



Ministero della Giustizia

Dipartimento per l'innovazione tecnologica della giustizia

Direzione generale per i sistemi informativi automatizzati

Vademecum

Multi Factor Authentication

(MFA)

Ver.	Elabora	Verifica	Data emissione	Descrizione delle modifiche
1.0	Min.Giustizia	Min.Giustizia	22/08/2022	Creazione documento
1.1	Min.Giustizia	Microsoft	16/01/2024	Revisione
1.2	Min.Giustizia	Min.Giustizia	06/05/2024	Integrazione screenshot di configurazione app
1.3	Min.Giustizia	Min.Giustizia	27/01/2025	Integrazione problemi ricorrenti
1.4	Min.Giustizia	Min.Giustizia	07/03/2025	Integrazione sommario
1.5	Min.Giustizia	Min.Giustizia	07/05/2025	Integrazione uso del codice per password monouso



Sommario

Introduzione.....	2
Scopo.....	2
Istruzioni.....	3
Problemi ricorrenti	11
1) Istruzioni da seguire per la sostituzione del dispositivo mobile.....	11
2) Codice a matrice già utilizzato	11
3) Come utilizzare il “Codice per Password Monouso” in assenza di rete (mobile e/o internet) per superare il secondo fattore di verifica	15



Introduzione

Configurando la MFA si aggiunge un ulteriore livello di sicurezza al proprio account Giustizia.

Con l'introduzione del secondo fattore di autenticazione non sarà sufficiente l'inserimento della password (primo fattore): occorrerà anche approvare una notifica inviata dall'applicazione Microsoft Authenticator preinstallata sul proprio telefono cellulare oppure occorrerà inserire un codice di verifica inviato al proprio numero di telefono cellulare via sms.

Tra le applicazioni che richiederanno il secondo fattore di autenticazione, quando si accede al di fuori della rete RUG (rete interna della Giustizia) figurano ad esempio Outlook, Teams e OneDrive.

Scopo

La complessità crescente degli attacchi da parte degli hacker e la palese inefficacia della sola password a protezione del proprio account rendono infatti doveroso un approccio più sofisticato.

La "Multi Factor Authentication" (autenticazione a più fattori) è quella tecnologia che permette di riconoscere, attraverso più metodi di autenticazione, la persona che effettua l'accesso (logon) a un sistema o a un'applicazione.

L'app 'Microsoft Authenticator', installata e configurata sul proprio telefono cellulare, consente di eseguire l'accesso al proprio account in modo sicuro in quanto permette di soddisfare in maniera semplice ed intuitiva l'autenticazione a doppio fattore.



Istruzioni

Per la configurazione della Multi Factor Authenticator (MFA) è necessario, lato utente, disporre contemporaneamente di un computer e di un telefono cellulare; andranno eseguite le azioni descritte nei seguenti punti:

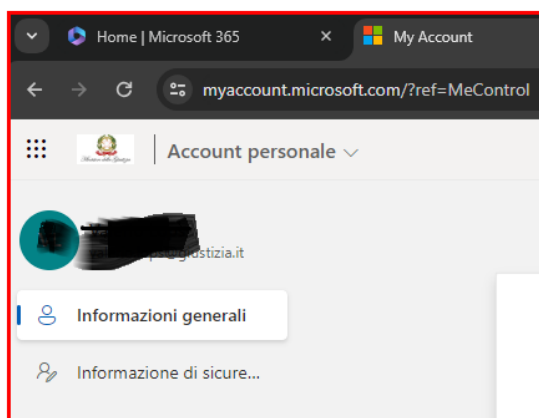
1. Scaricare dallo store del telefono **cellulare** [l'App Microsoft Authenticator](#) e installarla.
2. Collegarsi tramite browser del **pc** al seguente sito internet <https://portal.office.com>; quindi, se richiesto, inserire le proprie credenziali (indirizzo mail e relativa password di dominio) e scegliere **AVANTI**, come si vede nelle figure seguenti.

