

Zuletzt geändert am 15. September 2021

Einrichtung eines zweiten Faktors für die Authentifizierung an Web-Anwendungen

Kurzanleitung

Verfasser: Peter Müntener, Dienst für Informatikplanung
Version: 1.0
Datum: 15. September 2021



Inhaltsübersicht

1	Ausgangslage	3
2	Anmeldung beim Zugriff auf die Web-Anwendung	4
3	Registrierung eines zweiten Faktors für die Authentifizierung	5
3.1	Authentifizierungsart: OTP (One-Time-Password, Einmalpasswort)	6
3.2	Authentifizierungsart: SMS	7
3.3	Authentifizierungsart: Anruf (Voice)	8
4	Wiederherstellen (Recover) der Einstellungen	9
5	FAQ	10



1 Ausgangslage

Es ist ein Sicherheitsrisiko, wenn Sie sich bei Web-Anwendungen, in denen Sie vertrauliche Daten hinterlassen nur mit Benutzername und Kennwort anmelden. Obwohl auch die Kombination aus Benutzername und Kennwort einen gewissen Schutz bietet, ist dieses Anmeldeverfahren sehr anfällig für Angriffe von Cyberkriminellen, da sie Ihre Zugangsdaten leicht ausspähen können.

Der beste Weg Ihren Zugang zu Web-Anwendungen abzusichern, ist der Einsatz der sogenannten Multi-Faktoren-Authentifizierung (MFA). Bei diesem Verfahren kommen zwei oder mehrere voneinander unabhängige Komponenten zur Identitätsfeststellung zum Einsatz. Sie kennen diese Art von Zugang seit vielen Jahren aus ihrem privaten E-Banking.

Sie wollen mit einem privaten oder öffentlichen Gerät aus dem Internet das Webmail, Sharepoint oder eine andere kantonale Web-Applikation nutzen?

In diesem Fall benötigen Sie wie beim E-Banking zur Authentifizierung einen zusätzlichen «zweiten Faktor». Das heisst, Sie bestätigen Ihre Identität, indem Sie ein Einmalpasswort in Form eines Zahlencodes erhalten und diesen bei der Anmeldung zusätzlich zum Passwort eingeben.

Diese Kurzanleitung dokumentiert die einzelnen Schritte bei der Registrierung des zweiten Faktors für die Authentifizierung an einer Web-Anwendung des Kantons. Beim erstmaligen Login nach der Aktivierung des Multi-Faktoren-Authentifizierung-Verfahrens durchlaufen Sie einen kurzen Registrierungsprozess. Sie können dabei die für Sie passende Authentifizierungsmethode auswählen. Der zusätzliche Faktor wird von Abraxas über die «SecureConnect Plattform» als Service bereitgestellt.



2 Anmeldung beim Zugriff auf die Web-Anwendung

Beim ersten Zugriff auf die Web-Anwendung werden Sie aufgefordert, einen zweiten Faktor für die Authentifizierung einzurichten. Bei der Verbindung mit Ihrer Web-Anwendung (Webmail, Sharepoint oder ähnlich) melden Sie sich wie gewohnt mit der Eingabe von **Domäne\Benutzername** und Ihrem **Passwort** an. Danach werden Sie zum Registrierungsprozess für die Multi-Faktoren-Authentifizierung weitergeleitet.

Vorgehen

Melden Sie sich mit **pu1\Ihr Benutzername** (im Beispiel: pu1\iah8780) und ihrem **Passwort** an. Es folgt der Hinweis zur MFA-Einrichtung.

Kanton St.Gallen

Mit vorhandenem Konto anmelden

pu1\iah8780

.....

Einloggen

[Passwort vergessen](#)

[Password ändern](#)

Mehr Sicherheit mit 2-Faktor-Authentifizierung

Die Applikation verlangt eine 2-Faktor-Authentifizierung. Richten Sie diese nun ein und verbessern sie damit zudem die Sicherheit Ihres Accounts.


Jetzt einrichten



3 Registrierung eines zweiten Faktors für die Authentifizierung

Bei der Registrierung des zweiten Faktors haben Sie die Wahl zwischen drei verschiedenen Authentifizierungsarten. Die Auswahl wird Ihnen selber überlassen und hängt von Ihren eigenen Möglichkeiten und Bedürfnissen ab.

DE



Authentifizierungsart
wählen

☐ OTP

☒ SMS

☐ Anruf

4 Weiter

Zurück

3.1 Einmalpasswort (One-Time-Password bzw. OTP)
Das Einmalpasswort mittels Zahlencode wird in einer sogenannten OTP-App angezeigt. In den jeweiligen App-Stores stehen Ihnen hierfür unterschiedliche Authentisierungs-Apps kostenlos zur Verfügung. Wir empfehlen für iOS und Android Smartphones oder Tablets den **Google Authenticator**, **Microsoft Authenticator** oder **Authy** zu installieren.

