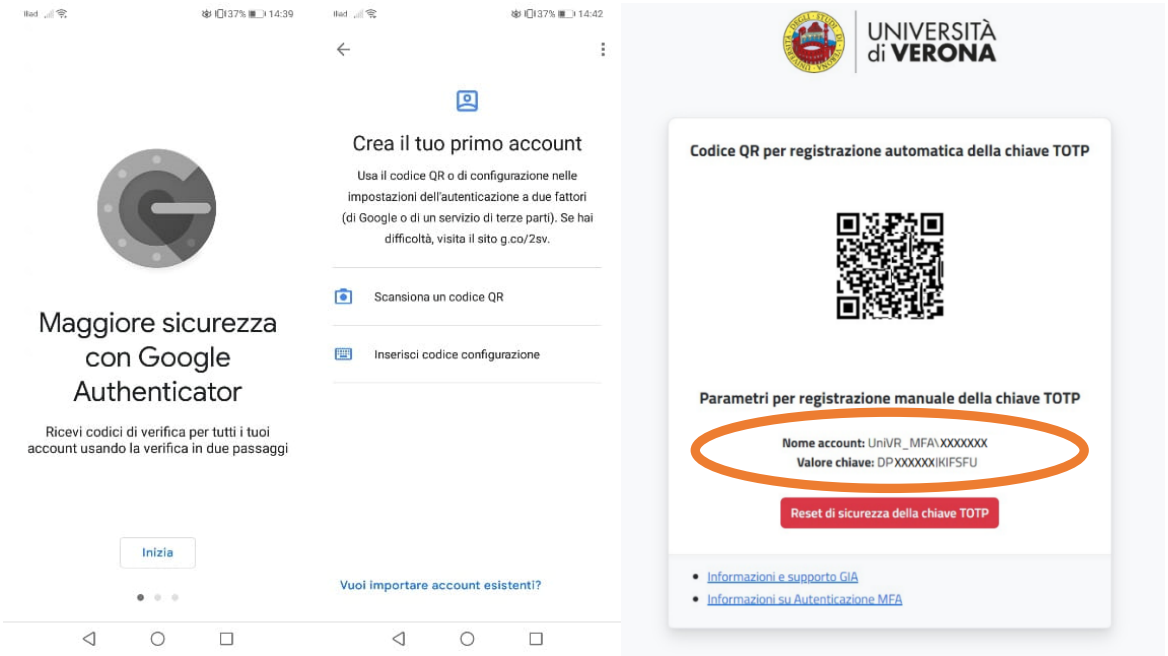
Configurare e ricevere i codici di verifica con Google Authenticator

Requisiti dell'app

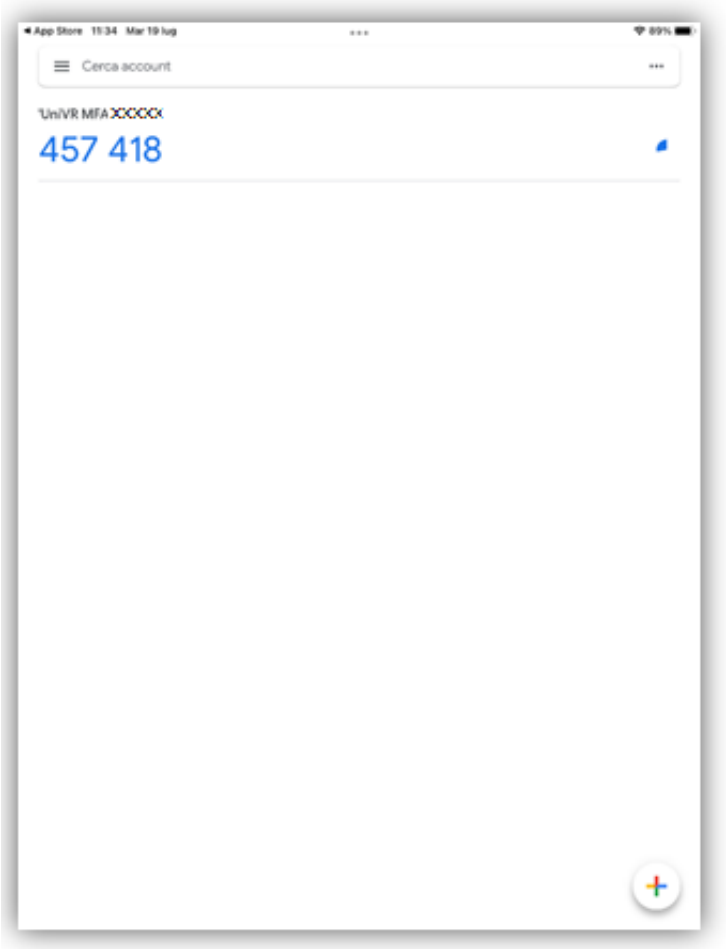
Per utilizzare Google Authenticator sul tuo dispositivo Android, occorre disporre di Android 4.4 o versioni successive.