3. È possibile che all'utente compaia a video un messaggio così come mostrato nella figura seguente, in cui gli viene chiesto di scegliere se procedere immediatamente con la configurazione del secondo fattore di autenticazione oppure di rimandare la configurazione fino a un massimo di 14 giorni. Qualora la configurazione non dovesse venir effettuata entro la tempistica indicata, l'utente potrà ugualmente effettuarla successivamente, ma fino a quel momento non potrà avere accesso alle applicazioni da fuori RUG. Per proseguire con la configurazione del secondo fattore di autenticazione, scegliere **AVANTI**.



Se all'utente non compare invece la finestra di cui alla figura precedente, occorre cliccare sul seguente link: <https://mysignins.microsoft.com/security-info>

Una volta aperta la pagina del link di cui sopra, occorre cliccare su 'Informazione di sicurezza':





Aggiungere metodo di accesso:

Informazione di sicurezza

Questi sono i metodi usati per accedere all'account o reimpostare la password.

You're using the most advisable sign-in method where it applies.
Sign-in method when most advisable is unavailable: Microsoft Authenticator - [Notifica Cambia](#)

[+ Aggiungere metodo di accesso](#)

App Authenticator:

Aggiungi un metodo ×

Specificare il metodo da aggiungere.

Scegliere un metodo ▼

App Authenticator

4. Per la configurazione dell'App precedentemente scaricata sul telefono cellulare scegliere AVANTI come evidenziato nelle due figure successive:

Proteggi l'account

L'organizzazione richiede la configurazione dei metodi seguenti per la dimostrazione dell'identità dell'utente.

Microsoft Authenticator

 **Ottenere prima di tutto l'app**

Nel telefono installare l'app Microsoft Authenticator. [Scarica ora](#)

Dopo l'installazione dell'app Microsoft Authenticator nel dispositivo, scegliere "Avanti".

[Voglio usare un'app di autenticazione diversa](#)

[Avanti](#)

[Si vuole configurare un metodo diverso](#)



Proteggi l'account

L'organizzazione richiede la configurazione dei metodi seguenti per la dimostrazione dell'identità dell'utente.

Microsoft Authenticator



Configura l'account

Se richiesto, consentire le notifiche. Aggiungere quindi un account e selezionare "Account aziendale o dell'istituto di istruzione".

Indietro

Avanti

[Si vuole configurare un metodo diverso](#)

5. Aprire l'App MFA dal telefono **cellulare**. Selezionare i tre puntini in alto a destra, selezionare **AGGIUNGI ACCOUNT** e scegliere **ACCOUNT AZIENDALE**. Eseguire la scansione del codice QR visualizzato sul computer e scegliere **AVANTI**.

Proteggi l'account

L'organizzazione richiede la configurazione dei metodi seguenti per la dimostrazione dell'identità dell'utente.

Microsoft Authenticator

Esegui la scansione del codice a matrice

Usare l'app Microsoft Authenticator per eseguire la scansione del codice a matrice. L'app Microsoft Authenticator verrà connessa all'account.

Dopo la scansione del codice a matrice, scegliere "Avanti".



Non è possibile digitalizzare l'immagine?

Indietro

Avanti

6. Sul telefono **cellulare** approvare la notifica inviata dall'app e scegliere **AVANTI**

Proteggi l'account

L'organizzazione richiede la configurazione dei metodi seguenti per la dimostrazione dell'identità dell'utente.

Microsoft Authenticator



Prova

Approvare la notifica che verrà inviata all'app.

[Indietro](#) [Avanti](#)

[Si vuole configurare un metodo diverso](#)

Proteggi l'account

L'organizzazione richiede la configurazione dei metodi seguenti per la dimostrazione dell'identità dell'utente.

