

# MFA - Multi Faktor Authentifizierung

Benutzerhandbuch

1	Einleitung.....	2
1.1	Umgebung in welcher die MFA erforderlich ist .....	2
2	Die erste Anmeldung über das Internet.....	3
2.1	Teil 1: Einrichtung des Telefons als zweiter Sicherheits-Faktor.....	3
2.2	Teil 2: Einrichtung einer E-Mail-Adresse als zweiter Sicherheits-Faktor .....	5
2.3	Optional: Einrichtung der Mobile App „Microsoft Authenticator“.....	6
2.3.1	Die Microsoft Authenticator-App am Mobiltelefon einrichten .....	9
3	Anmeldungen nach der ersten Einrichtung .....	10

## 1 Einleitung

Um den **Schutz Ihrer Identität und Ihrer Daten** vor unbefugtem Zugriff zu verbessern, wird in der Landesverwaltung der Autonomen Provinz Bozen ab 2021 die sogenannte „Multi Faktor Authentifizierung“, kurz MFA, eingeführt.

Mit Hilfe dieser Technologie wird die Zugangsberechtigung durch folgende, unabhängige Merkmale (Faktoren) überprüft:

- den Faktor „Wissen“ bestehend aus Benutzername und Kennwort
- den zusätzlichen Faktor „Besitz“ bestehend aus einer Komponente im Besitz des Benutzers:
  - das Mobiltelefon (SMS, Anruf, App)
  - das Haus- oder Geschäftstelefon (Anruf)
  - eine zweite E-Mail-Adresse (E-Mail)

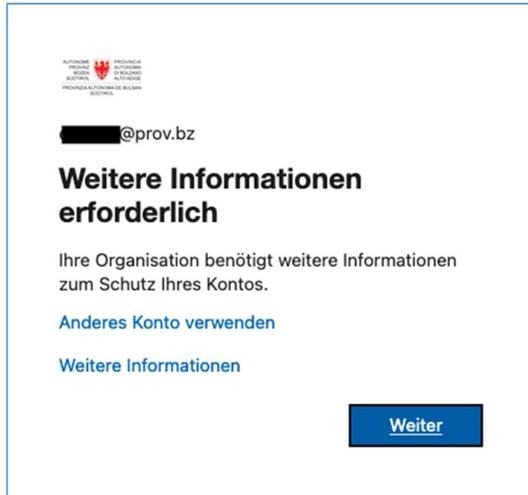
### 1.1 Umgebung in welcher die MFA erforderlich ist

Die neue Authentifizierung wird von den Benutzern der Landesverwaltung nur verlangt, falls diese sie aus dem Internet auf Dienste zugreifen wollen, wie z.B. zur Nutzung der Microsoft Office Suite über <https://www.office.com>.

Für den normalen Einstieg am Arbeitsplatz-PC im Büro ist die MFA **nicht erforderlich**.

## 2 Die erste Anmeldung über das Internet

Sobald die MFA Funktion für Ihren Benutzer aktiviert ist, wird beim Versuch auf einen Online-Dienst zuzugreifen, die Einrichtung der MFA von Ihnen verlangt:



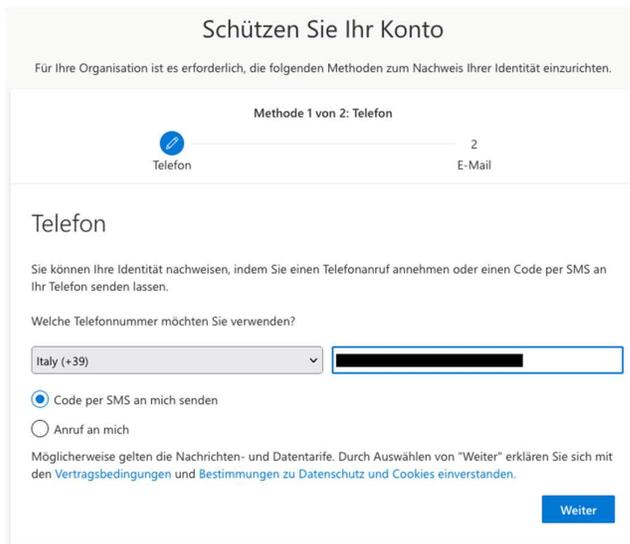
The screenshot shows a login page for a user with the email address [redacted]@prov.bz. The page title is "Weitere Informationen erforderlich" (Further information required). The text states: "Ihre Organisation benötigt weitere Informationen zum Schutz Ihres Kontos." (Your organization needs further information to protect your account). There are two links: "Anderes Konto verwenden" (Use another account) and "Weitere Informationen" (More information). A blue "Weiter" (Next) button is located at the bottom right.