Procedimento

Dopo aver generato il codice QR (vedere il relativo paragrafo):



1. Scaricare e installare l’app dal Play Store.
2. Creare un nuovo l’account e premere “Inizia”
3. Premere “Scansiona il codice QR”
   e usare la fotocamera del dispositivo per analizzare il codice
4. Compare un nuovo account “UniVR_MFA\XXXXXX”
5. Premere su “Aggiungi account”



NB

Se si è già installata l'app:

1. Nell'app authenticator selezionare il pulsante “+” (in basso a destra) quindi “Aggiungi account”
2. Premere “Scansiona il codice QR”
3. Compare un nuovo account “UniVR_MFA\XXXXXX”
4. Premere su “Aggiungi account”

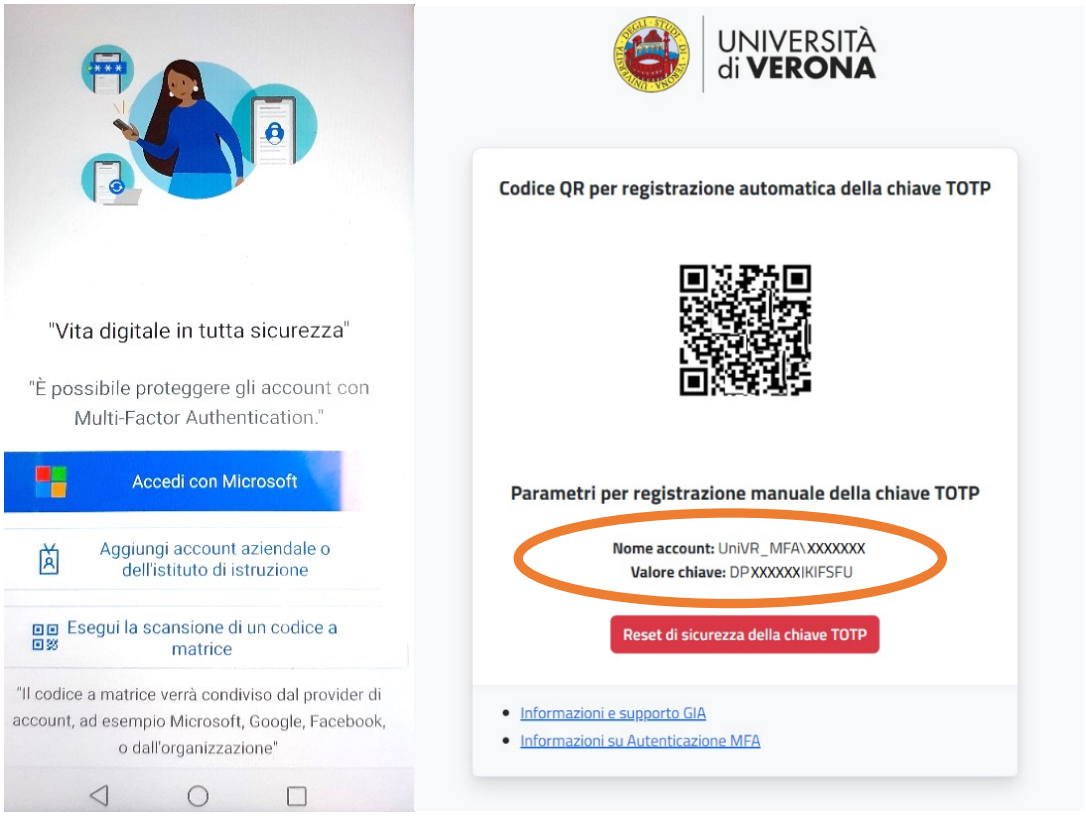
Configurare e ricevere i codici di verifica con Microsoft Authenticator