Microsoft Authenticator



✔ La notifica è stata approvata

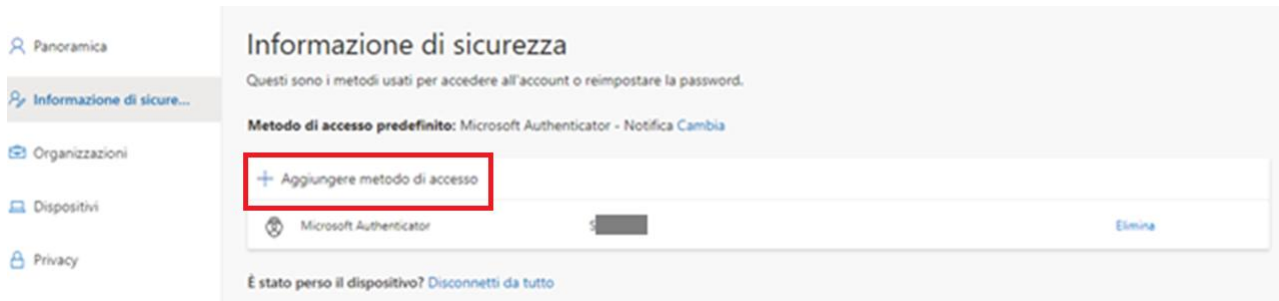
[Indietro](#) [Avanti](#)

[Si vuole configurare un metodo diverso](#)

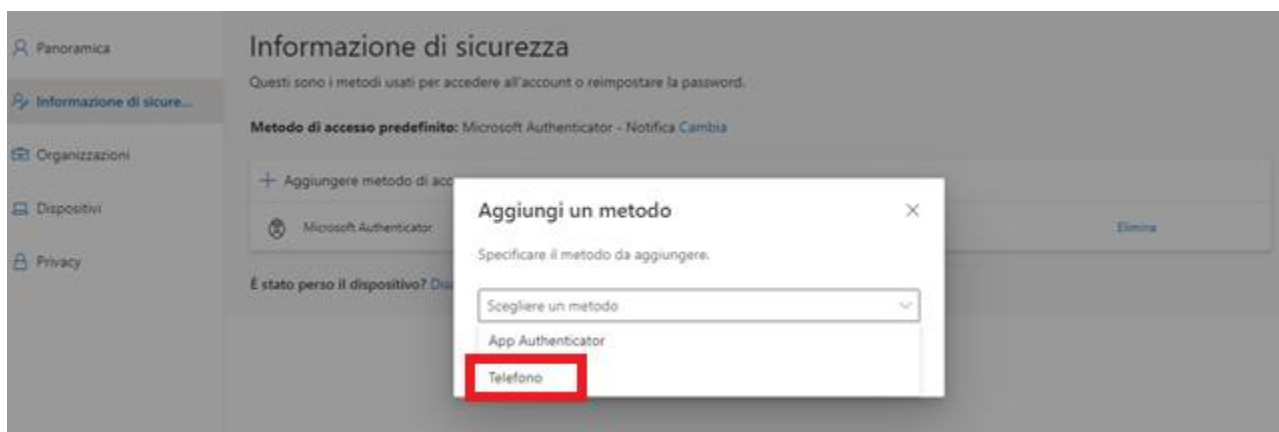
7. Scegliere **FINE** per concludere la configurazione

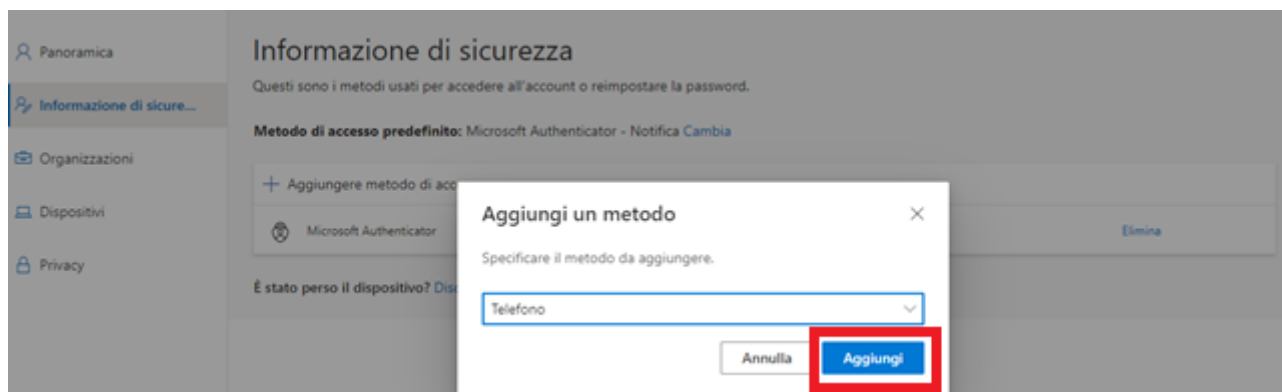


8. La configurazione dell'applicazione MFA è terminata. Si consiglia di aggiungere un ulteriore metodo di autenticazione ovvero la possibilità di ricevere un codice tramite SMS. Per avviare la configurazione, selezionare **+ aggiungere il metodo di accesso**