3.2 SMS (Short Message Service)
Das Einmalpasswort mittels Zahlencode wird per SMS an die von Ihnen registrierte, SMS-fähige Telefonnummer übermittelt.

3.3 Anruf (Voice)
Das Einmalpasswort mittels Zahlencode wird per Sprachanruf an die von Ihnen registrierte Telefonnummer (Mobile oder Festnetz) übermittelt.



3.1 Authentifizierungsart: OTP (One-Time-Password, Einmalpasswort)

Authentifizierungsart wählen

☒ OTP 3

☐ SMS

☐ Anruf

4 **Weiter**

Zurück

3. Wählen Sie **OTP** als Authentifizierungsart.

4. Klicken Sie auf **Weiter**.

OTP berechtigen

Scannen Sie den QR-Code mit einem Authentifizierungsprogramm (z.B. Google Authenticator) und geben Sie den generierten Code im Feld unten ein.

5

Code

242357 6

7 **Weiter**

Zurück

5. Scannen Sie den **QR-Code** mit Ihrer **Authentisierungs-App**.

6. Geben Sie den in der **App** angezeigten **OTP Code** ein.

7. Klicken Sie auf **Weiter**.

2-Faktor-Authentifizierung eingerichtet

Speichern Sie folgenden Schlüssel sicher ab, er wird Ihnen nicht erneut angezeigt. Er ist die einzige Möglichkeit, Ihre Einstellungen zurückzusetzen, falls Sie keinen Zugriff mehr auf Ihren 2. Faktor haben.

TH7Y-G64T-ENVX-7XZS 8

9 **Weiter**

8. **Speichern** Sie den angezeigten **Schlüssel** an einem **sicheren Ort**, wie z.B. in Ihrem **Passwortsafe**. Den Schlüssel benötigen Sie, um Ihre Einstellungen bei Bedarf zurückzusetzen.

9. Klicken Sie auf **Weiter**.

Zweifaktor Authentifizierung

Ein Verifizierungscode wurde versendet. Bitte geben Sie diesen hier ein. Sollten Sie den Code nicht erhalten haben, können Sie diesen erneut auslösen oder mit 'Wiederherstellen' ihre Einstellungen zurücksetzen.

OTP

187075 10

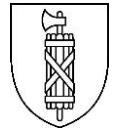
11 **verifizieren**

Code von anderem Provider anfordern

Recover

10. Geben Sie den in der **App** angezeigten **OTP Code** ein.

11. Klicken Sie auf **verifizieren**
Der zweite Faktor ist eingerichtet und wird bei der nächsten Anmeldung abgefragt.



3.2 Authentifizierungsart: SMS

Authentifizierungsart wählen

☐ OTP

☒ SMS **3**

☐ Anruf

4 Weiter

Zurück

- 3.** Wählen Sie **SMS** als Authentifizierungsart.
- 4.** Klicken Sie auf **Weiter**.

Authentifizierung über SMS

Geben Sie die Telefonnummer für SMS ein.

Telefonnummer **5**

+41798240828

6 Weiter

erneut senden

Zurück

- 5.** Erfassen Sie die SMS-fähige **Telefonnummer** auf der Sie den Code erhalten wollen.
- 6.** Klicken Sie auf **Weiter**.

Authentifizierung über SMS

Geben Sie bitte den Bestätigungscode ein.

Code **7**

493890

8 Weiter

erneut senden

Zurück

- 7.** Geben Sie den per **SMS** erhaltenen **Code** ein.
- 8.** Klicken Sie auf **Weiter**.

2-Faktor-Authentifizierung eingerichtet

Speichern Sie folgenden Schlüssel sicher ab, er wird Ihnen nicht erneut angezeigt. Er ist die einzige Möglichkeit, Ihre Einstellungen zurückzusetzen, falls Sie keinen Zugriff mehr auf Ihren 2. Faktor haben.

E4GM-E1LG-1AMX-0324 **9**

10 Weiter

- 9.** Speichern Sie den angezeigten **Schlüssel** an einem **sicheren Ort**, wie z.B. in Ihrem **Passwortsafe**. Den Schlüssel benötigen Sie, um Ihre Einstellungen bei Bedarf zurückzusetzen (Wiederherstellen, Recover).
- 10.** Klicken Sie auf **verifizieren**.

Der zweite Faktor ist eingerichtet und wird bei der nächsten Anmeldung abgefragt.



3.3 Authentifizierungsart: Anruf (Voice)

Authentifizierungsart wählen

☐ OTP

☐ SMS

☒ Anruf

4 Weiter

Zurück

3. Wählen Sie **Anruf** als Authentifizierungsart.

4. Klicken Sie auf **Weiter**.

Authentifizierung über Voice

Geben Sie die Telefonnummer für Voice ein.