Requisiti dell'app

Per utilizzare Microsoft Authenticator sul tuo dispositivo Android, occorre disporre di Android 4.4 o versioni successive.

Procedimento

Dopo aver generato il codice QR (vedere il relativo paragrafo):



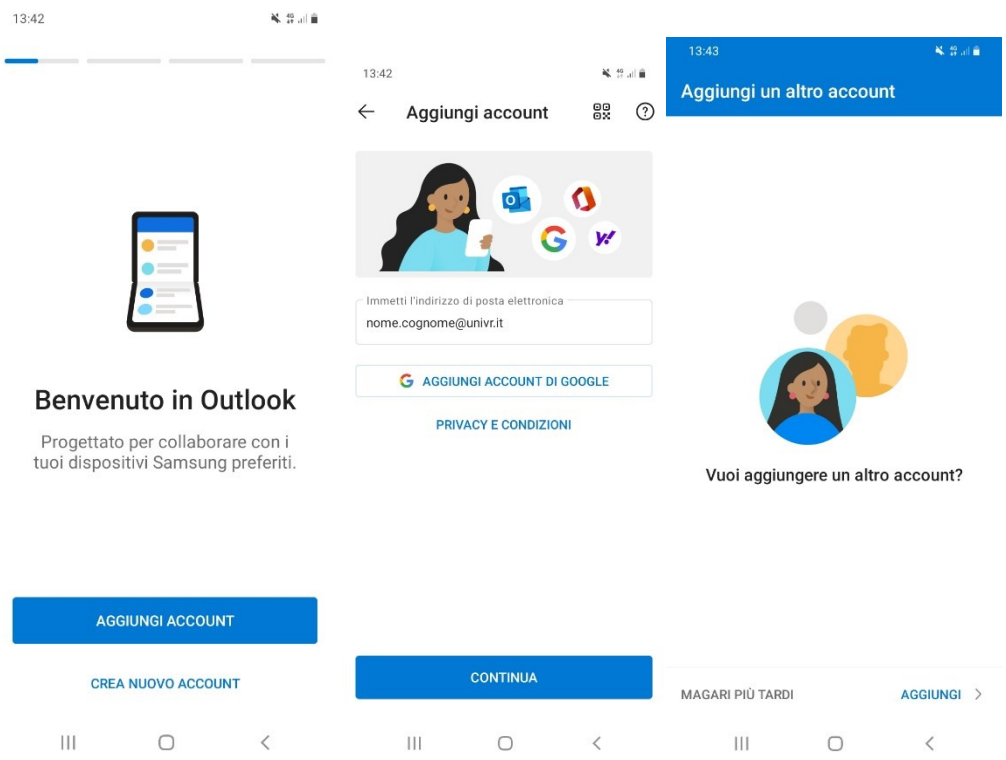
1. Scaricare e installare l'app dal Play Store .
2. Nell'app aggiungere un account e scegliere "Aggiungi account aziendale o dell'istituto di istruzione"
3. Premere "Esegui la scansione di un codice a matrice" e usare la fotocamera del dispositivo per analizzare il codice
4. Compare un nuovo account "UniVR_MFA\XXXXXX

NB

Se si è già installata l'app:

1. Nell'app authenticator selezionare [tre puntini] quindi + Aggiungi account
2. Scegliere "Aggiungi account aziendale o dell'istituto di istruzione"
3. Premere "Esegui la scansione di un codice a matrice" e usare la fotocamera del dispositivo per analizzare il codice
4. Compare un nuovo account "UniVR_MFA\XXXXXX"

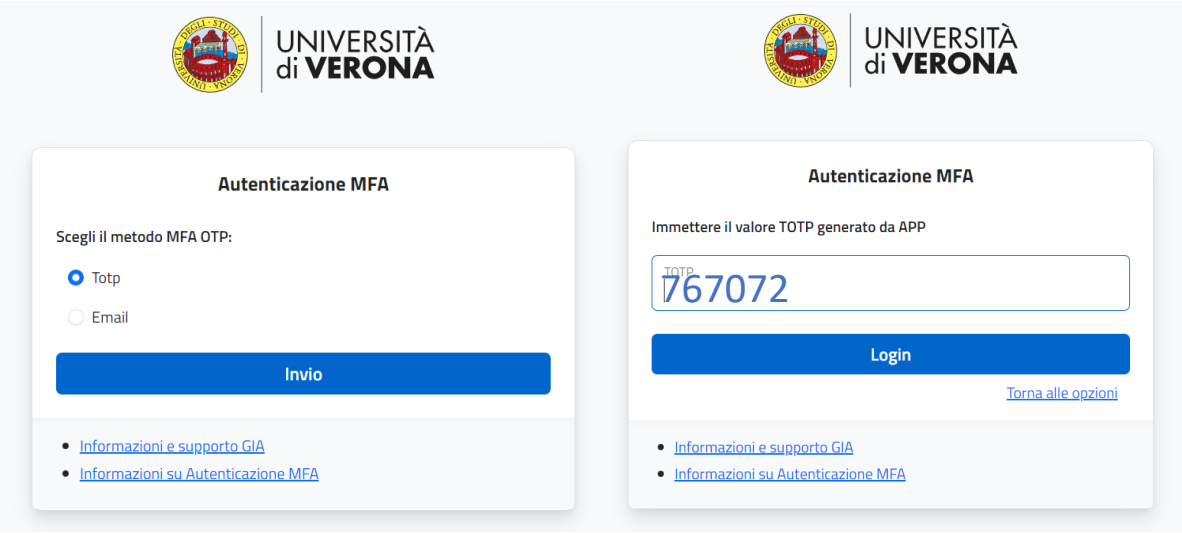
Configurare Outlook



Procedimento

1. Scaricare e installare l'app dal Play Store .
2. Scegliere "Aggiungi account"
3. Inserire la mail e premere "Continua"

Inserire le credenziali GIA e scegliere il metodo OTP preferito



Inserire il codice di sicurezza OTP ricevuto.

Errore di configurazione MFA

Se compare il seguente *errore*:

Significa che:

Non è stata fornita una *email privata* all'università e quindi non è presente in ESSE3 carriere studenti (per gli studenti) o a DBERW (per il personale TA/docenti)

- ✓ ESSE3 – Studenti
- ✓ Dberw - Personale

e *non è stata registrata nessuna applicazione* per l'autenticazione MFA via TOTP

Per risolvere:

- inserire un indirizzo email privata in ESSE3 carriere studenti (per gli studenti) o in DBERW (per il personale TA/docenti) ed autenticarsi con Login/password GIA e scegliere il metodo invio "Email" inserendo il codice OTP ricevuto. Vedi il paragrafo "Accesso da portale web – Metodo Email" nei manuali Windows o MAC

Oppure

- vedere il paragrafo "Generare il codice QR" nei manuali Android, Iphone o Ipad