Nach einem Klick auf „Weiter“ werden Sie aufgefordert, erst eine Telefonnummer und schließlich eine weitere E-Mail-Adresse als zweiten Faktoren zur Überprüfung Ihrer Identität einzurichten.

### 2.1 Teil 1: Einrichtung des Telefons als zweiter Sicherheits-Faktor

Die Einrichtung des Telefons ist der erste, obligatorische Teil der Konfiguration und kann sei es mittels Zustellung eines Codes in Form einer SMS oder mittels eines Anrufs erfolgen.

Eingabe der Nummer und Auswahl der Zustellungsmethode für den Überprüfungs-Code:



The screenshot shows the "Schützen Sie Ihr Konto" (Protect your account) setup page. It indicates that the user's organization requires the following methods to verify their identity. The user has selected "Methode 1 von 2: Telefon" (Method 1 of 2: Phone). The "E-Mail" method is also available. The "Telefon" section explains that the user can verify their identity by answering a phone call or receiving a code via SMS. The user is asked to provide a phone number, with a dropdown menu for the country code (Italy (+39)) and a text input field for the number. The user has selected "Code per SMS an mich senden" (Send code per SMS to me). A blue "Weiter" (Next) button is at the bottom right.

### Variante 1 - Zustellung des Codes in Form einer SMS:

#### Schützen Sie Ihr Konto

Für Ihre Organisation ist es erforderlich, die folgenden Methoden zum Nachweis Ihrer Identität einzurichten.

Methode 1 von 2: Telefon

Telefon 2  
E-Mail

#### Telefon

Wir haben gerade einen 6-stelligen Code an +39 [REDACTED] gesendet. Geben Sie den Code unten ein.

Code eingeben

[Code erneut senden](#)

### Variante 2 - Zustellung des Codes mittels eines Anrufs:

#### Schützen Sie Ihr Konto

Für Ihre Organisation ist es erforderlich, die folgenden Methoden zum Nachweis Ihrer Identität einzurichten.

Methode 1 von 2: Telefon

Telefon 2  
E-Mail

#### Telefon

Wir rufen jetzt +39 [REDACTED] an.

Wurde der Code aus der SMS korrekt eingegeben bzw. der Anruf bestätigt mittels drücken der Raute-Taste („#“ am Telefon) bestätigt, ist der erste Teil der Konfiguration abgeschlossen:

#### Schützen Sie Ihr Konto

Für Ihre Organisation ist es erforderlich, die folgenden Methoden zum Nachweis Ihrer Identität einzurichten.

Methode 1 von 2: Telefon

Telefon 2  
E-Mail

#### Telefon

Der Anruf wurde angenommen. Ihr Telefon wurde erfolgreich registriert.

## 2.2 Teil 2: Einrichtung einer E-Mail-Adresse als zweiter Sicherheits-Faktor

Es folgt die Abfrage des zweiten, obligatorischen Teils der Konfiguration mittels Zustellung eines Überprüfungs-Codes an eine zusätzliche, persönliche E-Mail-Adresse:

Schützen Sie Ihr Konto

Für Ihre Organisation ist es erforderlich, die folgenden Methoden zum Nachweis Ihrer Identität einzurichten.

Methode 2 von 2: E-Mail

Telefon E-Mail

---

E-Mail

Welche E-Mail-Adresse möchten Sie verwenden?

[Weiter](#)

[Ich möchte eine andere Methode einrichten.](#)

Schützen Sie Ihr Konto

Für Ihre Organisation ist es erforderlich, die folgenden Methoden zum Nachweis Ihrer Identität einzurichten.

Methode 2 von 2: E-Mail

Telefon E-Mail

---

E-Mail

Wir haben einen Code an [REDACTED] gesendet.

[Code erneut senden](#)

[Weiter](#)

[Ich möchte eine andere Methode einrichten.](#)

Wurde auch dieser Code korrekt eingegeben, ist der obligatorische Teil der Konfiguration abgeschlossen:

Schützen Sie Ihr Konto

Für Ihre Organisation ist es erforderlich, die folgenden Methoden zum Nachweis Ihrer Identität einzurichten.

Methode 2 von 2: Fertig

Telefon E-Mail

---

Erfolgreich!

Sehr gut! Ihre Sicherheitsinformationen wurden erfolgreich eingerichtet. Klicken Sie auf "Fertig", um die Anmeldung fortzusetzen.

**Standardanmeldemethode:**

Telefon +39 [REDACTED]

E-Mail [REDACTED]

[Fertig](#)

### 2.3 Optional: Einrichtung der Mobile App „Microsoft Authenticator“

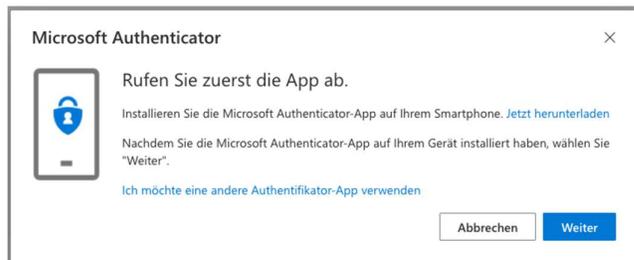
Die Konfiguration der Mobile App erfolgt nach Abschluss der obligatorischen Einrichtung und auf der Seite <https://mysignins.microsoft.com/security-info> mittels Auswahl des Punktes „Methode hinzufügen“:



Wählen Sie in der Folge die Methode „Authenticator-App“ und klicken Sie auf „Hinzufügen“:



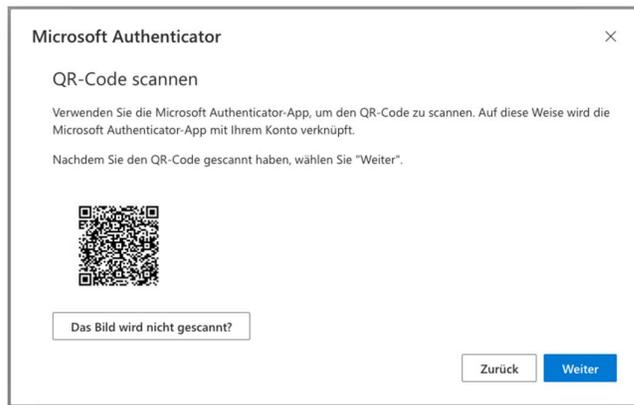
Es folgt eine Aufforderung die entsprechende App auf Ihrem Mobiltelefon zu installieren, inkl. Link zum Download der passenden App. Sobald dies erfolgt ist, klicken Sie auf „Weiter“:



Folgen Sie auch der nächsten Anweisung und klicken Sie auf „Weiter“:



Es wird nun ein QR-Code angezeigt, welcher mit der Mobile App „Microsoft Authenticator“ eingescannt werden muss – **folgen Sie nun den Anleitungen im nächsten Unterabschnitt zur Einrichtung der Mobile App!** Klicken Sie erst nach Abschluss wiederum auf „Weiter“:



Wurden alle Schritte korrekt befolgt werden Sie auf der Webseite dazu aufgefordert es mit der Authentifizierung über Mobile App zu versuchen (siehe dazu das Kapitel „Anmeldungen nach der ersten Einrichtung“ dieses Handbuchs):

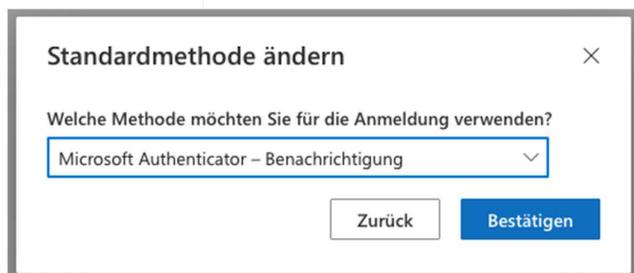
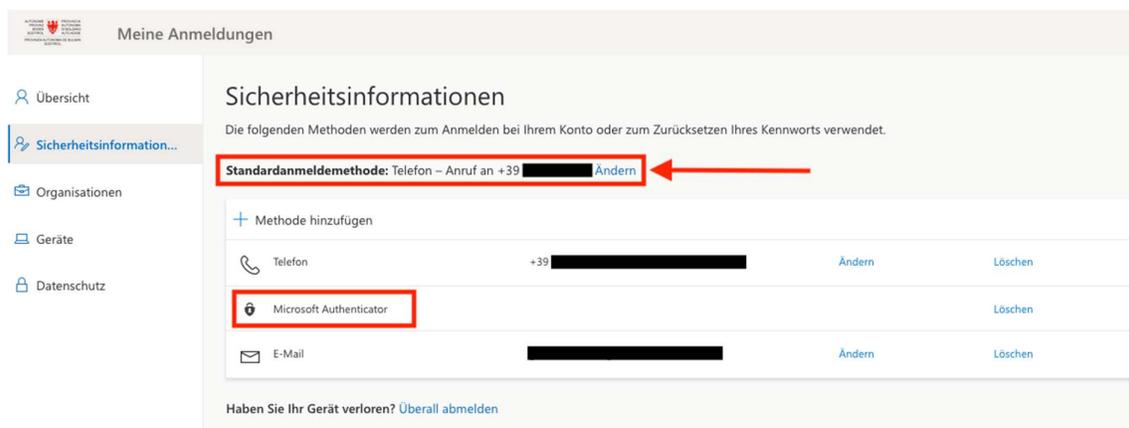


Sofern Sie dieser Aufforderung nun in der Mobile App auf Ihrem Mobiltelefon gefolgt sind, erhalten Sie eine Erfolgsmeldung, welche wieder durch einen Klick auf „Weiter“ geschlossen werden kann:



Die Webseite wechselt nun zurück zur Übersicht zur Konfiguration der eingerichteten Sicherheitsinformationen (<https://mysignins.microsoft.com/security-info>), in welcher nun auch „Microsoft Authenticator“ aufscheint.

**Dazu ein praktischer Hinweis:** für die Nutzung der „Mobile App“ müssen Sie zwar die Microsoft Authenticator App auf Ihrem Mobiltelefon installieren, aber sofern Sie mit Ihrem Mobiltelefon ins Internet gelangen, ist diese Methode die zuverlässigste, da schnellste und es empfiehlt sich die Einrichtung als **Standardanmeldemethode!**

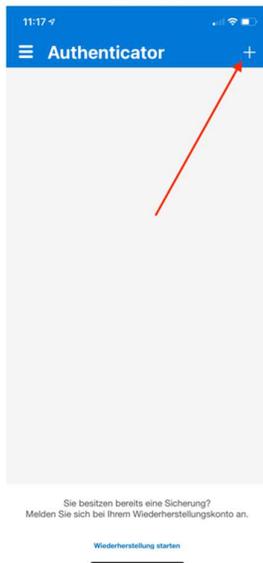


### 2.3.1 Die Microsoft Authenticator-App am Mobiltelefon einrichten

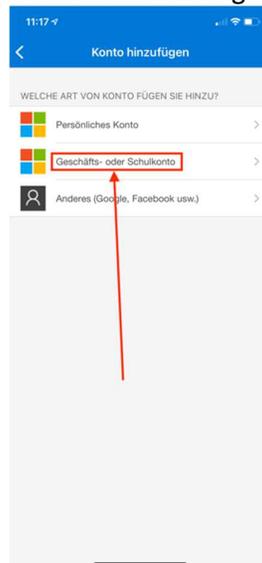
Die oben genannten Anweisungen enthalten u.a. die Links zur „**Microsoft Authenticator-App**“, welche auf dem Mobiltelefon installiert und in wenigen Schritten eingerichtet werden kann:

- für iPhone: <https://go.microsoft.com/fwlink/?linkid=869517>
- für Android: <https://go.microsoft.com/fwlink/?linkid=869516>
- für Windows Phone: <https://go.microsoft.com/fwlink/?linkid=823234>

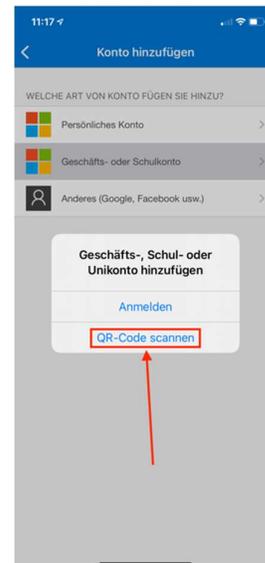
#### 1) das Plus-Symbol anklicken:



#### 2) Geschäfts- oder Schulkonto hinzufügen:



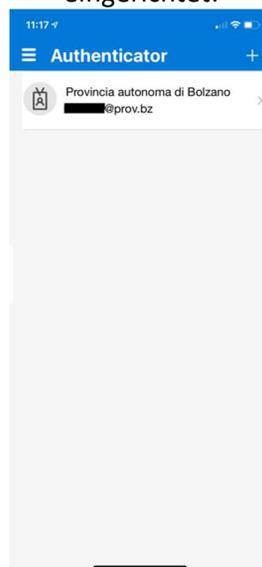
#### 3) QR-Code scannen auswählen:



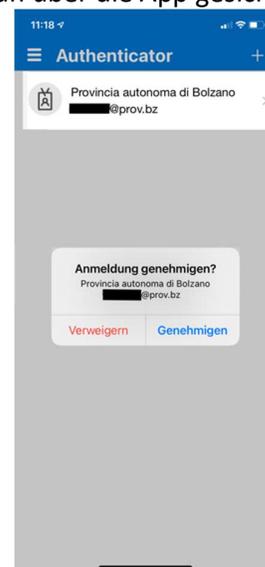
#### 4) QR-Code mit der Kamera einscannen:



#### 5) das Konto ist nun eingerichtet:



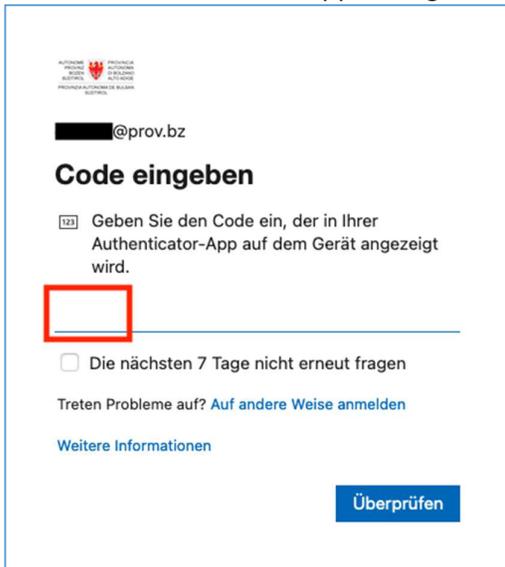
#### 6) das Anmelden ist nun über die App gesichert:



### 3 Anmeldungen nach der ersten Einrichtung

Nachdem die MFA eingerichtet wurde, werden Anmelde-Versuche über das Internet über den gewählten „Faktor“ abgesichert. Im folgenden Beispiel wurde vom Benutzer die „Mobile App“ als Authentifizierungs-Faktor gewählt und für eine Anmeldung genutzt

1) nach Anmeldung mit Benutzername und Kennwort, wird der Benutzer gebeten den Code der Authenticator-App einzugeben:



ALTO ADIGE PROVINCIA AUTONOMA DI BOLZANO  
AUTONOME PROVINZ BOZEN SÜDTIROL  
PROVINCIA AUTONOMA DE BULZAN  
SÜDTIROL

██████████@prov.bz

### Code eingeben

123 Geben Sie den Code ein, der in Ihrer Authenticator-App auf dem Gerät angezeigt wird.

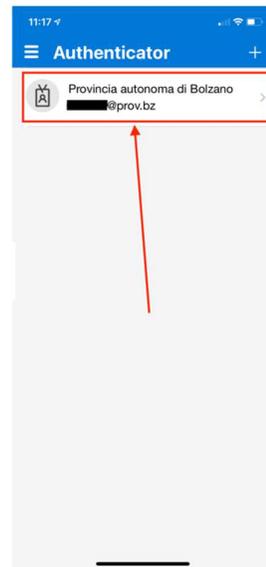
Die nächsten 7 Tage nicht erneut fragen

Treten Probleme auf? [Auf andere Weise anmelden](#)

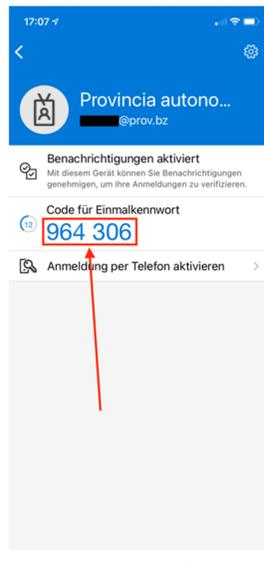
[Weitere Informationen](#)

**Überprüfen**

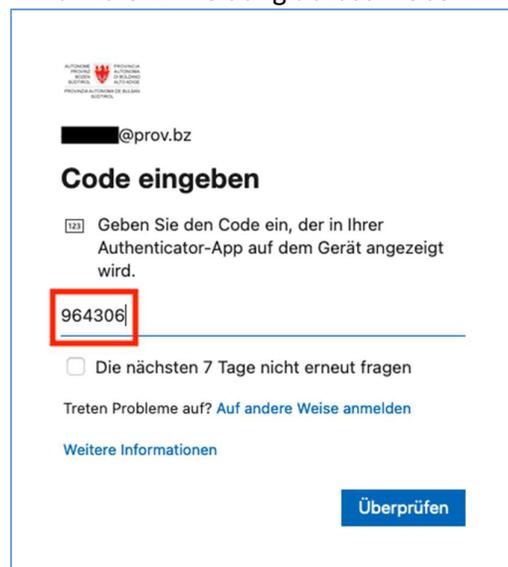
2) der Benutzer wählt in der Authenticator-App auf seinem Mobiltelefon seinen PROV.BZ Account aus:



3) der Benutzer liest den aktuellen Code aus:



4) der Benutzer gibt diesen Code ein, um die Anmeldung abzuschließen:



ALTO ADIGE PROVINCIA AUTONOMA DI BOLZANO  
AUTONOME PROVINZ BOZEN SÜDTIROL  
PROVINCIA AUTONOMA DE BULZAN  
SÜDTIROL

██████████@prov.bz

### Code eingeben

123 Geben Sie den Code ein, der in Ihrer Authenticator-App auf dem Gerät angezeigt wird.

Die nächsten 7 Tage nicht erneut fragen

Treten Probleme auf? [Auf andere Weise anmelden](#)

[Weitere Informationen](#)

**Überprüfen**