Südtiroler Informatik AG
the e-government company

MFA – Autenticazione fattori multipli

Manuale

1 Introduzione

Allo scopo di **migliorare la protezione della Sua identità e dei suoi dati** da accessi non autorizzati, viene introdotta la cosiddetta autenticazione multi-fattore nell'amministrazione della Provincia Autonoma di Bolzano (MFA).

Questa tecnologia si basa sulla verifica dell'accesso attraverso i seguenti fattori indipendenti tra loro:

- L'essere a conoscenza del nome utente e della password.
- L'essere in possesso dei seguenti componenti:
  - Telefono mobile (tramite SMS, telefonata, App)
  - Telefono fisso privato o aziendale (telefonata)
  - Indirizzo E-mail alternativo (E-Mail)

1.1 Ambito dove l'autenticazione multifattore è richiesta

La nuova modalità di autenticazione viene richiesta al personale dell'amministrazione provinciale, quando si vuole accedere da internet ai servizi come per esempio l'uso della Suite Office tramite http://www.office.com.

Per il normale accesso al PC in ufficio la MFA **non è necessaria.**

2 Il primo accesso tramite internet

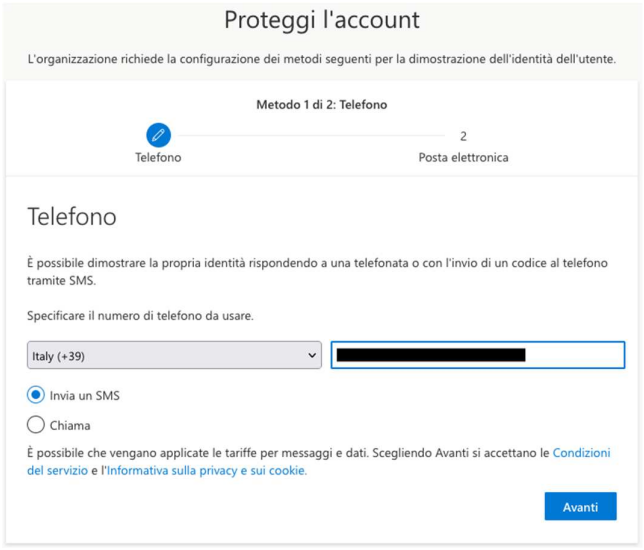
Una volta attivata la MFA, al primo accesso tramite internet appare all'utente la seguente schermata:

Dopo aver cliccato su "Avanti" Le verrà richiesto di configurare sia un numero di telefono che un indirizzo e-mail come secondo fattore per la verifica della sua identità.

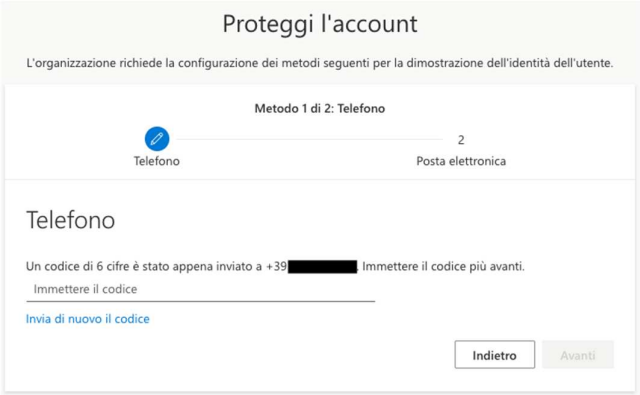
2.1 Parte 1: configurazione del telefono come secondo fattore di sicurezza

L'aggiunta di un numero di telefono è la prima parte obbligatoria di configurazione. La verifica di tale numero può avvenire con invio di un codice tramite SMS o tramite chiamata.

Inserimento del numero e scelta del metodo di comunicazione del codice di verifica:



Variante 1 - invio del codice tramite SMS:

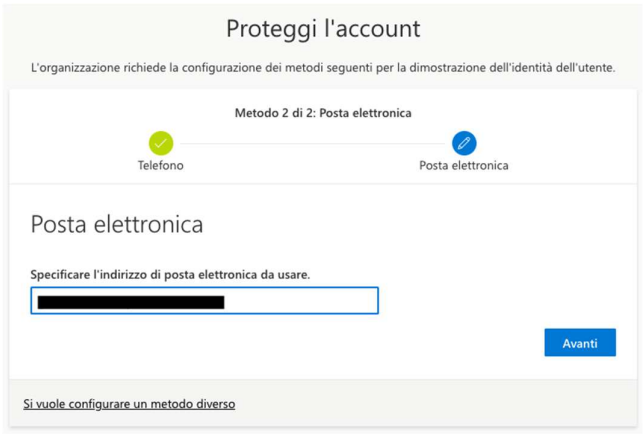


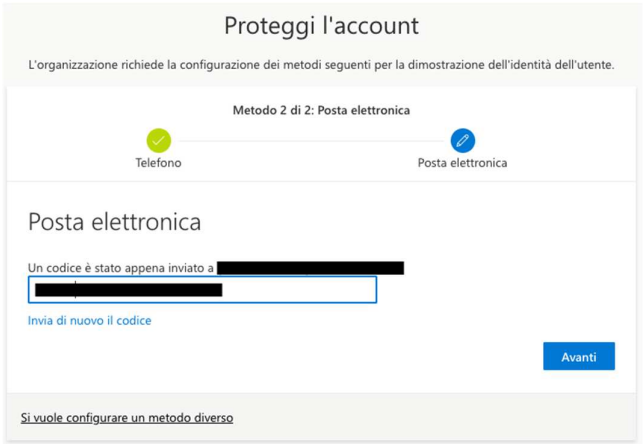
Variante 2 - invio del codice tramite chiamata:

Non appena inserito correttamente il codice ricevuto tramite SMS o confermata la chiamata scegliendo il tasto cancelletto (“#” sul telefono), si conclude la prima parte di configurazione:

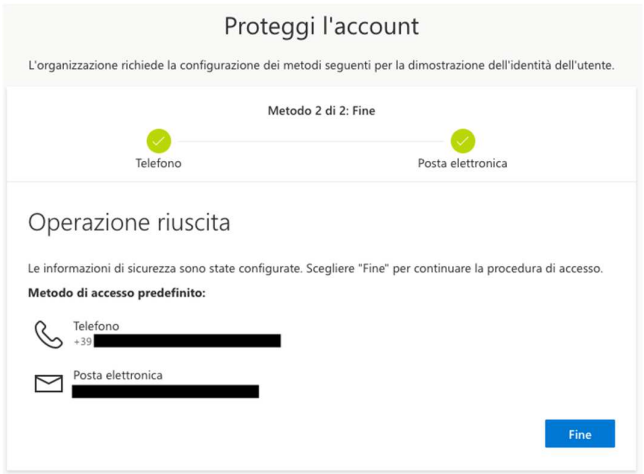
2.2 Parte 2: configurazione di un indirizzo e-mail come secondo fattore di sicurezza

Segue la seconda parte obbligatoria di configurazione tramite invio di un codice di verifica a un indirizzo e-mail personale aggiuntivo:



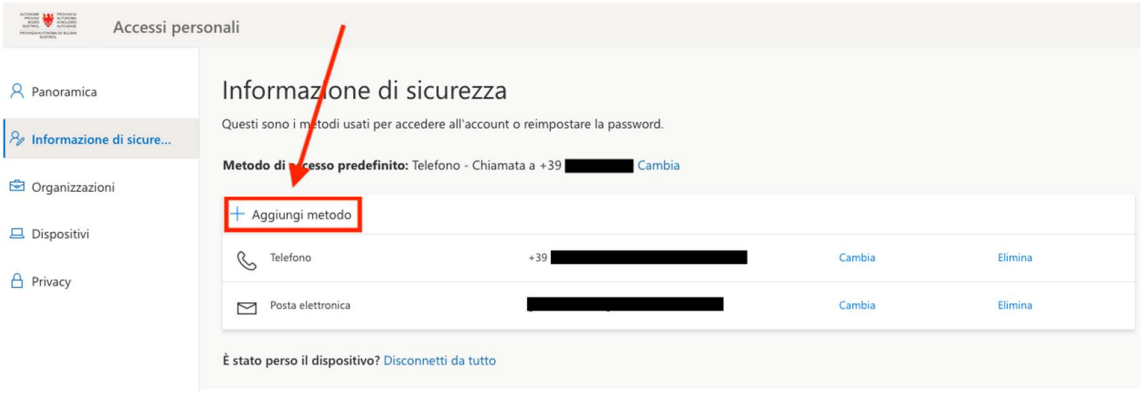


Non appena anche questo codice è stato inserito correttamente, si conclude la parte di configurazione obbligatoria:



2.3 Opzionale: configurazione dell'app mobile "Microsoft Authenticator"

Dopo aver concluso la configurazione obbligatoria, può essere abilitato l'utilizzo dell'app mobile sul sito https://mysignins.microsoft.com/security-info. Basterà scegliere il punto "Aggiungi metodo":

