FONDAZIONE
BRUNO KESSLER

CONFIGURAZIONE AUTENTICAZIONE MULTI-FATTORE

GUIDA UTENTE

Indice

1. Introduzione

Questo documento fornisce la procedura utente per proteggere il proprio account FBK mediante autenticazione multi-fattore[1] - di seguito denominata MFA. Questo permette, in accordo a quanto riportato da Alex Weinert[2] (direttore di *Identity Security* presso Microsoft), di prevenire il 99.9% degli attacchi all'identità digitale dell'utente. Tuttavia non costituisce una panacea: un attaccante può infatti intercettare la richiesta di accesso e, rubando tutti i dati in arrivo, impersonare l'utente[3]. Suggeriamo di fare quindi particolare attenzione ai meccanismi di rilevazione presentati in Sezione 1.1.

Sarà necessario utilizzare il secondo fattore nei seguenti casi:

- Per accedere a qualsiasi servizio Microsoft e Google con account FBK. Viene richiesto la prima volta ed ogni 30 giorni, a meno di non cambiare indirizzo da cui ci si collega (es. utilizzando reti Wifi differenti o la connessione dello smartphone);
- Per azioni amministrative sul cloud Microsoft Azure con un account FBK;
- Per il reset in autonomia della propria password FBK oppure quando Microsoft rileva un comportamento anomalo dell'account[4];
- Quando Microsoft rileva un rischio medio o elevato in fase di autenticazione[4].

Il pilot a cui questo documento fa riferimento rientra nel primo dei punti identificati per proteggere l'infrastruttura FBK (progetto biennale Zero Trust). Per maggiori informazioni o in caso di problemi, contattare help-it@fbk.eu.

Di seguito viene spiegato come configurare MFA tramite Microsoft Authenticator[5] come applicazione mobile (da PC illustrato in Sezione 2.1, da smartphone in Sezione 2.3).

Suggeriamo di configurare due metodi di autenticazione su due dispositivi diversi, poichè in caso di furto/smarrimento o sostituzione di uno dei due, l'accesso ai servizi di FBK sarà comunque possibile.

L'esperienza utente dopo aver configurato MFA è illustrata in Sezione 3.

[1] Per approfondire l'autenticazione multi-fattore, fare riferimento al seguente LINK.
[2] Per approfondire i tipi di attacco contro un'autenticazione basata su password, vedi LINK.
[3] Per approfondire i tipi di attacco contro l'autenticazione multi-fattore e possibili difese, vedi LINK.
[4] Per i comportamenti che Microsoft considera a rischio in fase di autenticazione (*Sign-in risk*) o uso dell'account (*User risk*) fare riferimento a LINK.
[5] Per configurare un'applicazione mobile di autenticazione differente (es. *Google Authenticator*), selezionare "voglio usare un'app di autenticazione diversa" (Paragrafo 2.1 V della Guida).

1.1. Difendersi dal furto d'identità

Come introdotto, anche un meccanismo di autenticazione multi-fattore è suscettibile ad attacchi informatici. In particolare, un attaccante riesce a impersonare l'utente se:

1. [In prossimità dell'utente] osserva le credenziali di accesso, anticipandolo nel login.

Rilevazione: mancato login; ricezione notifica per email, SMS o applicazione mobile, relativa all'accesso da nuovo dispositivo e/o locazione.
Possibili mitigazioni: (PRE) controllare di non essere osservato durante il login;
(POST) effettuare tempestivamente il logout dalle sessioni e da dispositivi non riconosciuti - LINK Google, LINK Microsoft.

2. [In prossimità dell'utente] conosce username e password dell'utente, ed entra in possesso del dispositivo utilizzato come secondo fattore (es. cellulare o chiavetta hardware).

Rilevazione: come in #1, anche se l'attaccante potrebbe cancellare le email/sms in maniera semplice e veloce. Controllare in maniera ricorrente le sessioni attive - LINK Google, LINK Microsoft.
Possibili mitigazioni: (PRE) scegliere una password "opportuna"[6]; non abbandonare il dispositivo utilizzato come secondo fattore (in caso di dispositivo mobile, proteggerlo con uno dei meccanismi supportati - es. PIN o impronta);
(POST) effettuare tempestivamente il logout dalle sessioni e da dispositivi non riconosciuti - LINK Google, LINK Microsoft.

3. [Da remoto] entra in possesso delle credenziali di accesso e secondo fattore avendo manomesso il browser, il sistema operativo e/o il dispositivo dell'utente. Per estensione, anche se meno probabile, compromette utenti amministratori in FBK, server FBK o di Google/Microsoft.

Rilevazione: come in #2.
Possibili mitigazioni: (PRE) mantenere aggiornati e sicuri i dispositivi utilizzati (es. utilizzare una soluzione antivirus);
(POST) effettuare tempestivamente il logout dalle sessioni e da dispositivi non riconosciuti - LINK Google, LINK Microsoft.

4. [Da remoto] si inserisce nelle comunicazioni tra utente e server e ruba i cookie[7].

Rilevazione: anche se l'icona del lucchetto mostrata dal browser[8] e i dettagli (cliccandoci) mostrano che la connessione è sicura/affidabile[9], il prefisso dell'URL è differente da https://accounts.google.com/ o https://login.microsoftonline.com/.
Ad esempio, potrebbe essere https://fbk-login.com, https://accounts.fbk.google.com o https://accounts.fbk-google.com/; oppure ancora https://login.mcrsft-online.com.

---

[6] Le ultime raccomandazioni (SP 800-63B) del National Institute of Standards and Technologies (NIST) raccomandano una password lunga almeno 8 caratteri (fino a 64) e semplice da ricordare (non forzare l'uso di minuscole, maiuscole o caratteri speciali); ovviamente, non banale (es. intervallo da 1 a 10, *nome, cognome* e simili).
[7] Un cookie è un oggetto tipicamente inviato al browser dell'utente quando si visita una pagina web. Viene utilizzato di norma per mantenere una sessione per ciascun utente che si autentica: una volta fatto il login, il server invia un cookie univoco al browser e questo lo usa in ogni successiva richiesta; in questo modo non occorre che l'utente debba autenticarsi per ogni pagina visitata.
[8] Per approfondimenti, fare riferimento a LINK Safari, LINK Chrome, LINK Firefox, LINK Edge.
[9] Di norma, un attaccante scaltro utilizza un server con un certificato valido che permette anche le connessioni considerate sicure dal browser utilizzato.

Come spiegato da Microsoft (LINK), esistono modalità di attacco per cui l'utente non è in grado di distinguere l'esperienza di login malevola da quella prevista: tranne l'URL, corrispondono tutti i loghi, la loro posizione ed il testo (sia di Google/Microsoft, che eventuali personalizzazioni dell'interfaccia introdotte da FBK); in aggiunta, se l'attacco avviene attraverso un'email malevola[10], un attaccante potrebbe riuscire a pre-compilare il campo username per trarre ulteriormente in inganno l'utente.
Infine, diversamente dall'attacco #1, l'utente riesce a tutti gli effetti ad accedere al servizio richiesto ed i portali di Google e Microsoft non possono rilevare il login dell'attaccante (mai avvenuto poiché ruba la sessione attiva dell'utente).
Possibili Mitigazioni: (PRE) utilizzare una chiavetta hardware (es. YubiKey) e verificare le email inviate da Google/Microsoft come riportato in LINK - e.s. campo "firmato da" con valore "accounts.google.com" o "accountprotection.microsoft.com".
(POST) Controllare in maniera ricorrente le regole impostate nella propria email (LINK).

2. Procedura di configurazione

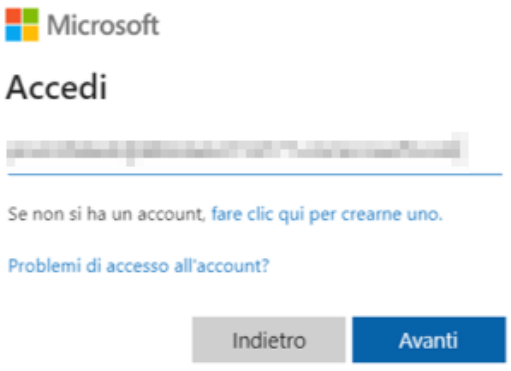
Questa procedura guida l'utente nella configurazione dell'app Microsoft Authenticator come fattore di autenticazione aggiuntivo, allo scopo di proteggere l'account FBK.

2.1. Configurazione tramite PC

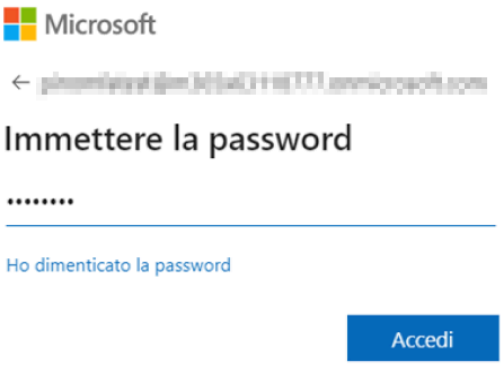
Di seguito sono indicati gli step da seguire per avviare la procedura da PC.

I. **Collegarsi via browser** al seguente indirizzo: https://aka.ms/mfasetup.

II. Se non è già stato fatto, **eseguire l'accesso con le proprie credenziali utente**.



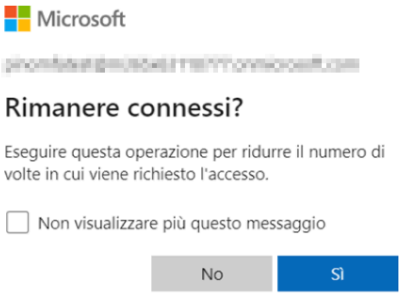
Schermata inserimento nome utente (indirizzo email)



Schermata inserimento password

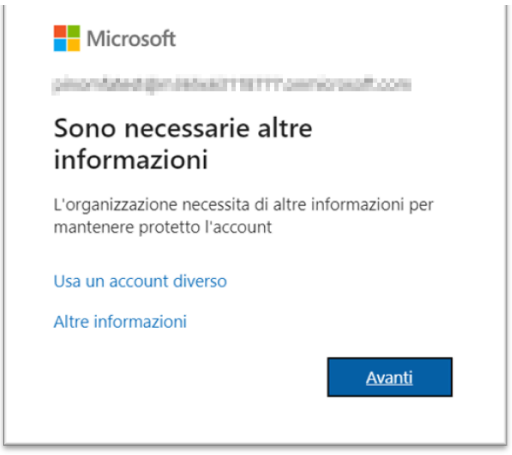
[10] Per approfondire il fenomeno del *Phishing*, visita LINK.

III. Se compare la schermata seguente, cliccare su *NO* se ci si collega da una rete wireless/cablata esterna (non personale o di FBK) o da dispositivo non personale.



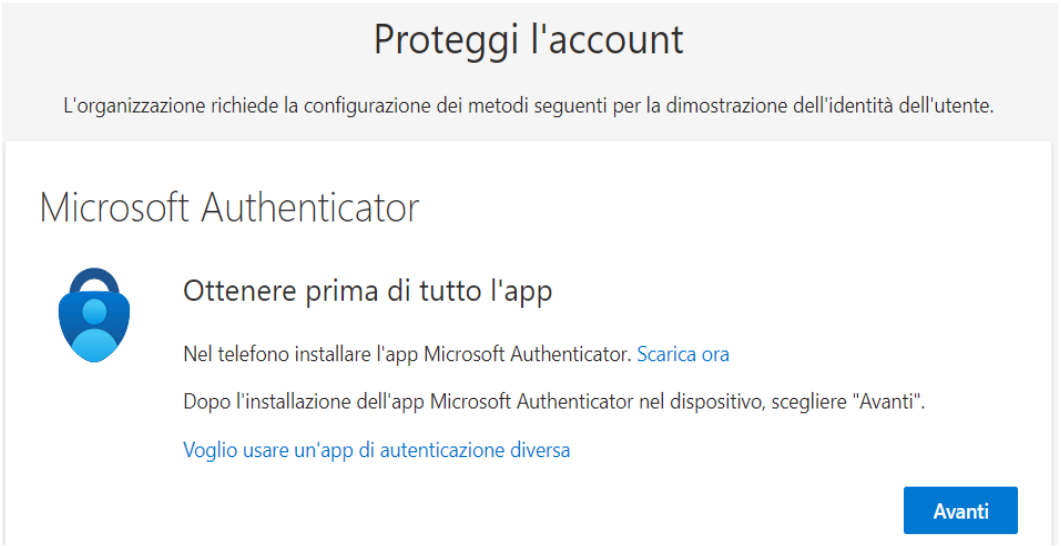
Schermata persistenza sessione

IV. Verrà visualizzata una pagina che richiede la registrazione di informazioni aggiuntive. **Cliccare su *Avanti*:**



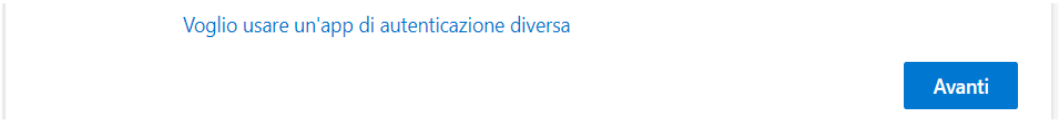
Schermata che informa della necessità di impostare MFA

V. Se ancora non è stato fatto, <u>scaricare sul proprio smartphone l'applicazione Microsoft Authenticator</u> come suggerito dalla pagina e **cliccare *su Avanti***.



Prima schermata di configurazione MFA selezionando MS Authenticator (da browser)

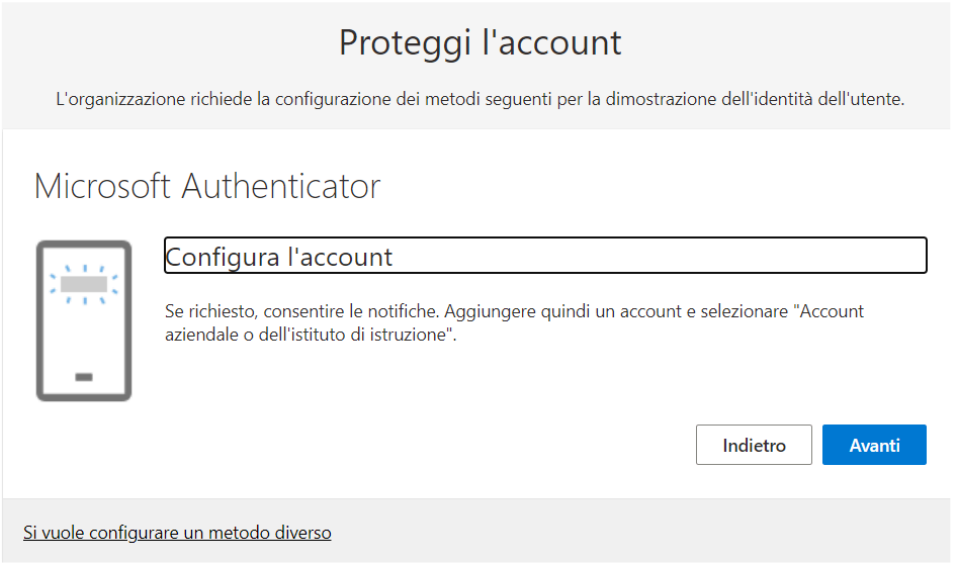
In alternativa, è possibile utilizzare un'applicazione di autenticazione diversa da Microsoft Authenticator: in tal caso cliccare su ***Voglio usare un'app di autenticazione diversa.***



Per Google Authenticator, avviare l'applicazione sul proprio dispositivo mobile, fare clic sull'icona "+" e successivamente "Scansiona un codice QR". Inquadrare il codice QR mostrato a schermo, successivamente fare clic su "avanti" nel browser e inserire il codice di 6 cifre generato da Google Authenticator. Facendo ancora clic su "avanti", la seguente notifica conferma l'avvenuta registrazione;

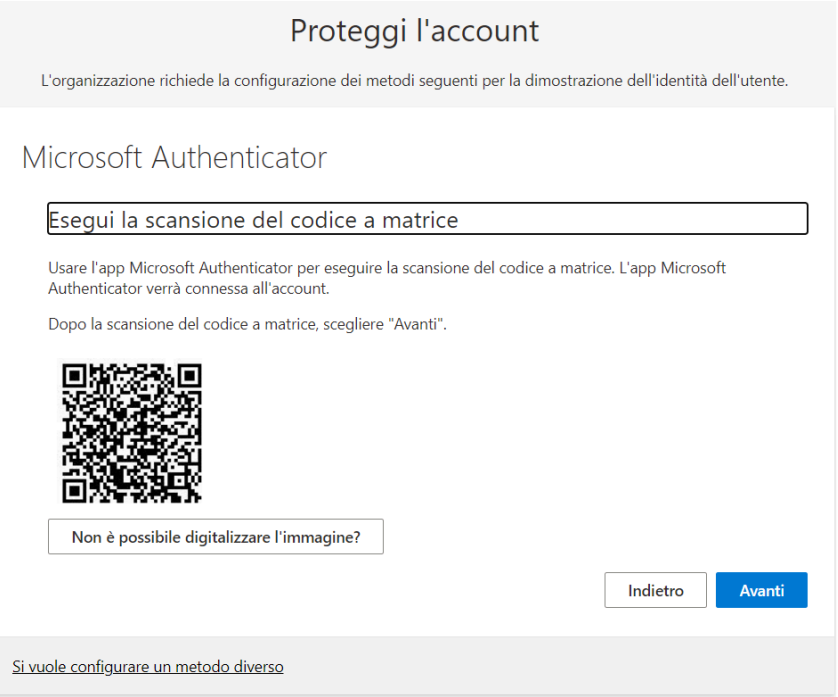
Esempio di notifica di avvenuta registrazione

VI. **Cliccare su *Avanti*** nella schermata successiva per avviare la configurazione di Microsoft Authenticator sul proprio dispositivo mobile.



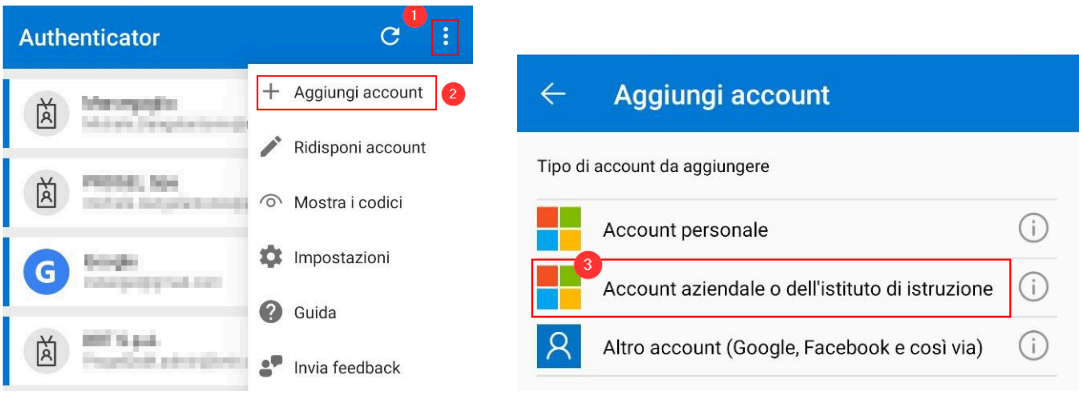
Seconda schermata di configurazione MFA su browser (MS Authenticator)

VII. Compare ora una schermata con un QR Code da inquadrare in Microsoft Authenticator.



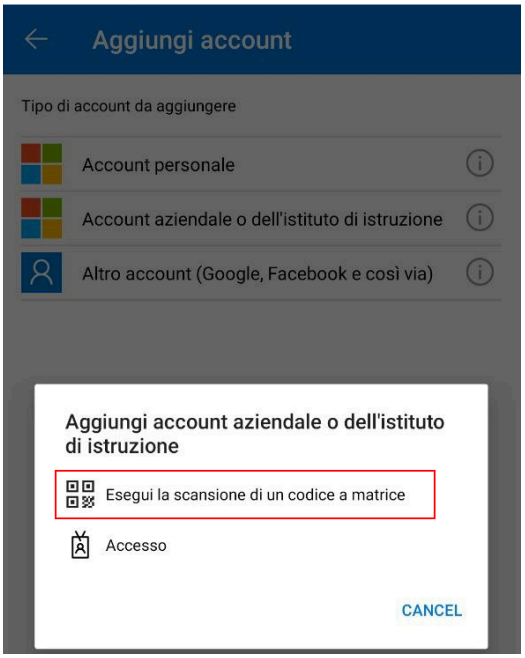
Terza schermata di configurazione MFA su browser (MS Authenticator)

VIII. Aprire quindi l'applicazione sul proprio dispositivo mobile e cliccare sul tasto per aggiungere un account. In Microsoft Authenticator, fare clic su ***"+ aggiungi account"*** e aggiungere un nuovo account di tipo ***"Account aziendale o dell'istituto di istruzione"***



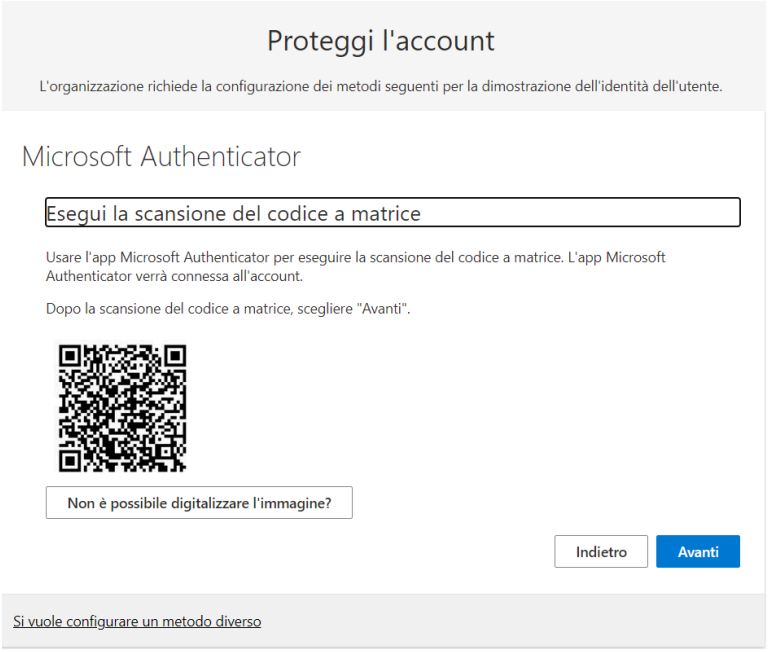
Schermate di configurazione MS Authenticator sul dispositivo mobile

IX. In Microsoft Authenticator, fare tap su ***"Esegui la scansione di un codice a matrice".***



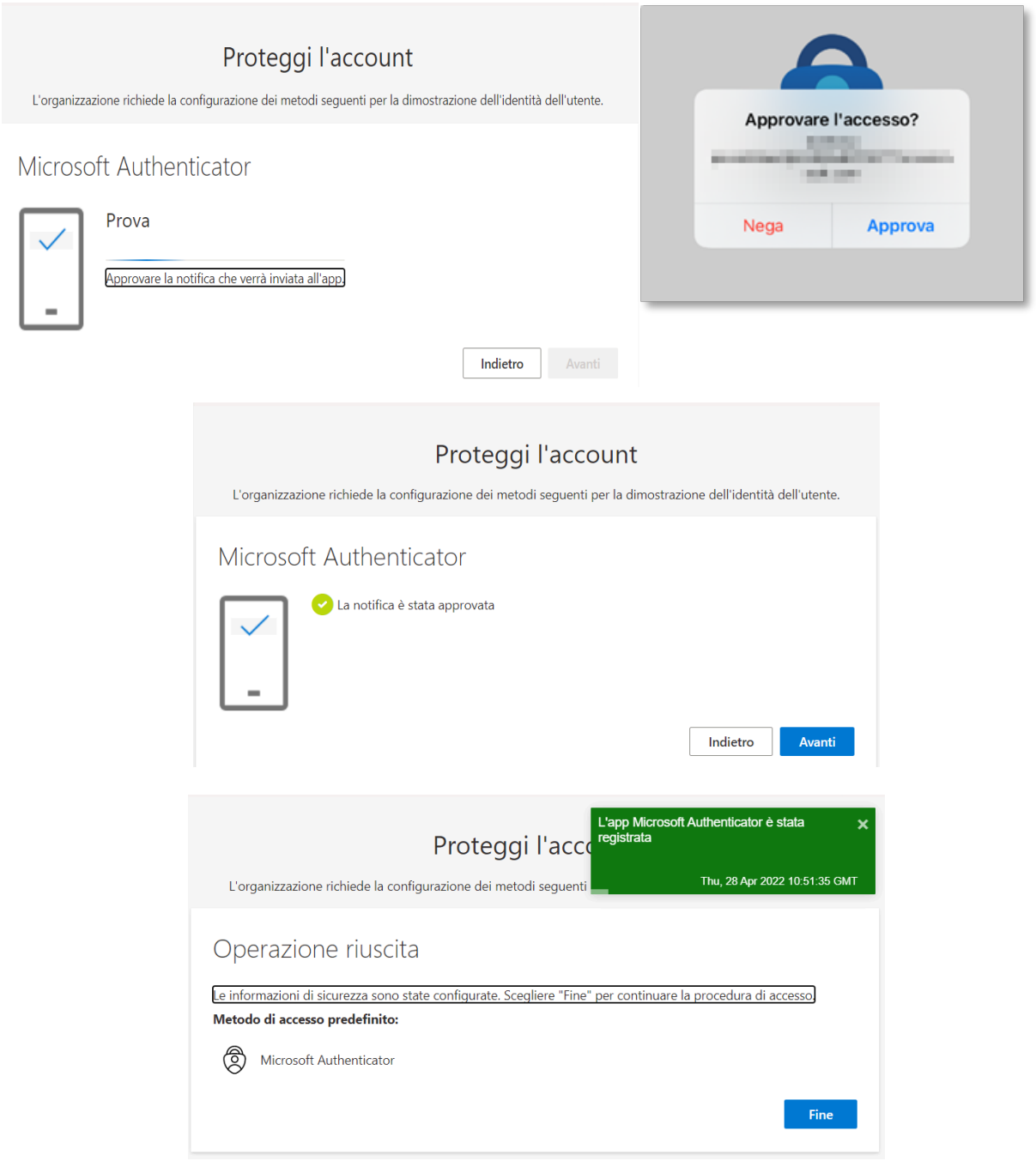
Schermata di configurazione MS Authenticator sul dispositivo mobile

X. Usare Microsoft Authenticator (o altra app di autenticazione) per **inquadrare con la fotocamera il codice QR** sulla schermata del pc.



Quarta schermata di configurazione MFA su browser (MS Authenticator)

XI. Nel caso di Microsoft Authenticator, è necessario **cliccare su *Avanti*** per arrivare nella schermata di attesa approvazione tramite notifica sull'applicazione mobile (codice numerico OTP); approvare quindi la notifica e verificare da PC che tutto sia andato a buon fine.



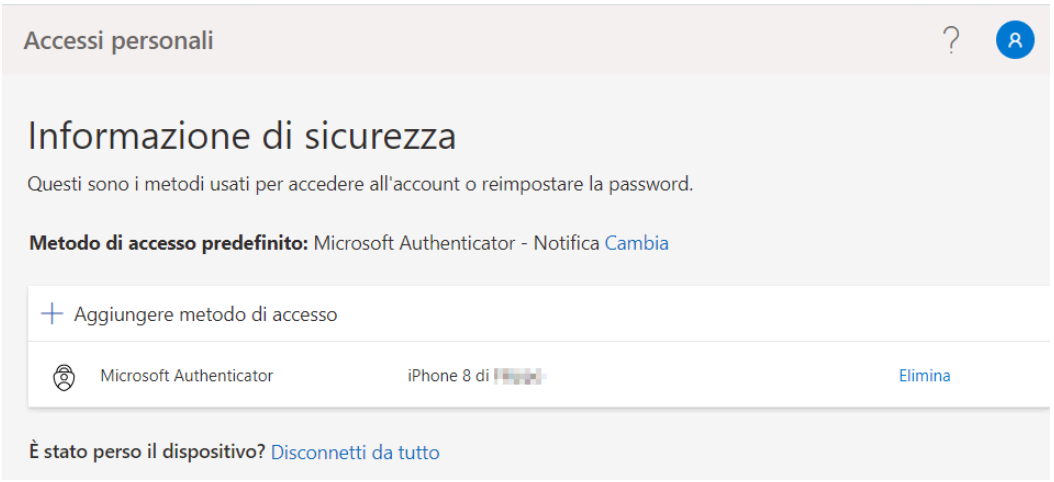
Schermate di invio notifica dal browser (in alto a sinistra), ricezione notifica sul mobile (in alto a destra) e conferme di fine configurazione.

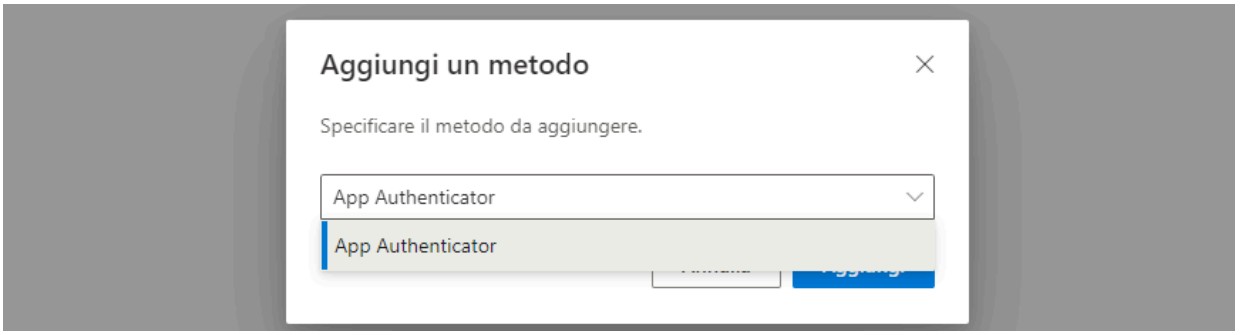
La notifica conferma che la procedura di configurazione con MS Authenticator è stata **completata**.

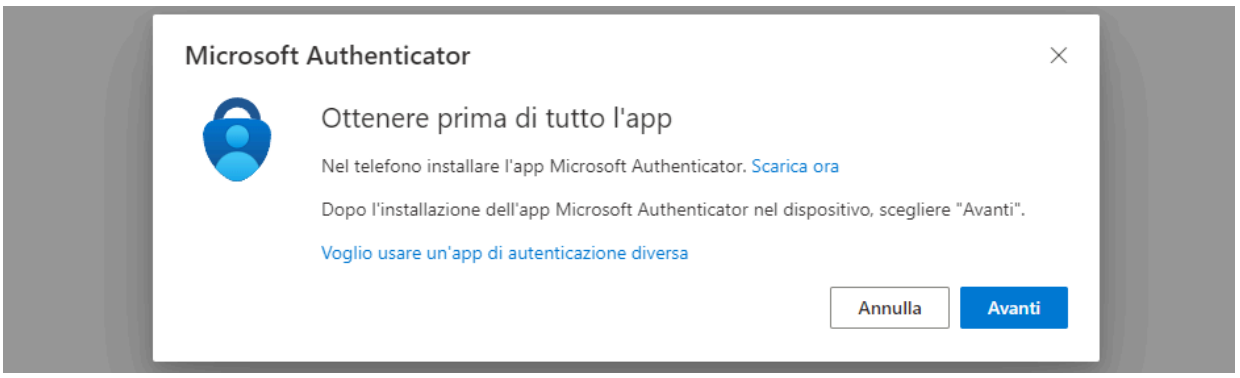
2.2. Configurazione aggiuntiva dell'applicazione autenticatore

Una volta completata la procedura (applicazione mobile) la schermata mostra che è possibile aggiungere ulteriori metodi di verifica tra quelli supportati.
Visitare in alternativa https://mysignins.microsoft.com/security-info entrando con l'account FBK.

Proseguire per l'applicazione autenticatore come indicato in Sezione 2.1;





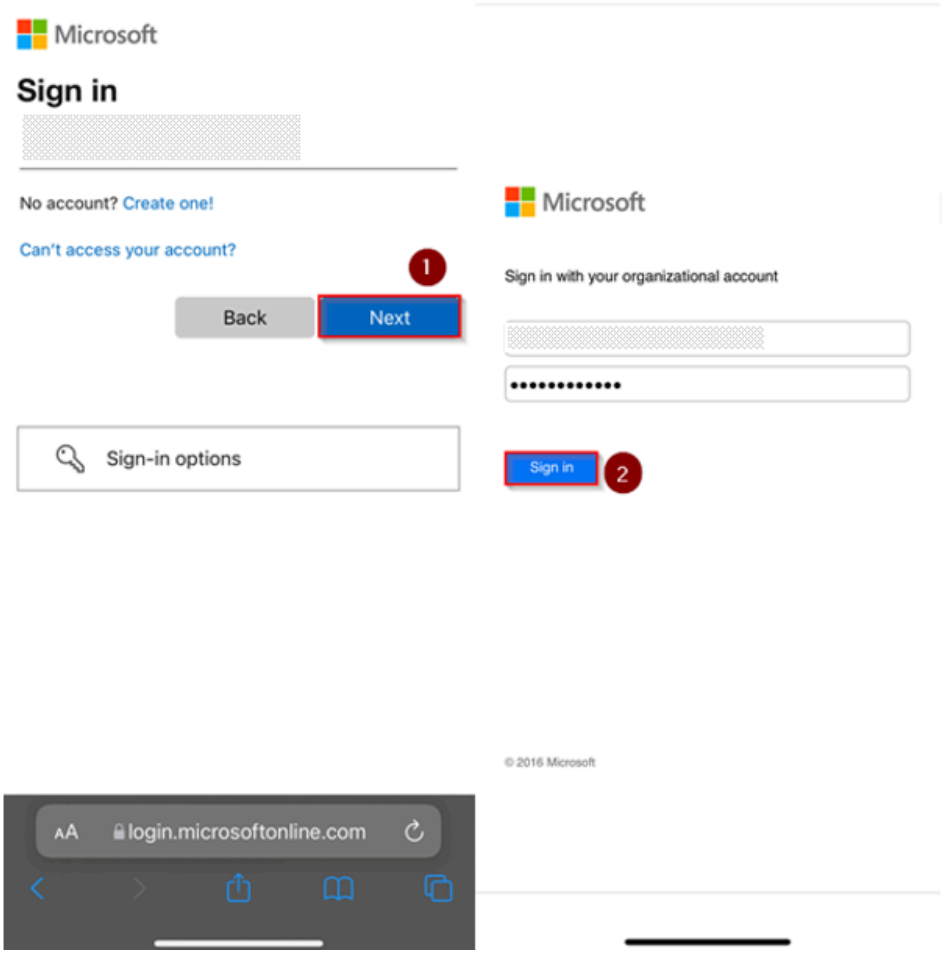


2.3. Configurazione MS Authenticator tramite smartphone

Di seguito sono indicati gli step da seguire per registrare il dispositivo mobile come fattore di autenticazione secondario al proprio account FBK, tramite l'utilizzo del cellulare.

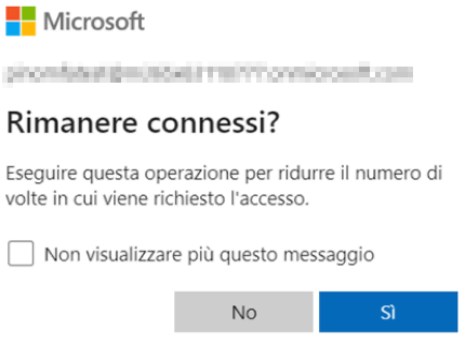
I. **Collegarsi via browser** al seguente indirizzo: https://aka.ms/mfasetup.

II. Se non è già stato fatto, **eseguire l'accesso con le proprie credenziali utente** (account FBK oppure account esterno utilizzato per accedere alle risorse FBK).



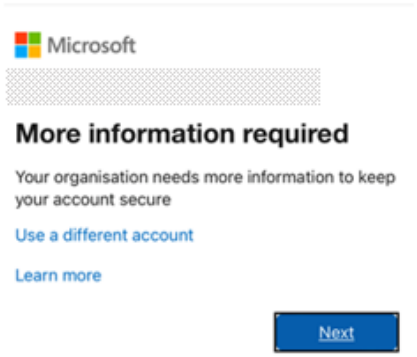
Schermate di login sul dispositivo mobile

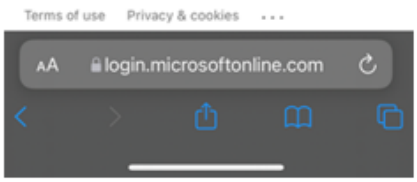
III. Se compare la seguente schermata cliccare su *NO* se ci si collega da una rete wireless/cablata esterna (non personale o di FBK) o da dispositivo non personale.



Schermata per la persistenza della sessione

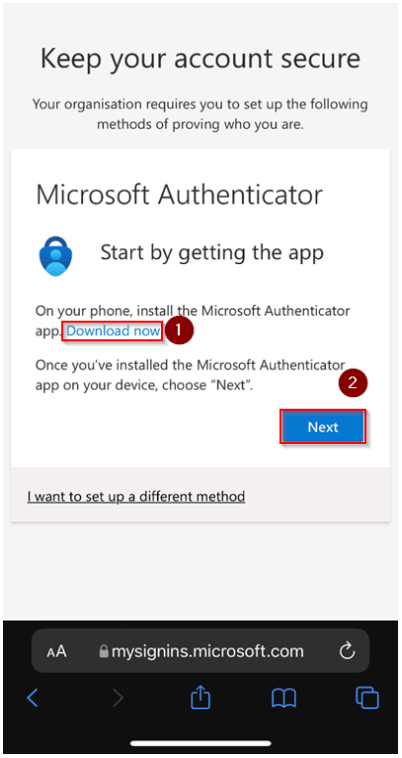
IV. Verrà visualizzata una pagina che richiede la registrazione di informazioni aggiuntive. **Cliccare su *Avanti*:**





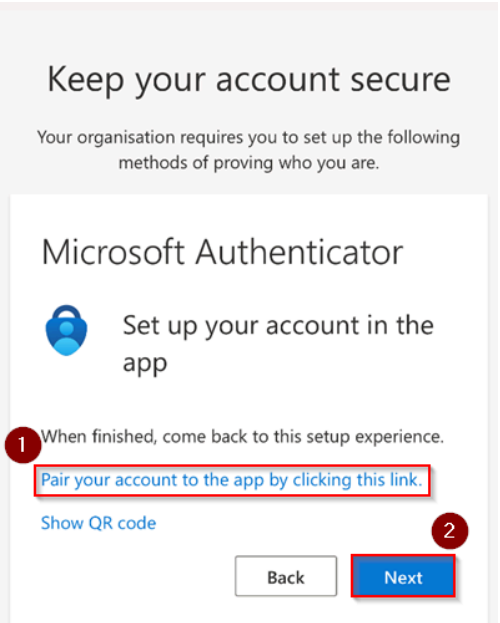
Prima schermata di configurazione MS Authenticator da dispositivo mobile

V. Se ancora non è stato fatto, scaricare l'applicazione Microsoft Authenticator e **cliccare su *Avanti***:



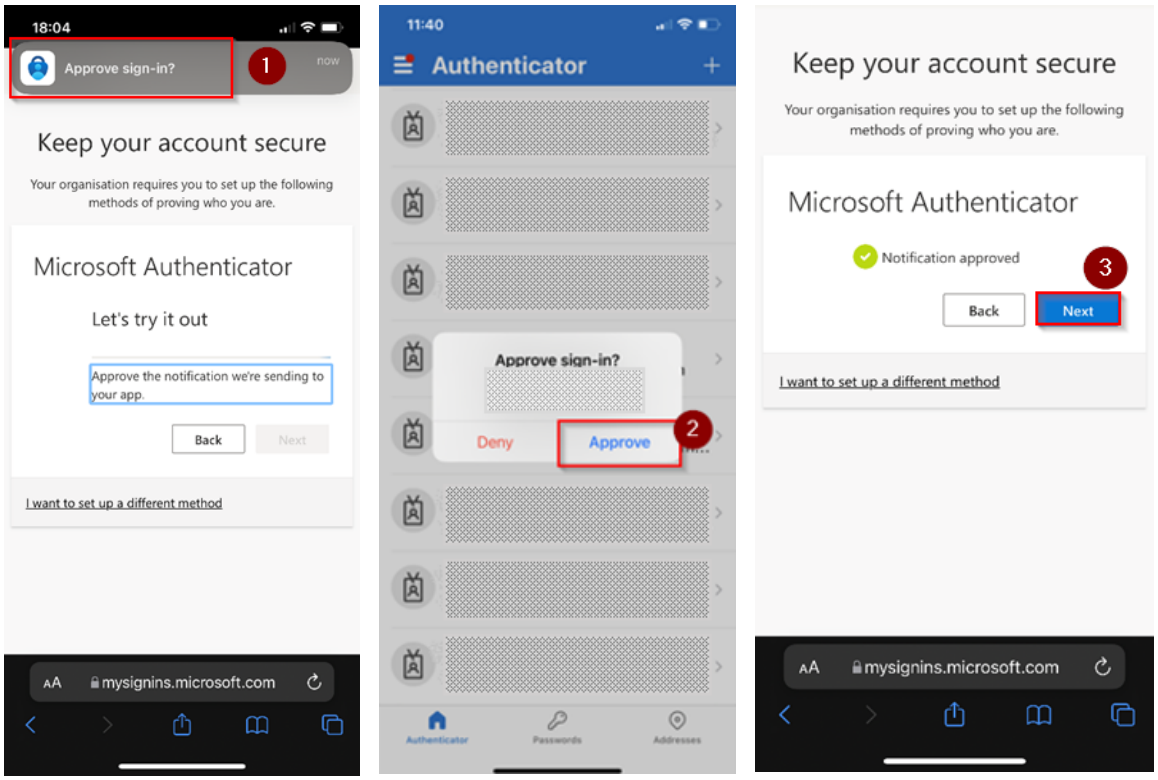
Schermata che invita al download di MS Authenticator

VI. Dopo aver scaricato l'app cliccare su "*Collega il tuo account all'app cliccando su questo link*":



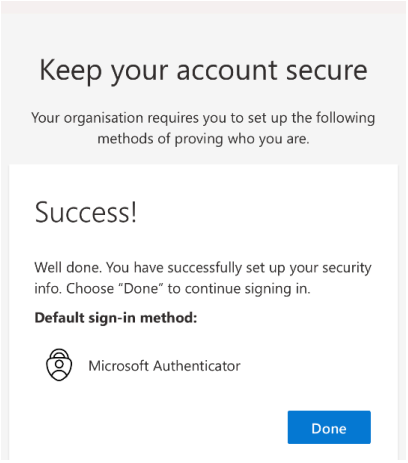
Schermata per l'invio di una notifica all'applicazione mobile MS Authenticator

VII. Dall'app Authenticator **approvare la notifica** di richiesta autenticazione.
Nella schermata sul browser **cliccare poi su *Avanti***:



Approvazione e conferma della notifica per la registrazione di MS Authenticator sul mobile

VIII. Nella schermata successiva **cliccare su *Done***:



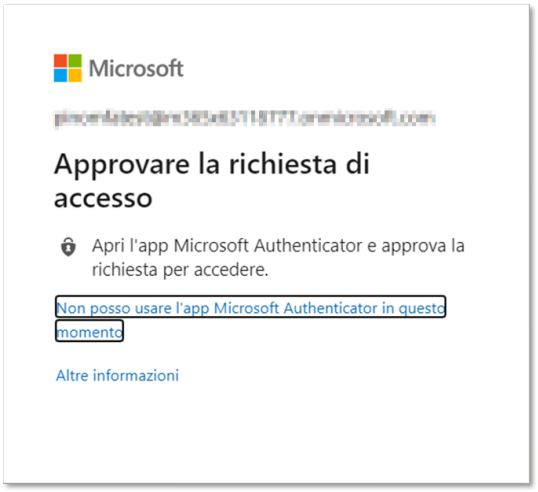
Schermata di conferma avvenuta registrazione

La procedura di configurazione è stata **completata**.

3. Esperienza utente dal prossimo sign in

Dal prossimo accesso, dopo l'inserimento della password all'utente verrà chiesto di verificare la propria identità con uno dei metodi precedentemente configurati.

Il metodo di default è la notifica tramite Microsoft Authenticator: l'utente approverà la notifica sul proprio dispositivo e proseguirà con l'autenticazione.



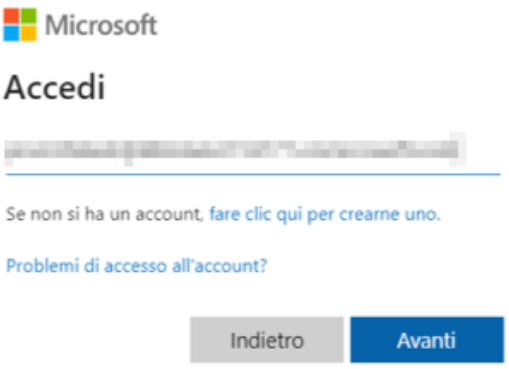
Schermata di richiesta di fattore aggiuntivo per l'autenticazione

4. Cosa fare in caso di sostituzione del device

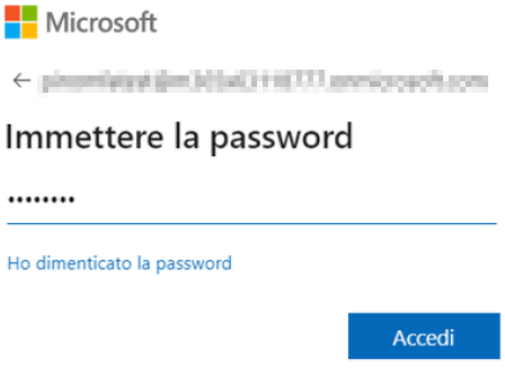
In caso di sostituzione del dispositivo mobile su cui è installato l'autenticatore mobile, è necessario seguire la procedura qui descritta, prima di dismettere il dispositivo.
Le operazioni risultano più semplici utilizzando il browser di un PC.

I. **Collegarsi via browser** al seguente indirizzo: https://aka.ms/mfasetup.

II. Se non è già stato fatto, **eseguire l'accesso con le proprie credenziali utente** (account FBK oppure account esterno utilizzato per accedere a risorse FBK).

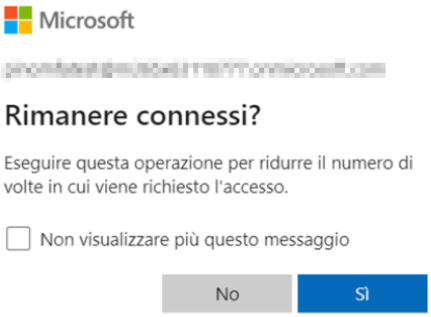


Schermata inserimento nome utente



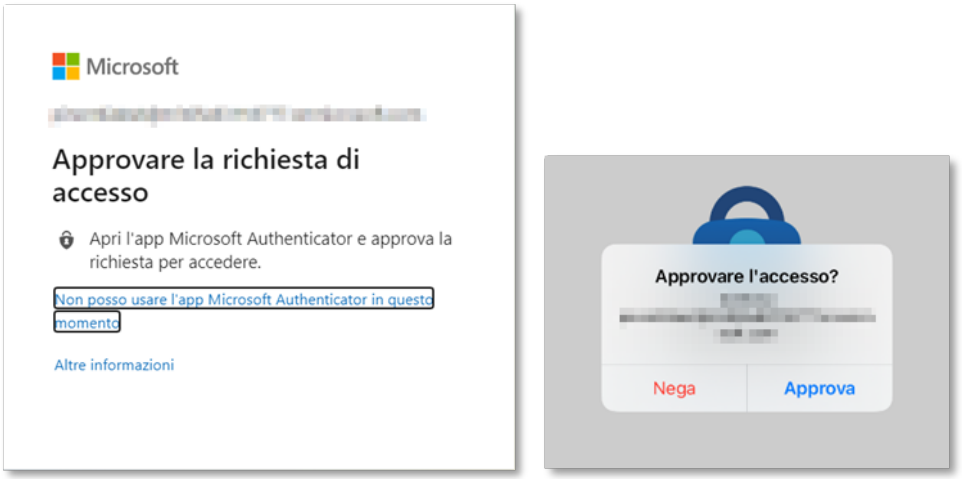
Schermata inserimento password

III. Se compare la schermata seguente, cliccare su *NO* se ci si collega da una rete wireless/cablata esterna (non personale o di FBK) o da dispositivo non personale.



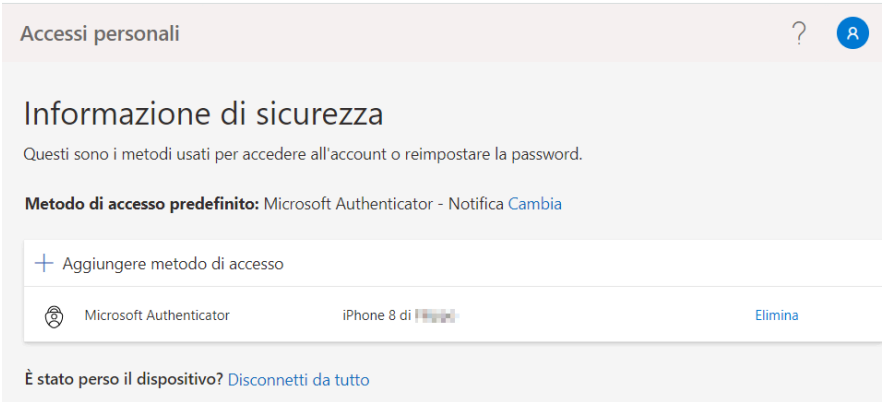
Schermata persistenza sessione

IV. Dall'app Authenticator **approvare la notifica** di richiesta autenticazione:



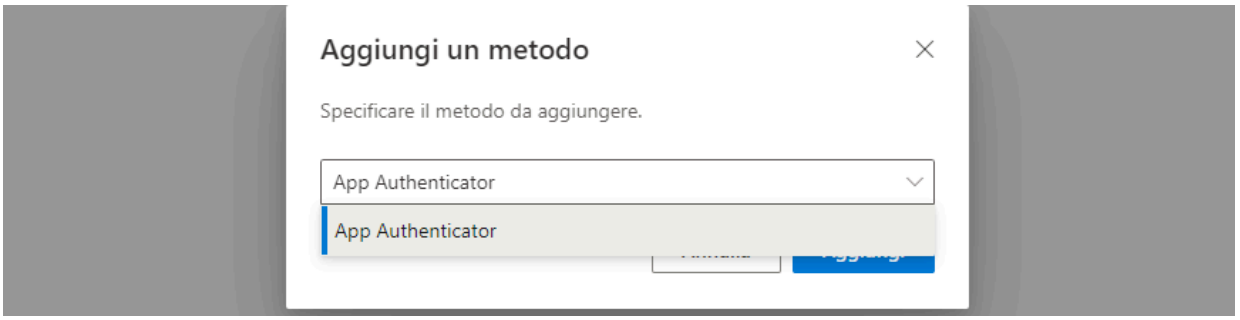
Autenticazione mediante notifica

V. Nella pagina che viene mostrata **cliccare su *Aggiungere metodo di accesso***:



Schermata per l'aggiunta di meccanismi MFA al proprio account

VI. Dal menù a tendina scegliere un altro metodo di configurazione



Schermata con meccanismi disponibili

Proseguire con la procedura di configurazione, e una volta terminata eliminare l'app mobile del vecchio device tramite l'apposito tasto ***Elimina***.

5. Cosa fare in caso di smarrimento del device

Nel caso in cui il dispositivo utilizzato come secondo fattore di autenticazione (con l'applicazione Microsoft Authenticator o altra) dovesse essere stato smarrito o comunque fosse inutilizzabile, è necessario contattare l'Help Desk (help-it@fbk.eu) che dovrà forzare la richiesta di registrazione del secondo fattore di autenticazione.

Una volta eseguito il reset da parte dell'Help Desk, è possibile procedere con la registrazione di una nuova applicazione per l'MFA, seguendo gli step in Sezione 2.