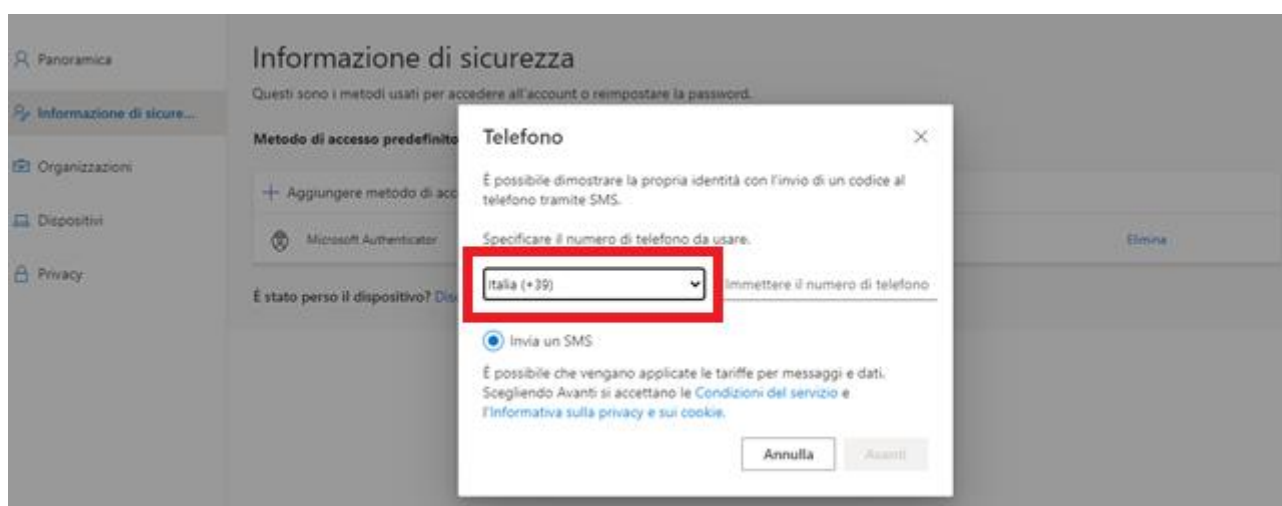


9. dall'elenco scegliere **TELEFONO** e selezionare **AGGIUNGI**

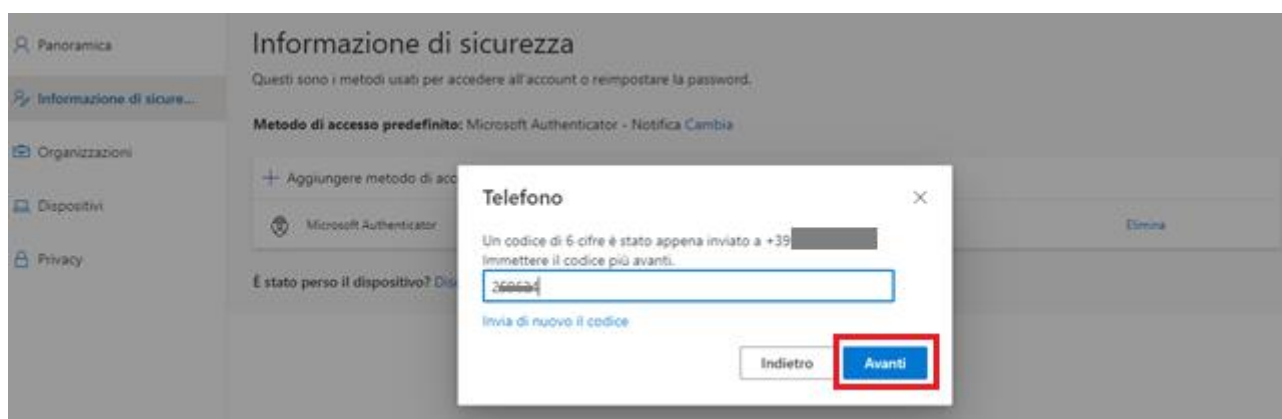


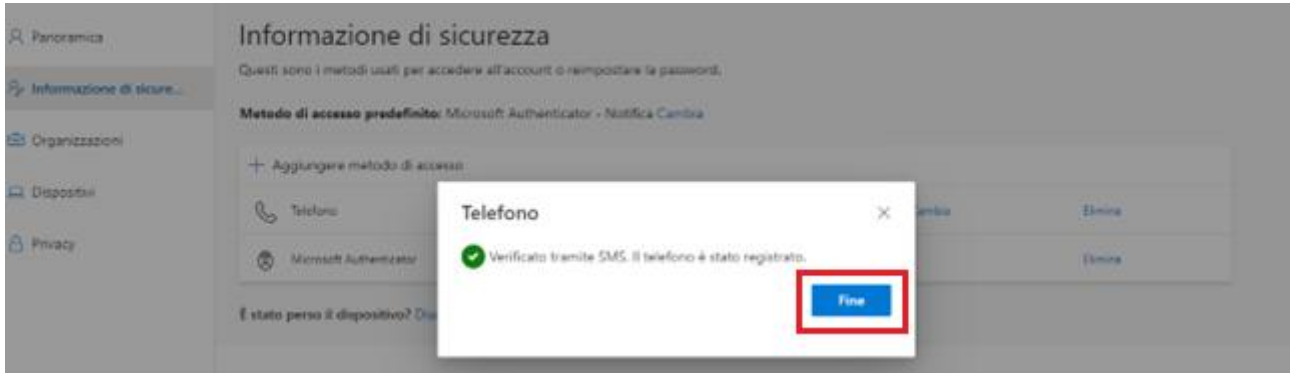


10. Scegliere ITALIA, inserire il proprio numero di telefono e scegliere **AVANTI**

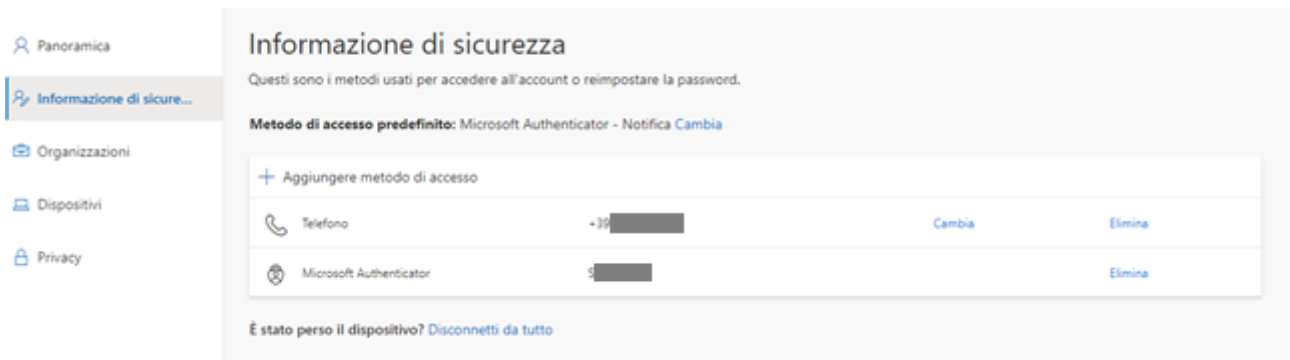


11. Immettere il codice inviato al telefono via sms e scegliere **AVANTI**. Dopo la verifica scegliere **FINE**





12. La configurazione è terminata e si possono verificare i dati immessi.





Problemi ricorrenti

1) Istruzioni da seguire per la sostituzione del dispositivo mobile

A seguito del cambio del dispositivo seguire la seguente procedura per riconfigurare l'app Authenticator sul nuovo. Dal browser andare su: <https://mysignins.microsoft.com/security-info> → + aggiungere metodo di accesso → App Authenticator → seguire l'iter di configurazione dell'app Authenticator già descritto.

Per aggiornare le informazioni di sicurezza verrà chiesto di superare la verifica MFA, utilizzando un metodo già impostato (ex OTP oppure approvazione della notifica su Authenticator del vecchio telefono).

Al termine della configurazione dell'app Authenticator sul nuovo dispositivo, se lo si ritiene opportuno, è possibile conservare o rimuovere l'app Authenticator associata al vecchio dispositivo, agendo dal browser sul tasto "elimina" allineato al vecchio dispositivo (nella medesima sezione informazioni di sicurezza).

2) Codice a matrice già utilizzato

In fase di configurazione dell'app Authenticator potrebbe verificarsi questo tipo di problema che impedisce l'associazione tra il proprio account *@giustizia e l'app Authenticator del cellulare.

In questo caso occorre prima di tutto provare a cancellare i dati dell'app Authenticator memorizzati nel proprio dispositivo.

A volte nonostante l'operazione di disinstallazione e successiva reinstallazione alcuni dati dell'app potrebbero rimanere memorizzati nel dispositivo.

Per tale motivo occorre eseguire la seguente procedura:

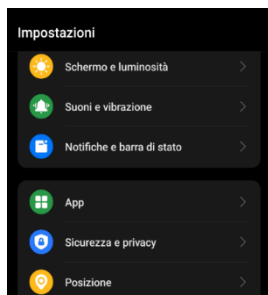
- 1) Aprire l'app Impostazioni
- 2) Recarsi in Applicazioni > Authenticator > Spazio di archiviazione > Cancellati dati
- 3) Chiudere tutte le app del telefono
- 4) Aprire nuovamente l'app Authenticator e cliccare su + > Account aziendale o dell'Istituto di Istruzione

quindi seguire i passi illustrati nel vademecum per le operazioni di configurazione dell'app Authenticator.

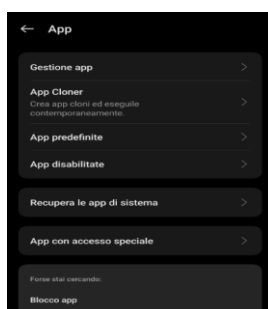
Di seguito gli screenshot presi sia da un dispositivo Android che iOS per illustrare l'iter necessario per rimuovere i dati dell'app memorizzati nel dispositivo.

Android

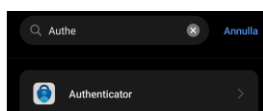
1) Andare nelle impostazioni del cellulare in app



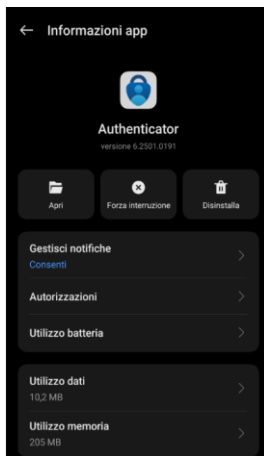
2) Cliccare su Gestione App



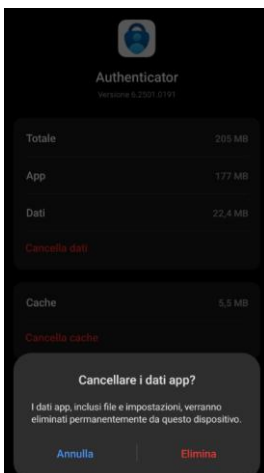
3) Nel menù di ricerca scrivere Authenticator



4) Entrare in Authenticator



5) Andare su Utilizzo memoria e quindi selezionare l'opzione cancella dati ed eliminare i dati

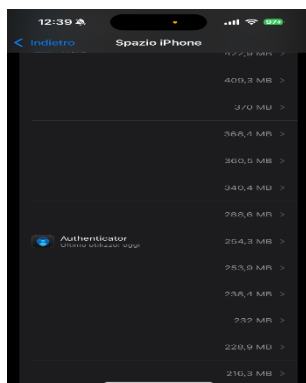


iOS

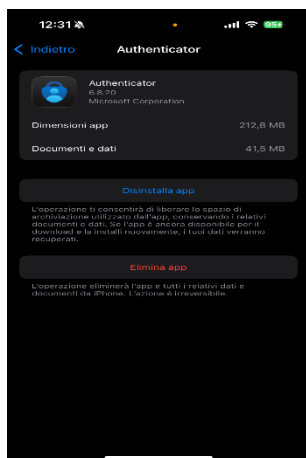
1) Andare in Impostazioni > Generali > Spazio su iPhone



2) Nella lista scorrere fino alla voce Authenticator



3) Cliccare su Elimina app e quindi confermare l'operazione



Qualora tale approccio non sia risolutivo, è necessario aprire un ticket all'assistenza, tramite portale <https://helpdesk.giustizia.it/>, alla quale riportare tramite screenshot l'errore segnalato.

L'assistenza provvederà a resettare il sistema MFA associato al vostro account Giustizia.

Successivamente occorre disinstallare e reinstallare l'app M.Authenticator e seguire nuovamente i passaggi appena illustrati.

Qualora nemmeno con l'intervento dell'assistenza si riuscisse a configurare correttamente l'app si invita ad attivare il sistema OTP via SMS come strumento per superare la verifica MFA.

Si ricorda che la modalità OTP è di pari efficacia all'app M.Authenticator per superare il secondo fattore di verifica previsto dalla policy MFA del Ministero.



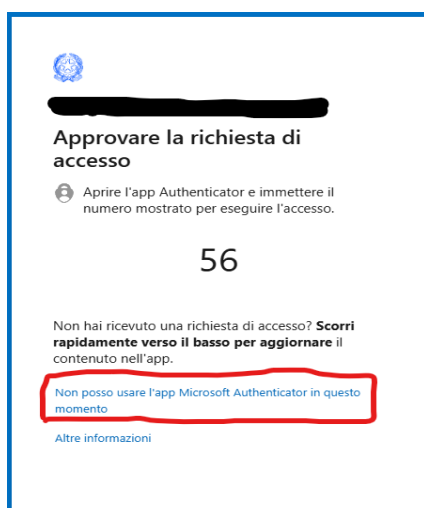
3) Come utilizzare il “Codice per Password Monouso” in assenza di rete (mobile e/o internet) per superare il secondo fattore di verifica

L'app Microsoft Authenticator, come altri generatori di codici TOTP (Time-based One-Time Password), genera codici offline, cioè senza aver bisogno di connessione Internet o rete mobile.

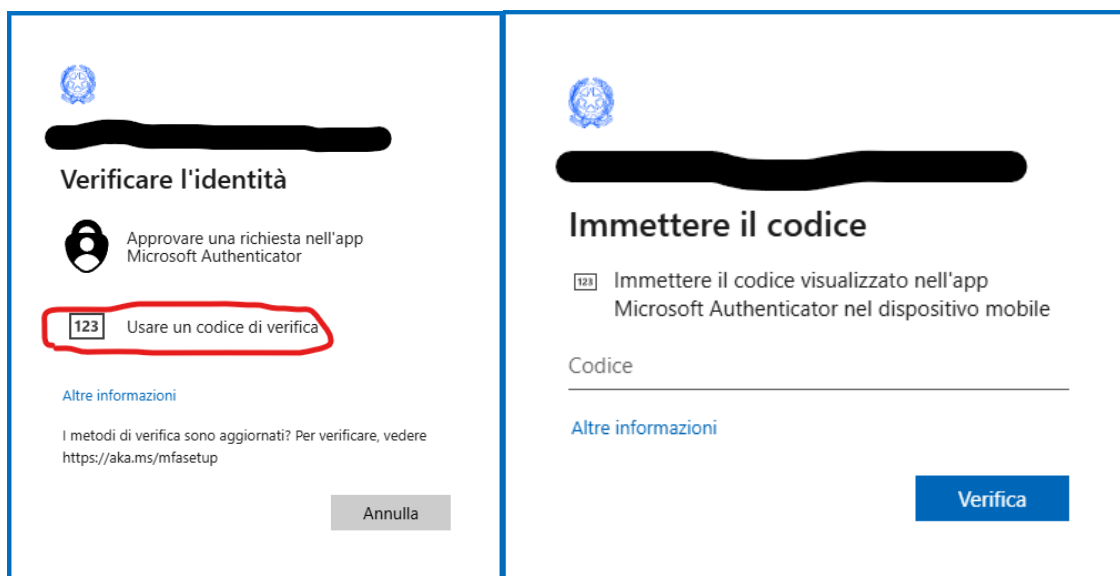
I codici si aggiornano ogni 30 secondi e possono essere usati per accedere a servizi che supportano l'autenticazione a due fattori (2FA) tramite codice.

Di seguito i passaggi necessari per utilizzare questa modalità, utile quando non è possibile approvare la normale notifica al cellulare che non può arrivare non essendoci connessione.

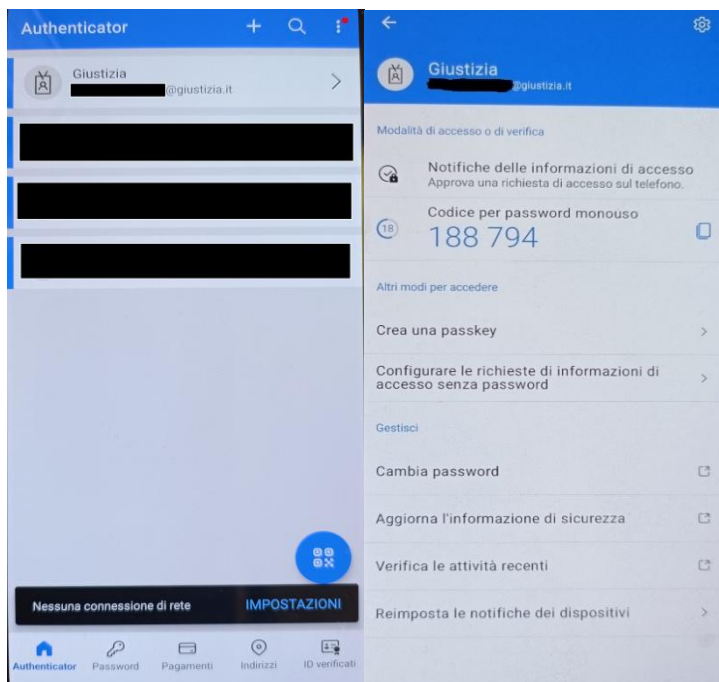
1) Cliccare sulla dicitura “Non posso usare l'app Microsoft Authenticator in questo momento”.



2) Si visualizzerà un elenco di metodi, registrati in precedenza, con i quali verificare l'identità; Cliccare poi su “usare un codice di verifica”.



3) Sul telefono entrare nell'app Microsoft Authenticator e cliccare sul profilo "Giustizia". Si visualizza un codice per password monouso da copiare nella schermata del PC



4) Inserire il codice password monouso nella schermata visualizzata sul computer; cliccare poi il tasto "Verifica".