Telefonnummer

+41796260931

5

6 Weiter

erneut senden

Zurück

5. Erfassen Sie die **Telefonnummer** (Mobile oder Festnetz), auf der Sie angerufen werden wollen.

6. Klicken Sie auf **Weiter**.

Authentifizierung über Voice

Geben Sie bitte den Bestätigungscode ein.

Code

274332

7

8 Weiter

erneut senden

Zurück

7. Sie erhalten einen **Sprachanruf** per ausländischer Nummer. Geben Sie den per **Sprache** übermittelten **Code** ein.

8. Klicken Sie auf **Weiter**.

2-Faktor-Authentifizierung eingerichtet

Speichern Sie folgenden Schlüssel sicher ab, er wird Ihnen nicht erneut angezeigt. Er ist die einzige Möglichkeit, Ihre Einstellungen zurückzusetzen, falls Sie keinen Zugriff mehr auf Ihren 2. Faktor haben.

TH7Y-G64T-ENVX-7XZS

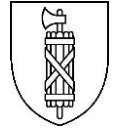
9

10 Weiter

9. Speichern Sie den angezeigten **Schlüssel** an einem **sicheren Ort**, wie z.B. in Ihrem **Passwortsafe**. Den Schlüssel benötigen Sie, um Ihre Einstellungen bei Bedarf zurückzusetzen. (Wiederherstellen, Recover).

10. Klicken Sie auf **verifizieren**.

Der zweite Faktor ist eingerichtet und wird bei der nächsten Anmeldung abgefragt.



4 Wiederherstellen (Recover) der Einstellungen

Falls Sie Ihre bisherige Authentifizierungsart ändern wollen, Ihre Rufnummer sich geändert hat oder das für die Authentifizierung genutzte Gerät ersetzt wurde, können Sie die Einstellungen über Wiederherstellen bzw. Recover zurücksetzen. Dazu benötigen Sie den Schlüssel, den Sie bei der Registrierung erhalten haben. Es ist daher wichtig, dass Sie diesen an einem sicheren Ort aufbewahren. Nun werden Sie erneut durch den initialen Registrierungsprozess geleitet.

Bitte kontaktieren Sie den Abraxas Servicedesk, falls Sie den Schlüssel für die Wiederherstellung nicht mehr im Zugriff haben oder Sie die Einstellungen nicht mehr selbständig zurücksetzen können.

Zweifaktor Authentifizierung

Ein Verifizierungscode wurde versendet. Bitte geben Sie diesen hier ein. Sollten Sie den Code nicht erhalten haben, können Sie diesen erneut auslösen oder mit 'Wiederherstellen' ihre Einstellungen zurücksetzen.

OTP
Code

verifizieren

Code von anderem Provider anfordern

Recover

1. Klicken Sie auf **Recover (Wiederherstellen)**.

Zweifaktor Authentifizierung

Beim Aufsetzen des Zweiten-Faktors haben sie einen RecoveryCode erhalten. Bitte geben Sie diesen hier ein.

Recover
12312312313123

verifizieren

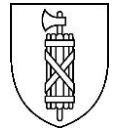
Code von anderem Provider anfordern

OTP

2. Geben Sie den **Schlüssel** ein, den Sie bei der Registrierung erhalten haben.

3. Klicken Sie auf **verifizieren**.

Bei der nächsten Anmeldung werden Sie erneut durch den Registrierungsprozess geführt.



5 FAQ

5.1 Wie kann ich meine persönlichen Einstellungen anpassen?

MyAccount (Intern direkt über den APZ Login, Extern mit MFA Anmeldung)

https://accounts.abraxas.ch/authorize?client_id=MA&response_type=code&redirect_uri=https://portal.abraxas.ch/myaccount&scope=openid%20profile%20urn:abraxas:iam:hosted_domain:sg-adfs

Folgen Sie dabei: Einstellungen -> Authentifizierung -> Zwei Faktor Authentifizierung.

5.2 Wer kann mir helfen, wenn ich meinen Schlüssel zur Wiederherstellung nicht mehr habe und auch nicht auf die MyAccount Seite zugreifen kann?

Kontaktieren Sie den Abraxas Servicedesk, Telefon: 058 660 00 10, E-Mail: servicedesk@abraxas.ch und lassen Sie ihre Einstellungen zurücksetzen.

5.3 Wen kontaktiere ich, wenn die Registrierung oder die Anmeldung mit dem zweiten Faktor fehlschlägt?

Kontaktieren Sie den Abraxas Servicedesk, Telefon: 058 660 00 10, E-Mail: servicedesk@abraxas.ch.

5.4 Wo finde ich diese Kurzanleitung in elektronischer Form?

Diese Anleitung ist Intranet unter <https://intranet.sg.ch/informatik/Seiten/Home-Office-Anleitungen.aspx> und bei den KOM SG Anleitungen unter <https://komsg.ch/mail> abgelegt.