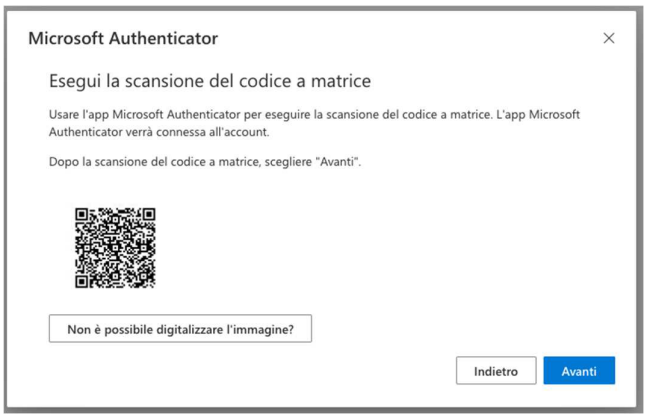


In seguito, scelga il metodo "App Authenticator" e clicchi su "Aggiungi":

Segue una richiesta con link relativo per scaricare e installare l'app apposita sul Suo cellulare. Appena eseguito questo passo, cliccare su "Avanti":

Seguire anche l'indicazione successiva e cliccare su "Avanti":

Le verrà mostrato un codice QR, il quale deve essere scannerizzato con l'app "Microsoft Authenticator" – **segua a questo punto le istruzioni relative all'impostazione dell'app mobile che trova nel capitolo successivo!** Solo una volta configurato cliccare su "Avanti":

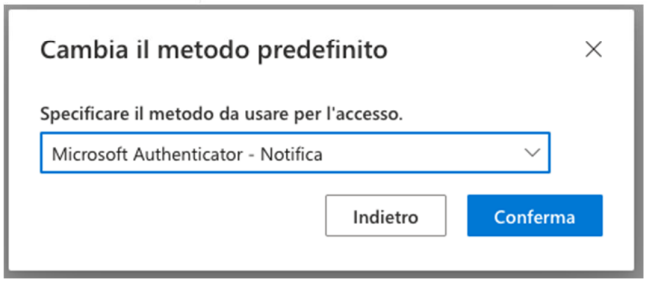


Se tutti i passi sono stati eseguiti correttamente, le verrà richiesto di eseguire un tentativo di autenticazione sull'app mobile (vedesi anche il capitolo "Accesso dopo la prima configurazione" di questo manuale):

Non appena eseguito quanto richiesto sull'app mobile del suo cellulare, le verrà visualizzato un messaggio di successo che può essere chiuso cliccando su "Avanti":

La pagina web ora torna a visualizzare l'elenco di configurazione relativo alle informazioni di sicurezza (https://mysignins.microsoft.com/security-info) e sul quale ora troverà anche elencato "Microsoft Authenticator".

Un consiglio pratico: per poter usare l'App mobile è necessario scaricare e installare il Microsoft Authenticator, ma avendo una connessione internet attiva sul cellulare, questo è il metodo più pratico e rapido per autorizzare gli accessi e per questo anche adatto alla configurazione come **metodo di accesso predefinito**!

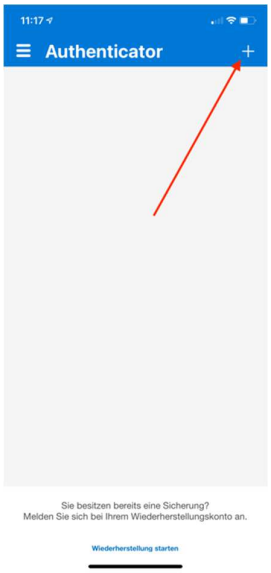


2.3.1 Configurazione dell'app Authenticator sul cellulare

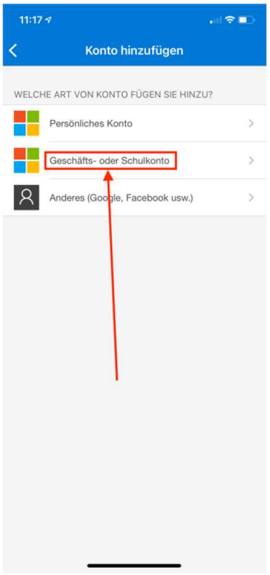
Le istruzioni riportate fin qui contengono anche riferimenti all'App "Microsoft Authenticator", che può essere scaricata su telefono mobile e configurata in pochi passaggi.

- Per iPhone: https://go.microsoft.com/fwlink/?linkid=869517
- Per Android: https://go.microsoft.com/fwlink/?linkid=869516
- für Windows Phone: https://go.microsoft.com/fwlink/?linkid=823234
- Per Huawei Gallery (tramite Petal Search): https://www.petalsearch.com/search?query=microsoft+authenticator&channel=app&from=CC000400&sregion=it&locale=it-it

1) Cliccare sul simbolo +



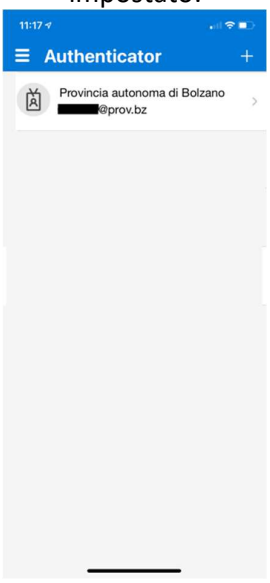
2) Cliccare su account aziendale o dell'istituto d'istruzione



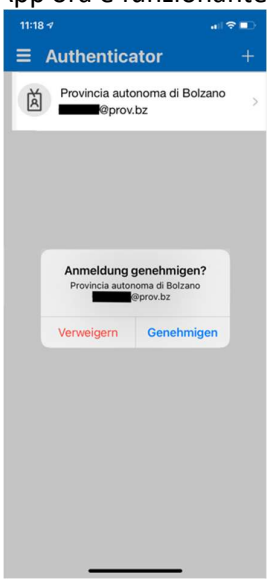
3) scegliere scan codice QR:

4) Scannerizzare il codice con la fotocamera:

5) l'account è ora impostato:



6) l'autenticazione tramite App ora è funzionante:

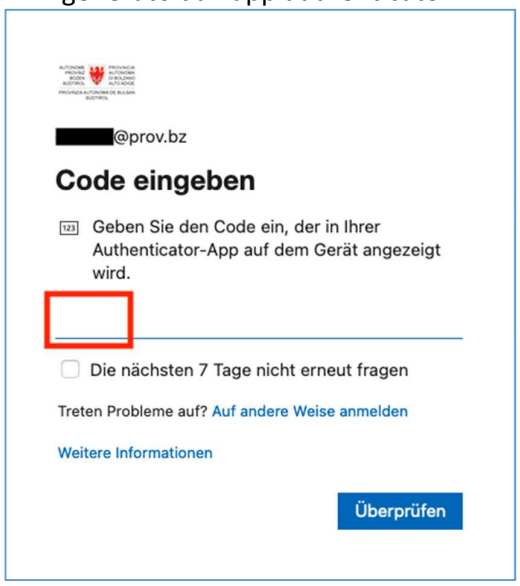


Südtiroler Informatik AG
the e-government company

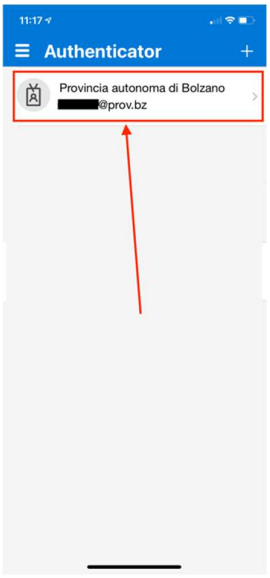
3 Accesso dopo la prima configurazione

Dopo la configurazione dell'autenticazione a fattore multiplo, viene chiesta conferma con il metodo di autenticazione aggiuntivo scelto non appena si prova ad accedere da internet. Nell'esempio seguente viene usata la app come metodo di autenticazione aggiuntivo.

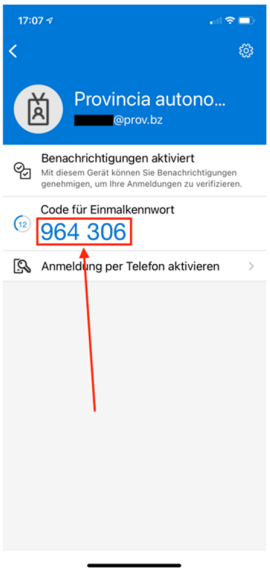
1) Dopo aver inserito nome utente e password, viene chiesto di inserire il codice generato dall'app authenticator:



2) l'utente clicca sul suo account nell'App Authenticator:



3) legge il codice mostrato nell'app:



4) e lo riporta nella finestra per completare l'autenticazione: