

## Installation von Softzertifikaten / Einrichtung von 2-Faktor-Authentifizierung

---

### Inhaltsverzeichnis

1. Informationen zu Ihrem Softzertifikat .....	2
1.1 Laufzeit des Zertifikates .....	2
1.2 Aufbewahrung des Softzertifikates .....	2
1.3 Verwendung des Softzertifikates auf mehreren, unterschiedlichen Systemen .....	2
1.4 Installation von Softzertifikaten .....	2
2. Installation des Softzertifikates .....	3
2.1 Installation von Softzertifikaten unter Windows (Chrome und Microsoft Edge) .....	3
2.2 Installation von Softzertifikaten unter Windows (Firefox) .....	6
2.3 Installation von Softzertifikaten unter MAC OS X (Safari) .....	8
2.4 Installationsvarianten von Softzertifikaten unter einem iPad / iPhone (Safari-Browser) .....	10
2.5 Installation von Softzertifikaten unter Android-Geräten .....	16
3. 2-Faktor-Authentifizierung (Fido) für mobile Endgeräte .....	17
3.1 2-Faktor-Authentifizierung/Registrierung iPhone / iPad .....	17
3.2 2-Faktor-Authentifizierung/Registrierung Android-Geräten .....	19
3.3 2-Faktor-Authentifizierung Windows Hello-Fingerabdruck Einrichtung .....	21
3.4 2-Faktor-Authentifizierung Einrichtung Fido-Stick .....	25

## Installation von Softzertifikaten / Einrichtung von 2-Faktor-Authentifizierung

---

### 1. Informationen zu Ihrem Softzertifikat

Das Softzertifikat wird für die Authentifizierung und Anmeldung im PVSconnect Portal benötigt.

#### 1.1 Laufzeit des Zertifikates

Das Softzertifikat ist ab dem Ausstellungsdatum **5 Jahre gültig**. Nach dieser Laufzeit erhalten Sie von uns ein Folgezertifikat, welches ab Ausstellungsdatum wieder 5 Jahre gültig ist. Dieses muss auf Ihrem System erneut installiert werden.

#### 1.2 Aufbewahrung des Softzertifikates

Sie haben von uns eine E-Mail mit einem Zertifikatsanhang erhalten (Dateiendung.p12). **Bitte speichern Sie diese Datei auf Ihrem Computer an einem Ort ab, den Sie leicht wiederfinden.**

Zusätzlich speichern Sie das Zertifikat aus dem **E-Mail-Anhang** bitte als Sicherheitskopie auf einem USB-Stick, auf einer CD, oder auf einem sonstigen externen Datenträger und bewahren diesen an einem sicheren und geheimen Ort auf. Wenn das Betriebssystem auf Ihrem Computer einmal neu installiert wird oder Sie einen neuen Computer verwenden, können Sie das Zertifikat von dem externen Datenträger erneut verwenden.

Unter anderem haben Sie von uns ein Installationspasswort für Ihr persönliches Zertifikat auf postalischem Wege erhalten. Bitte legen Sie diesen Brief ebenfalls zu Ihren Akten und bewahren Sie diesen an einem sicheren und geheimen Ort auf.

#### 1.3 Verwendung des Softzertifikates auf mehreren, unterschiedlichen Systemen

Sie können das Zertifikat auf beliebig vielen Systemen installieren und damit unser Online-Portal PVSconnect aufrufen. Wichtig hierbei ist nur, dass die unterschiedlichen Computer internetfähig sind.

#### 1.4 Installation von Softzertifikaten

Sie haben die E-Mail mit dem Zertifikatsanhang erhalten und müssen diese im ersten Schritt herunterladen und abspeichern. Die Details zum Herunterladen der Datei hängen von dem Programm und Betriebssystem ab, mit dem Sie auf Ihre E-Mails zugreifen. Sie können die Zertifikatsdatei nach dem Download an einem beliebigen Platz abspeichern (z.B. Desktop).

## Installation von Softzertifikaten / Einrichtung von 2-Faktor-Authentifizierung

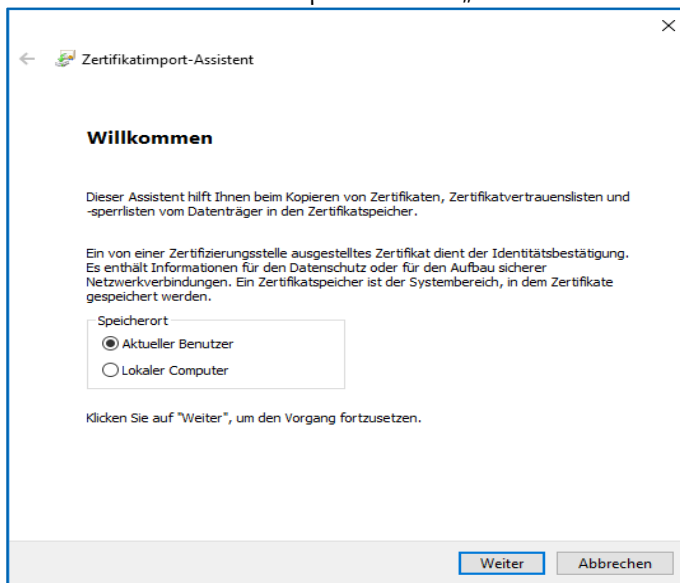
### 2. Installation des Softzertifikates

#### 2.1 Installation von Softzertifikaten unter Windows (Chrome und Microsoft Edge)

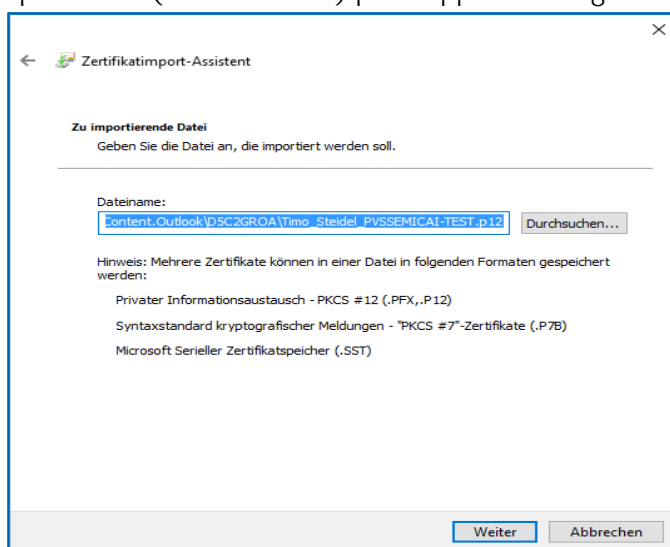
Diese Browser nutzen den Zertifikatsspeicher des Windows-Betriebssystems.

Um Ihr Zertifikat dort zu installieren, führen Sie folgende Schritte durch:

- Das per E-Mail erhaltene Zertifikat auf dem PC speichern (Desktop, Eigene Dateien, o.ä.)
- Zertifikat vom Speicherort mit Doppelklick öffnen und somit den Zertifikatimport-Assistent von Windows öffnen. Den Import für den „aktuellen Benutzer“ starten

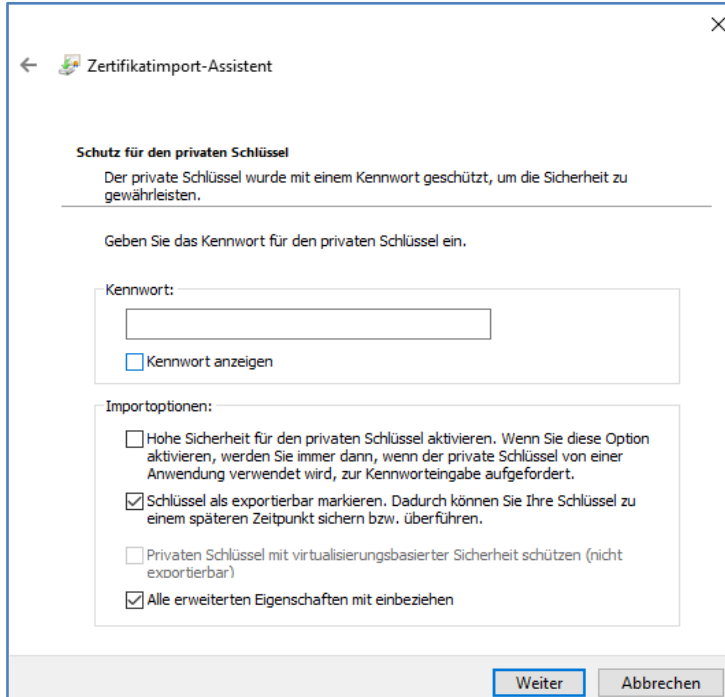



- Ggf. richtige Datei auswählen (dies ist grundsätzlich nicht erforderlich, wenn die Datei von Ihrem Speicherort (siehe Schritt 1) per Doppelklick aufgerufen wurde. Mit „Weiter“ fortführen



## Installation von Softzertifikaten / Einrichtung von 2-Faktor-Authentifizierung

- Den per Brief erhaltenen „privaten Schlüssel“ (Installationspasswort) in das Feld Kennwort eintragen. Außerdem die Option „Schlüssel als exportierbar markieren“ per Checkbox aktivieren



←  Zertifikatimport-Assistent

**Schutz für den privaten Schlüssel**  
Der private Schlüssel wurde mit einem Kennwort geschützt, um die Sicherheit zu gewährleisten.

Geben Sie das Kennwort für den privaten Schlüssel ein.

Kennwort:

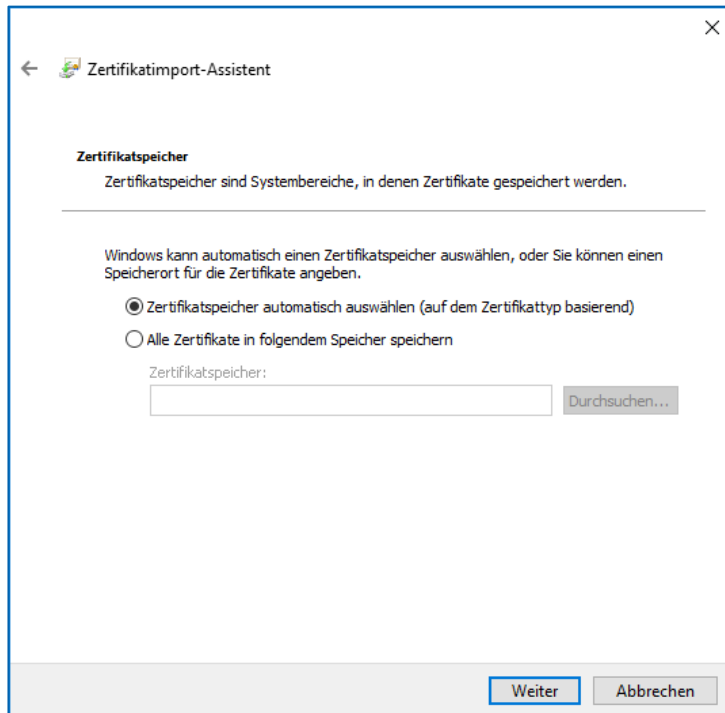
☐ Kennwort anzeigen


Importoptionen:

- ☐ Hohe Sicherheit für den privaten Schlüssel aktivieren. Wenn Sie diese Option aktivieren, werden Sie immer dann, wenn der private Schlüssel von einer Anwendung verwendet wird, zur Kennworteingabe aufgefordert.
- ☒ Schlüssel als exportierbar markieren. Dadurch können Sie Ihre Schlüssel zu einem späteren Zeitpunkt sichern bzw. überführen.
- ☐ Privaten Schlüssel mit virtualisierungsbasierter Sicherheit schützen (nicht exportierbar)
- ☒ Alle erweiterten Eigenschaften mit einbeziehen

Weiter Abbrechen

- Option „Zertifikatsspeicher automatisch wählen“ aktivieren und mit „Weiter“ bestätigen



←  Zertifikatimport-Assistent

**Zertifikatsspeicher**  
Zertifikatsspeicher sind Systembereiche, in denen Zertifikate gespeichert werden.

Windows kann automatisch einen Zertifikatsspeicher auswählen, oder Sie können einen Speicherort für die Zertifikate angeben.

☒ Zertifikatsspeicher automatisch auswählen (auf dem Zertifikattyp basierend)  
☐ Alle Zertifikate in folgendem Speicher speichern

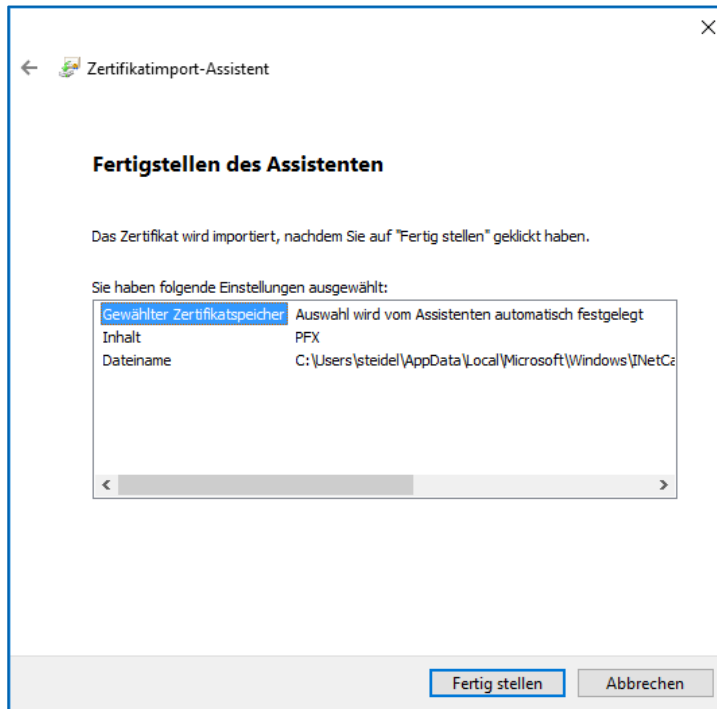
Zertifikatsspeicher:

Durchsuchen...

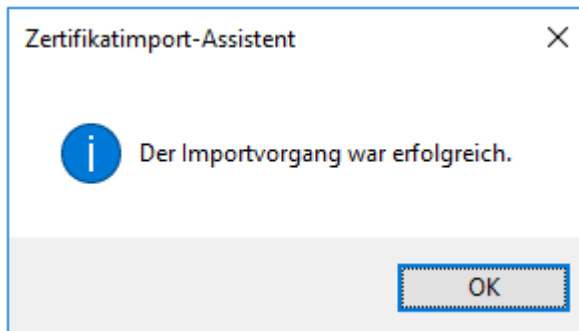
Weiter Abbrechen

## Installation von Softzertifikaten / Einrichtung von 2-Faktor-Authentifizierung

- Zertifikatimport-Assistent über „Fertig stellen“ abschließen



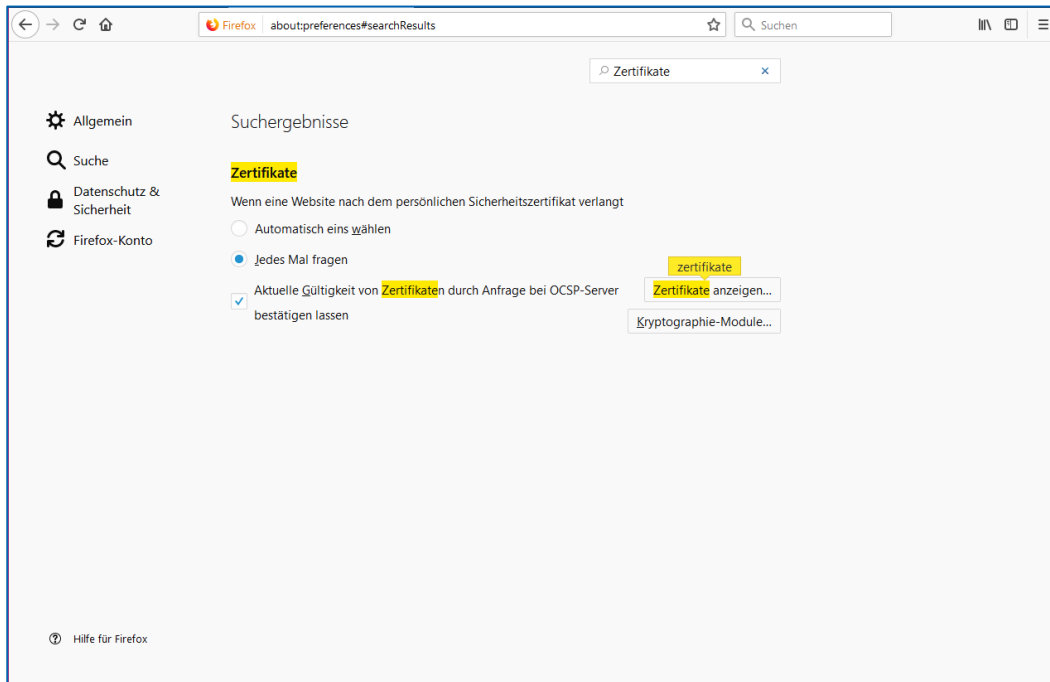
- Sie erhalten eine Erfolgsmeldung, dass der Importvorgang erfolgreich abgeschlossen wurde
- Nun ist die Zertifikatsinstallation abgeschlossen. Über die Webseite <https://connect.pvs-se.de> können Sie sich mit den per E-Mail erhaltenen Zugangsdaten anmelden



## Installation von Softzertifikaten / Einrichtung von 2-Faktor-Authentifizierung

### 2.2 Installation von Softzertifikaten unter Windows (Firefox)

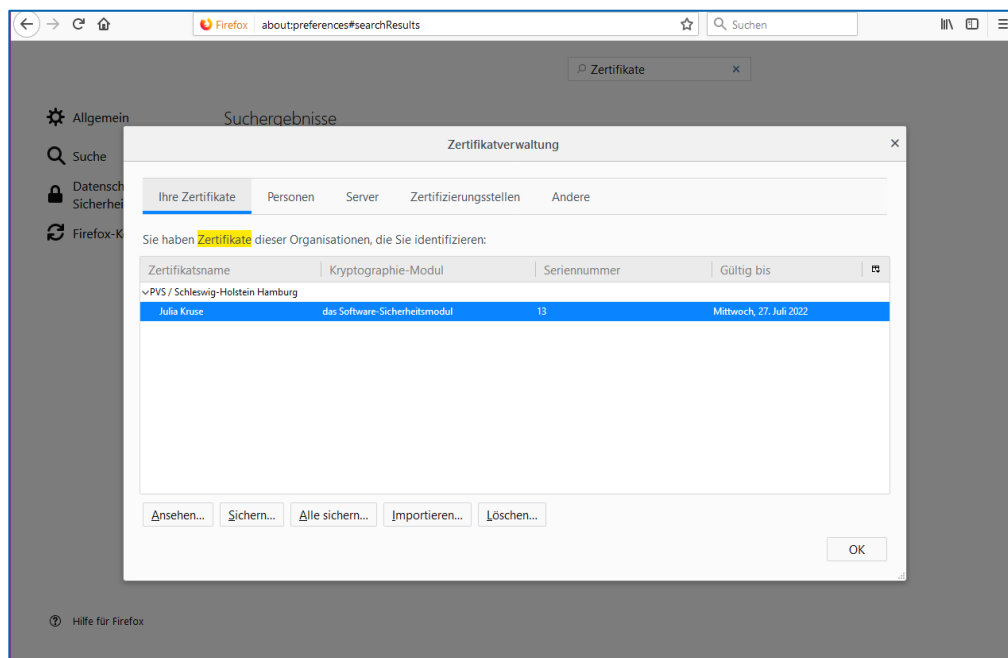
- Das per E-Mail erhaltene Zertifikat auf dem PC speichern (Desktop, Eigene Dateien, o.ä.)
- Den Firefox Browser öffnen
- Klicken Sie oben rechts auf das Anwendungsmenü und wählen Sie die Einstellungen aus
- In der Suchleiste der Einstellungen „Zertifikate“ eintragen



- Zertifikate anzeigen

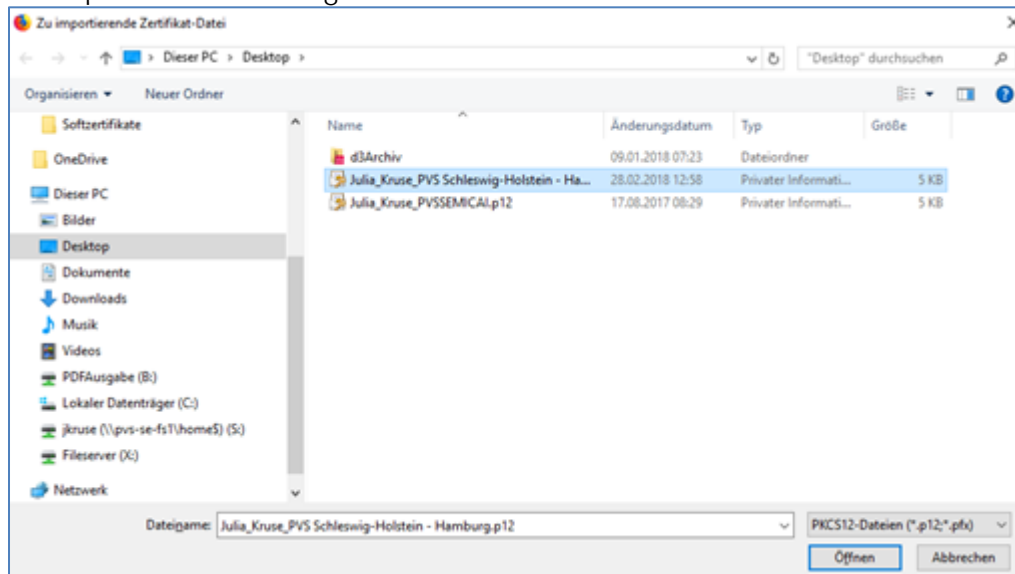


- Wählen Sie in der Zertifikatsverwaltung den Reiter „Ihre Zertifikate“ aus und klicken auf die Schaltfläche „Importieren“

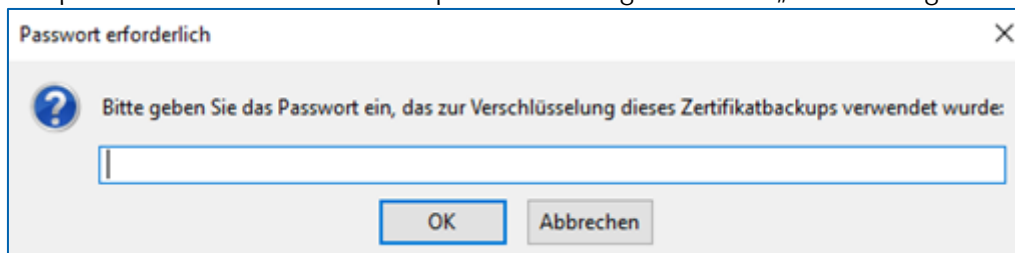


## Installation von Softzertifikaten / Einrichtung von 2-Faktor-Authentifizierung

- Vom Speicherort das richtige Zertifikat auswählen und Öffnen



- Das per Brief erhaltene Installationspasswort eintragen und mit „OK“ bestätigen



- Nun ist die Zertifikatsinstallation abgeschlossen. Über die Webseite <https://connect.pvs-se.de> können Sie sich mit den per E-Mail erhaltenen Zugangsdaten anmelden

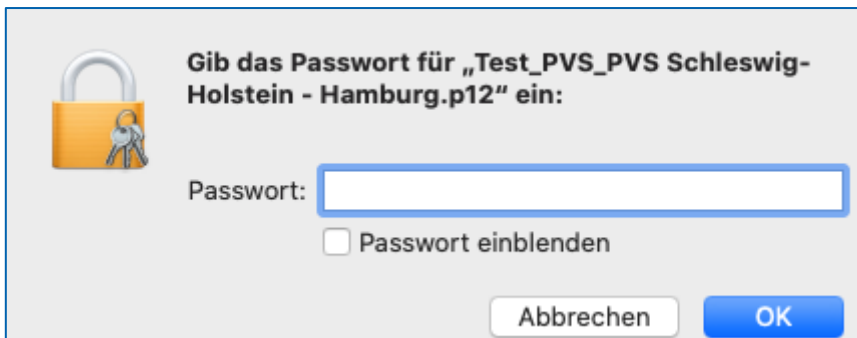
## Installation von Softzertifikaten / Einrichtung von 2-Faktor-Authentifizierung

### 2.3 Installation von Softzertifikaten unter MAC OS X (Safari)

- Das per E-Mail erhaltene Zertifikat auf dem PC speichern (Schreibtisch, Dateien o.ä.)
- Zertifikat vom Speicherort mit Doppelklick öffnen. Es erscheint eine Nachfrage, ob das Zertifikat in die Schlüsselbundverwaltung übernommen werden soll. Wählen Sie den Button „Hinzufügen“ aus



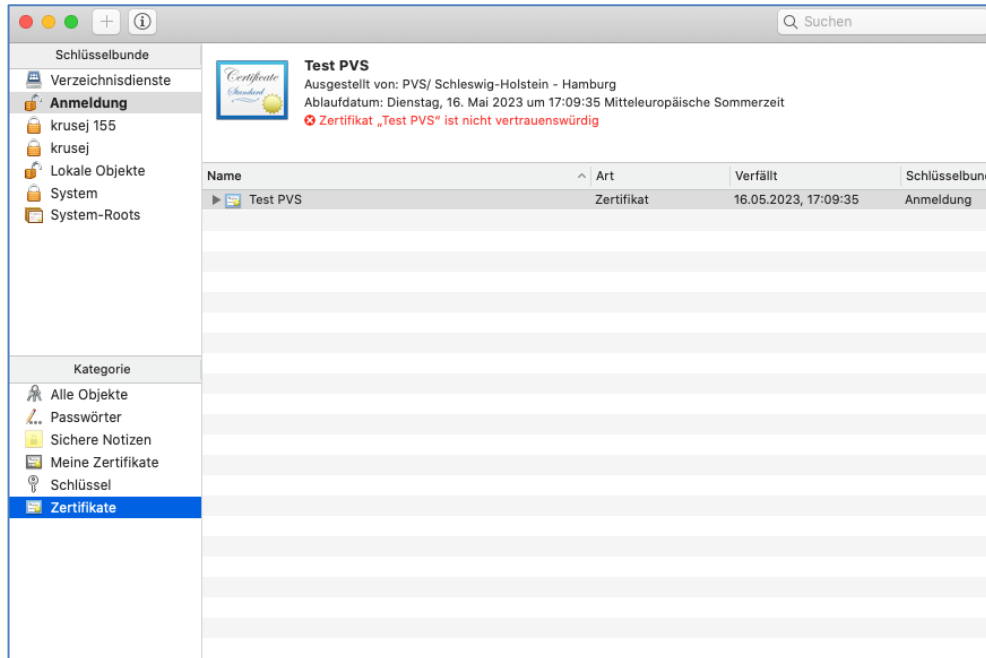
- Das per Brief erhaltene Installationspasswort in das Feld „Passwort“ eintragen und im Anschluss mit „OK“ bestätigen



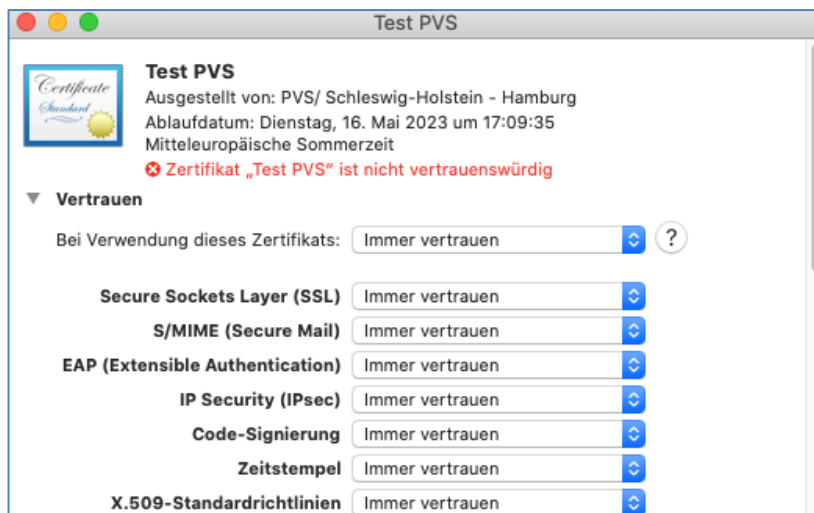


## Installation von Softzertifikaten / Einrichtung von 2-Faktor-Authentifizierung

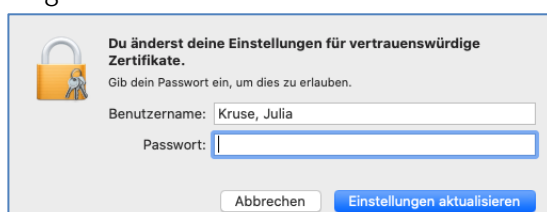
- Öffnen Sie Ihre Schlüsselbundverwaltung auf Ihrem System
- Klicken Sie in der Schlüsselbundverwaltung auf „Zertifikate“ und wählen Sie Ihr persönliches Zertifikat mit Doppelklick aus



- Klicken Sie auf den Menüpunkt „Vertrauen“. In der Zeile „Bei Verwendung dieses Zertifikats“ setzen Sie die Schaltfläche auf „Immer vertrauen“ und schließen das Fenster



- Tragen Sie das Passwort der Schlüsselbundverwaltung ein, um die Einstellungen zu aktualisieren



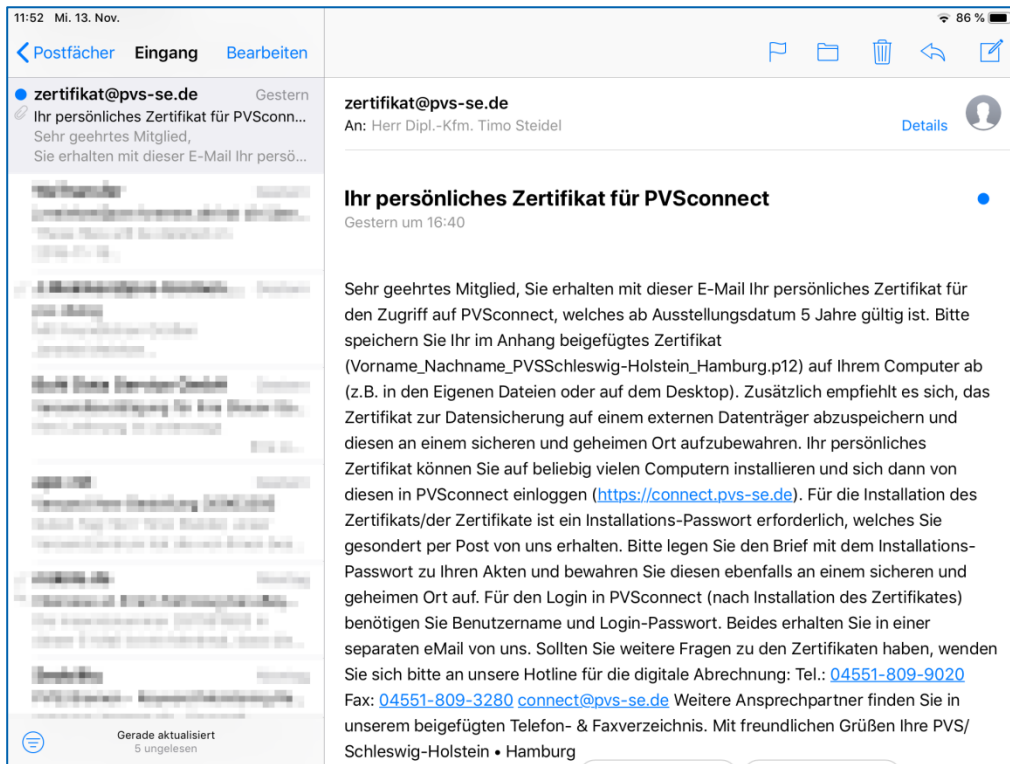
- Nun ist die Zertifikatsinstallation abgeschlossen. Über die Webseite <https://connect.pvs-se.de> können Sie sich mit den per E-Mail erhaltenen Zugangsdaten anmelden

## Installation von Softzertifikaten / Einrichtung von 2-Faktor-Authentifizierung

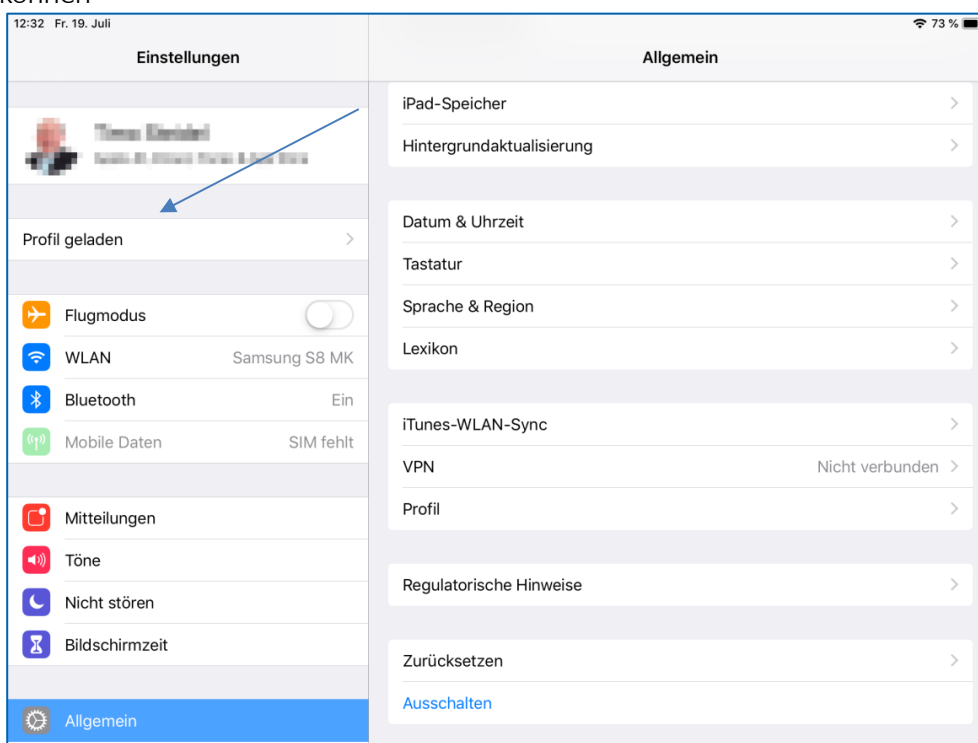
### 2.4 Installationsvarianten von Softzertifikaten unter einem iPad / iPhone (Safari-Browser)

#### Variante 1:

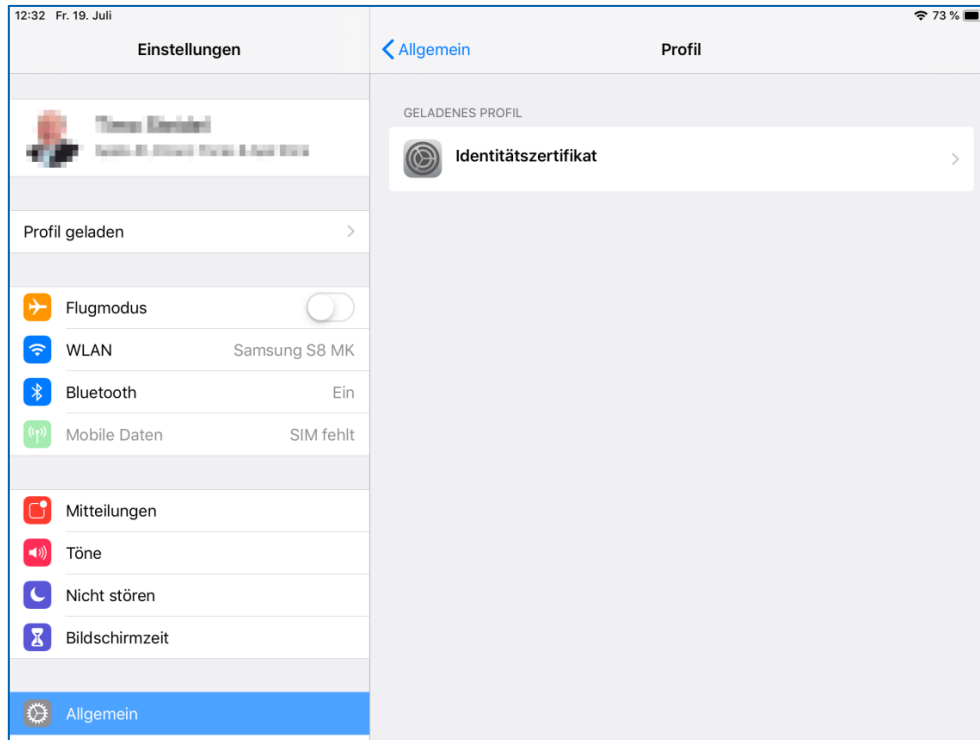
- Klicken Sie das PVScconnect Softzertifikat aus der E-Mail an und schließen Sie die u.g. Meldung



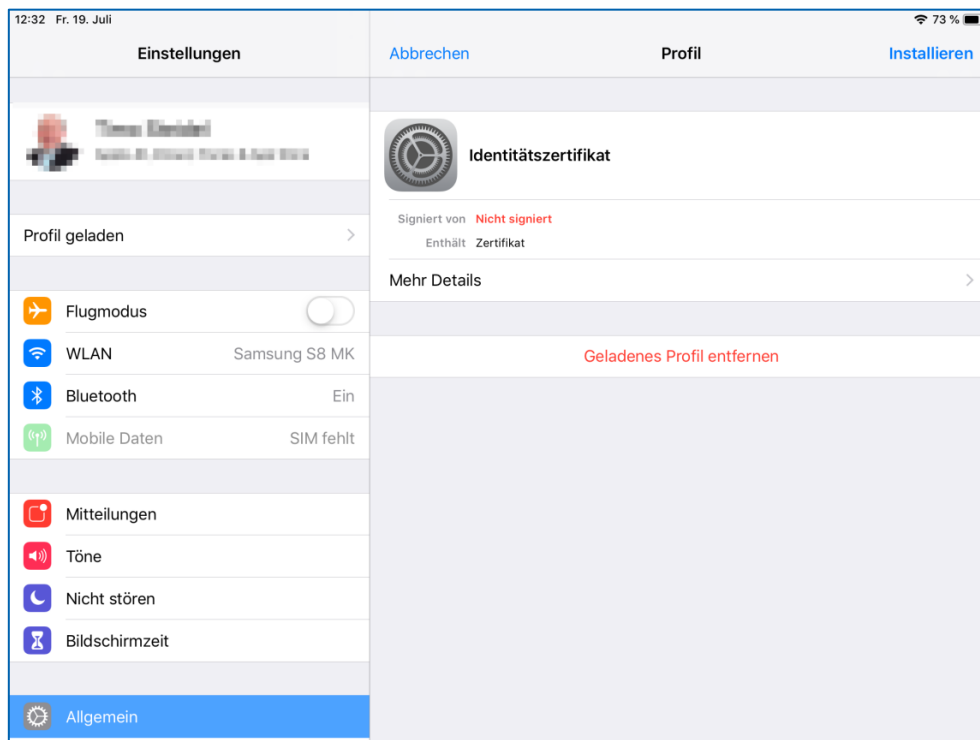
- Öffnen Sie die Einstellungen und klicken auf das „Profil geladen“, um das Zertifikat installieren zu können



- Öffnen Sie das Identitätszertifikat

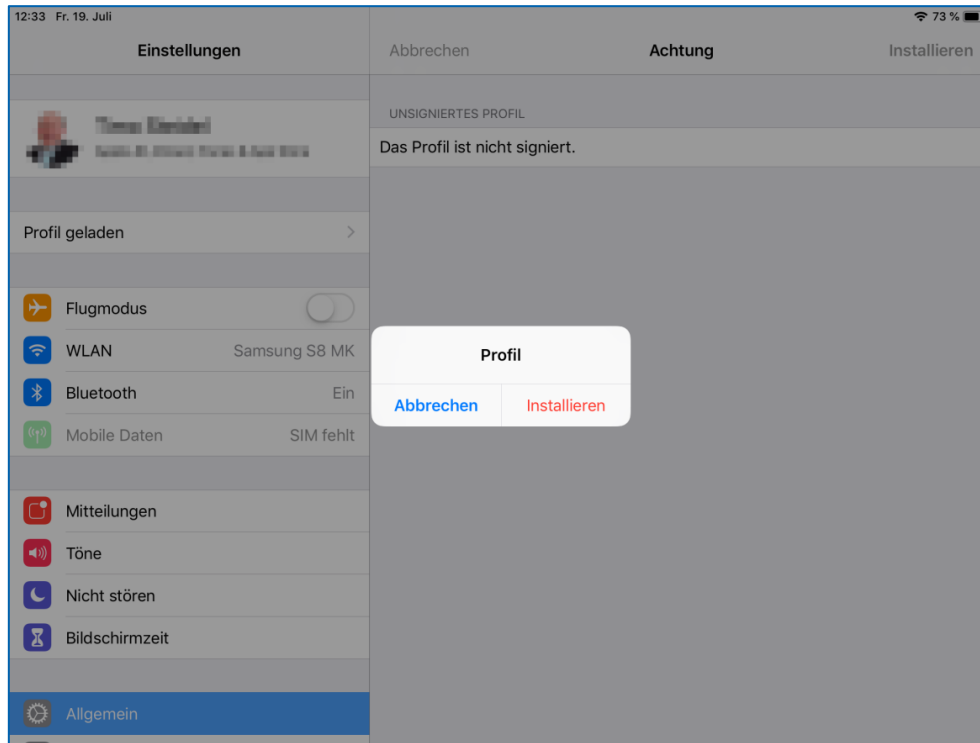


- Klicken Sie oben rechts auf „Installieren“

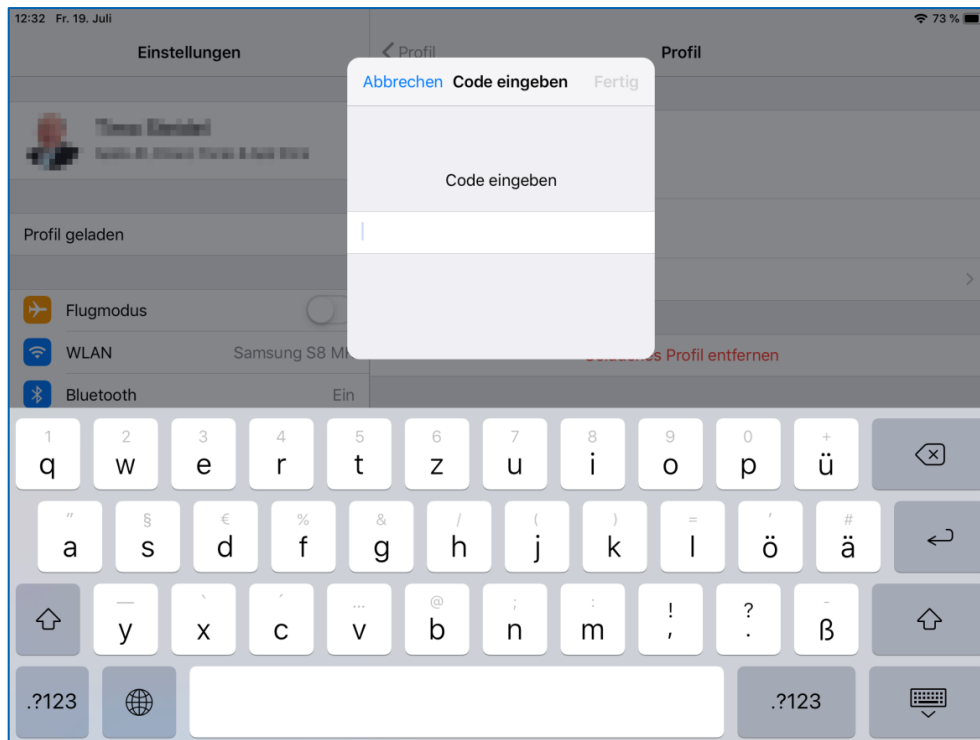


## Installation von Softzertifikaten / Einrichtung von 2-Faktor-Authentifizierung

- Es öffnet sich ein weiteres Fenster, bei dem Sie die den Vorgang abbrechen oder die Installation fortführen können

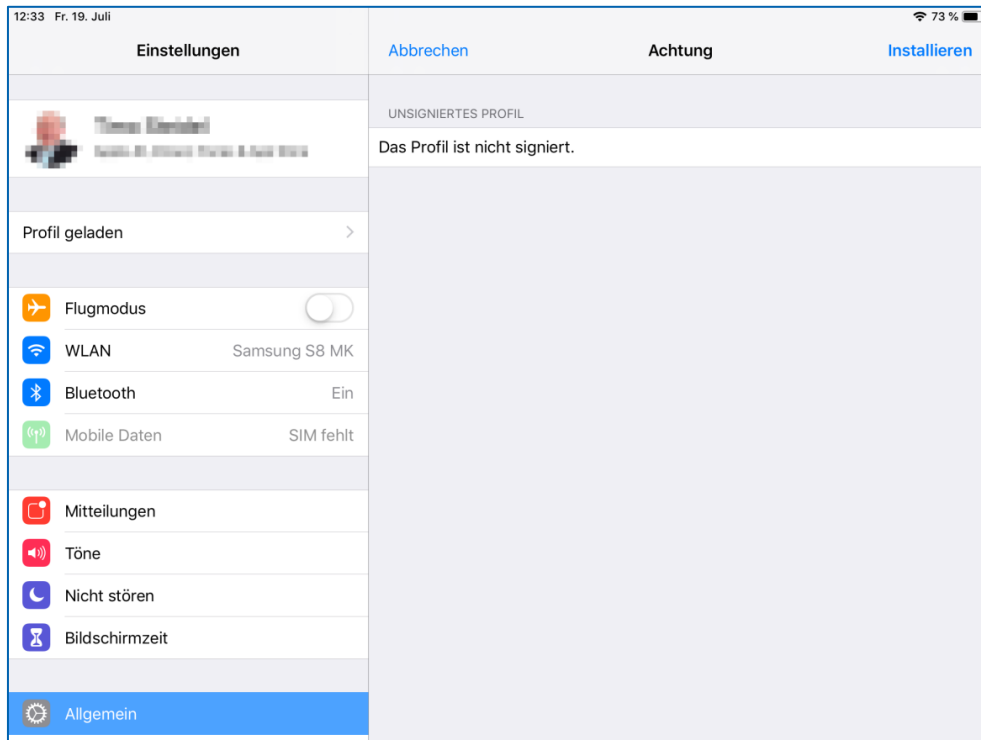


- Geben Sie den Sperrcode Ihres iPad / iPhone ein

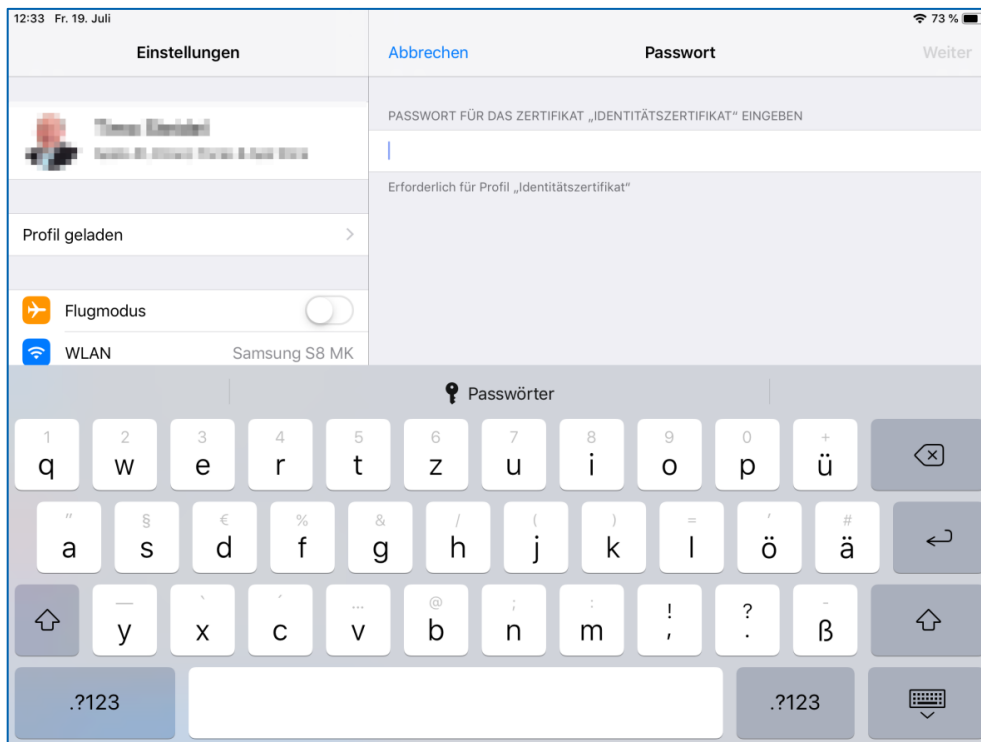


## Installation von Softzertifikaten / Einrichtung von 2-Faktor-Authentifizierung

- Klicken Sie ein weiteres Mal oben rechts auf „Installieren“



- Tragen Sie das per Brief erhaltene Installationspasswort in das Feld „Passwort für das Zertifikat“ ein und klicken Sie auf „Weiter“

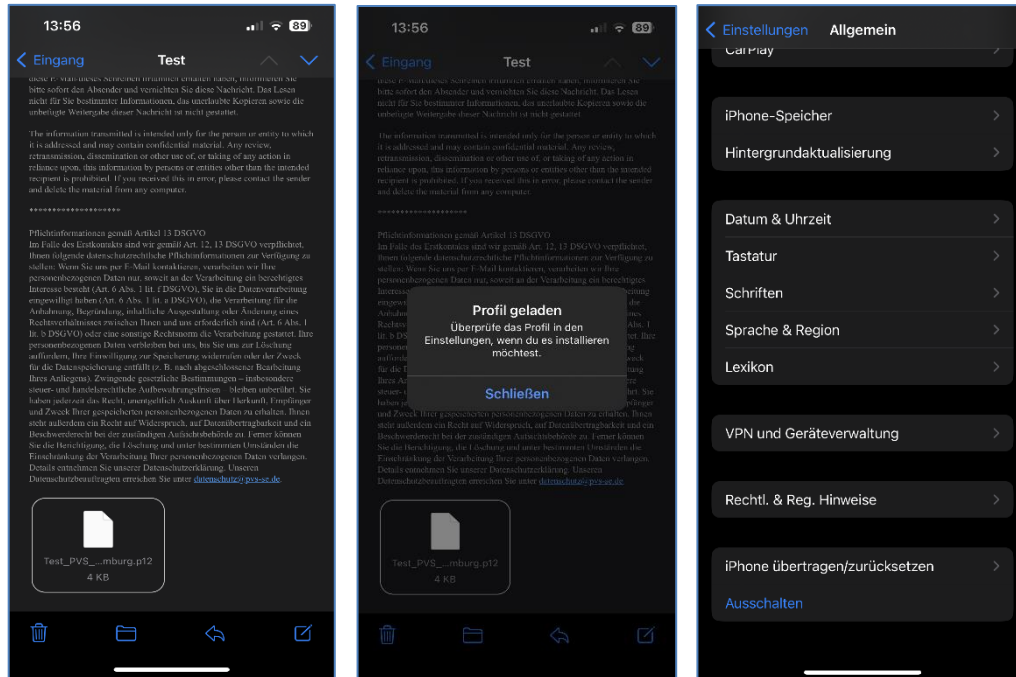


- Nun ist die Zertifikatsinstallation abgeschlossen. Über die Webseite <https://connect.pvs-se.de> können Sie sich mit den per E-Mail erhaltenen Zugangsdaten anmelden

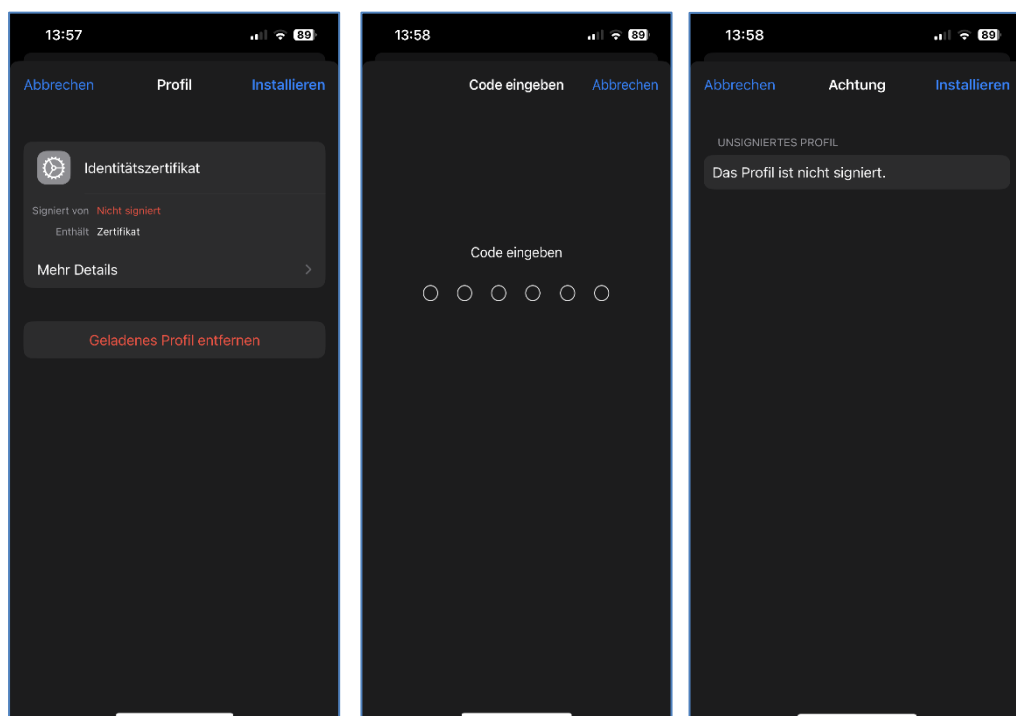
## Installation von Softzertifikaten / Einrichtung von 2-Faktor-Authentifizierung

### Variante 2:

- Klicken Sie das PVSconnect Softzertifikat aus der E-Mail an und schließen Sie die u.g. Meldung
- Öffnen Sie die Einstellungen und wählen die Schaltfläche „Allgemein“ -> „VPN und Geräteverwaltung“ um das Zertifikat installieren zu können

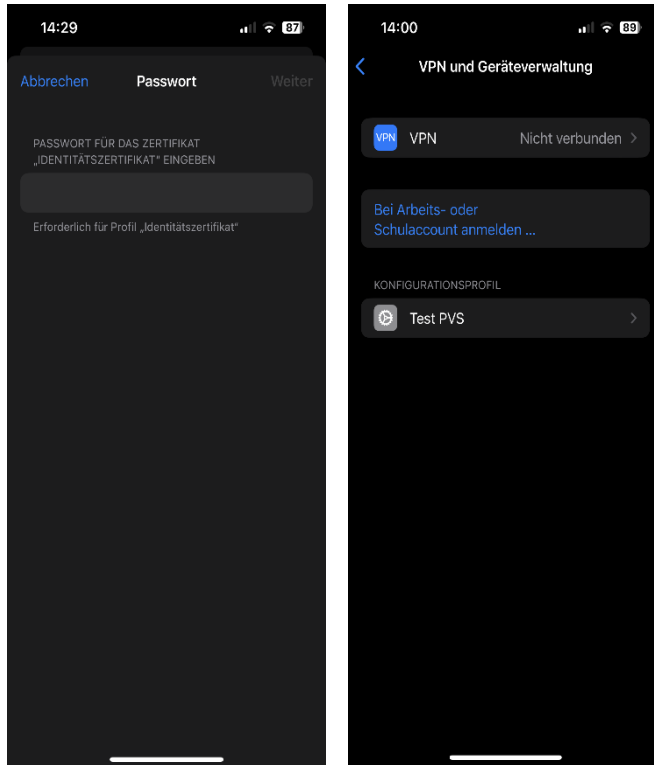


- Klicken Sie auf „Geladenes Profil“ -> „Identitätszertifikat“
- Klicken Sie oben rechts auf „Installieren“. Geben Sie den Sperrcode Ihres iPad / iPhone ein und klicken erneut oben rechts auf „Installieren“



## Installation von Softzertifikaten / Einrichtung von 2-Faktor-Authentifizierung

- Tragen Sie das per Brief erhaltene Installationspasswort in das Feld „Passwort für das Zertifikat“ ein und klicken auf „Weiter“

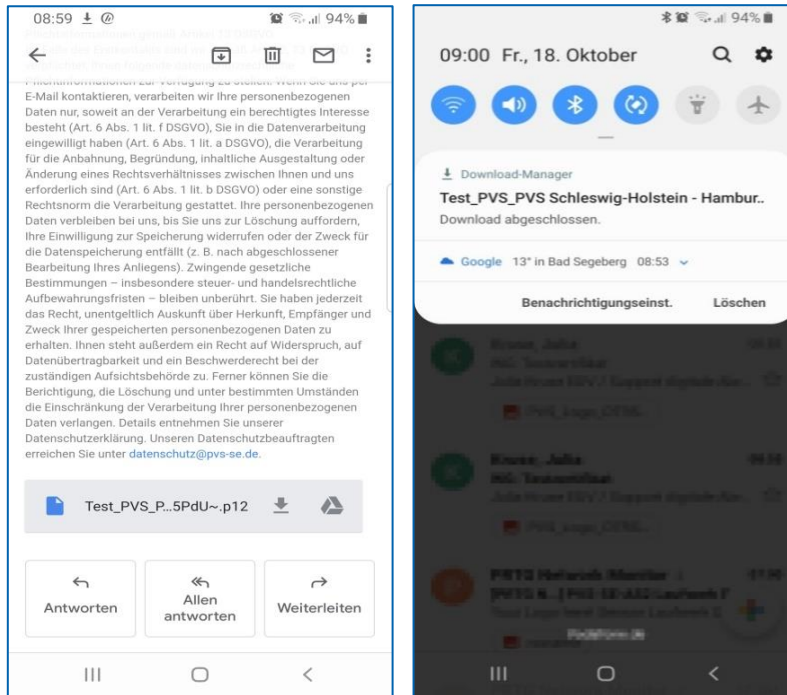


- Nun ist die Zertifikatsinstallation abgeschlossen. Über die Webseite <https://connect.pvs-se.de> können Sie sich mit den per E-Mail erhaltenen Zugangsdaten anmelden

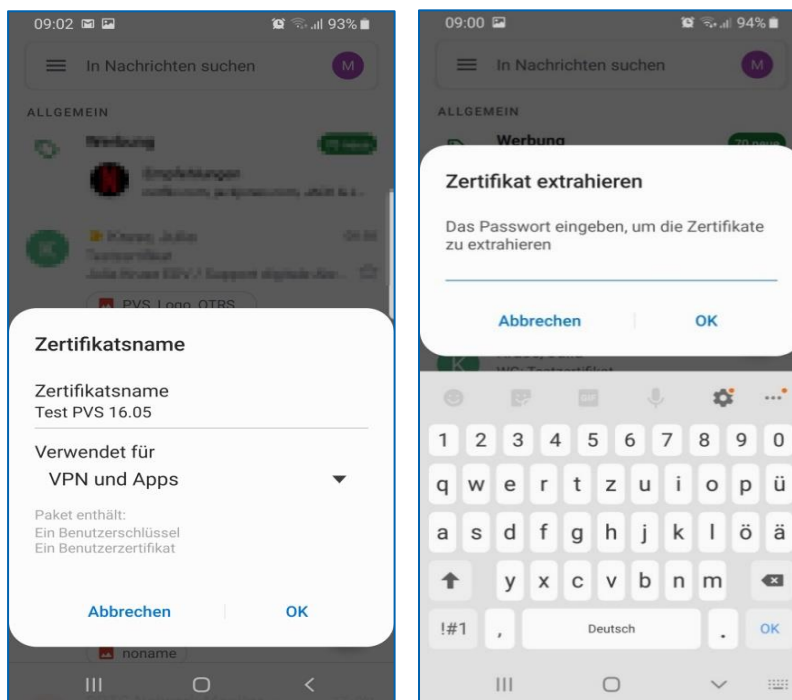
## Installation von Softzertifikaten / Einrichtung von 2-Faktor-Authentifizierung

### 2.5 Installation von Softzertifikaten unter Android-Geräten

- Klicken Sie das PVSconnect Softzertifikat aus der E-Mail an und laden es mit dem hinterlegten Downloadbutton herunter. Sie erhalten eine Info, sobald das Zertifikat heruntergeladen wurde



- Bestätigen Sie mit „OK“, dass Sie das Zertifikat extrahieren möchten und tragen Sie das per Brief erhaltene Installations-Passwort in das Feld ein. Bestätigen Sie das Passwort ein weiteres Mal mit „OK“
- Sobald das Zertifikat installiert wurde, erhalten Sie eine Bestätigung über die erfolgreiche Installation



- Nun ist die Zertifikatsinstallation abgeschlossen. Über die Webseite <https://connect.pvs-se.de> können Sie sich mit den per E-Mail erhaltenen Zugangsdaten anmelden



## Installation von Softzertifikaten / Einrichtung von 2-Faktor-Authentifizierung

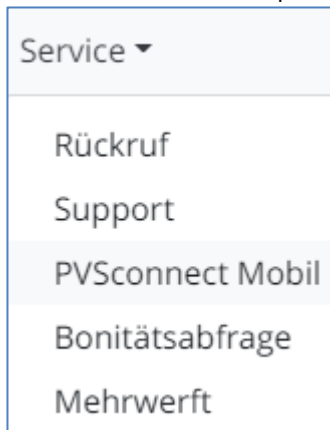
### 3. 2-Faktor-Authentifizierung (Fido) für mobile Endgeräte

Mit der 2-Faktor Authentifizierung (Fido) haben Sie die Möglichkeit weitere mobile Endgeräte wie z.B. Smartphone, Tablet, Fido Stick, weitere PCs (mit Windows Hello, Fingerabdruck) zu registrieren ohne eine separate Zertifikatsinstallation vorzunehmen.

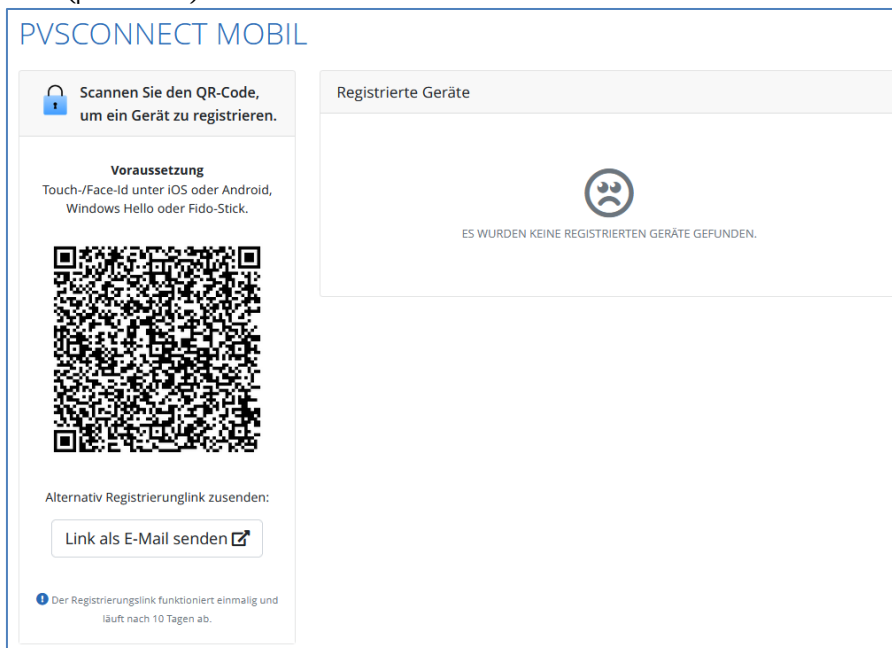
Das von uns versendete Zertifikat wird nur auf einem PC benötigt, alle weiteren Geräte können mit Fido registriert werden.

#### 3.1 2-Faktor-Authentifizierung/Registrierung iPhone / iPad

- Melden Sie sich mit Ihren PVSconnect Zugangsdaten bei PVSconnect auf einem PC an, bei dem das Zertifikat bereits installiert wurde
- Wählen Sie den Menüpunkt Service aus und klicken auf „PVSconnect Mobil“

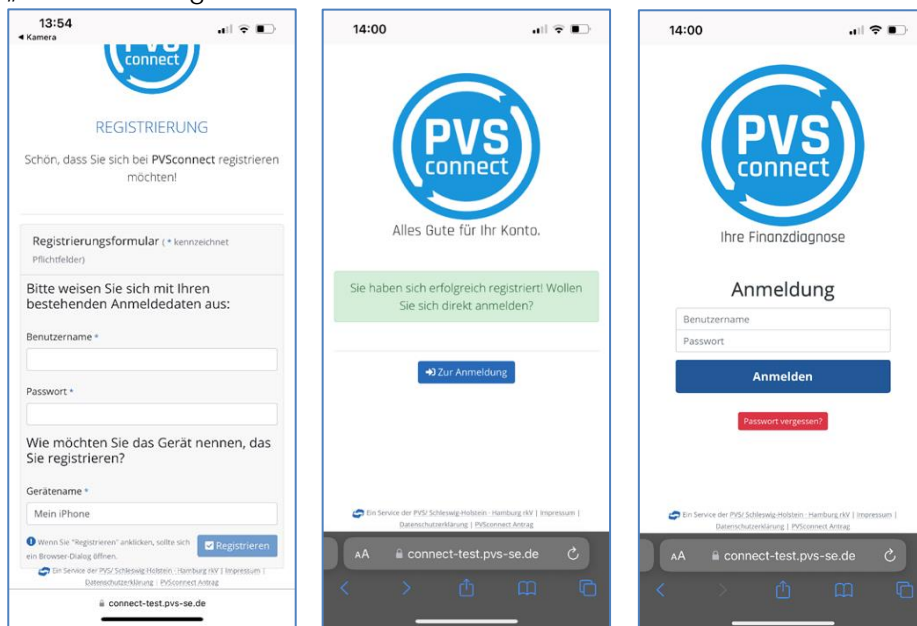


- Scannen Sie den QR-Code mit Hilfe Ihrer Kamera oder einem Barcode Scanner ab und öffnen den Link (pvs-se.de)

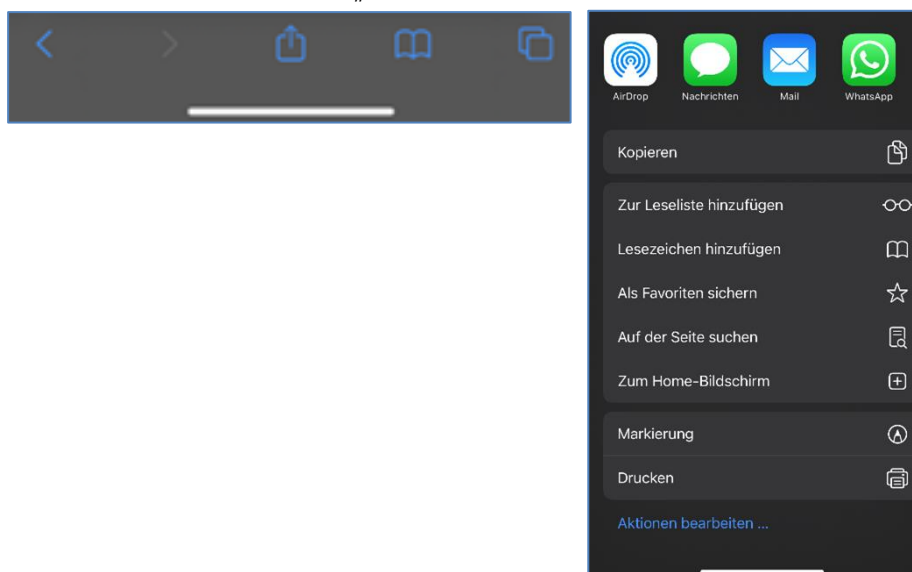


## Installation von Softzertifikaten / Einrichtung von 2-Faktor-Authentifizierung

- Auf der Registrierungswebseite weisen Sie sich mit Ihren PVSconnect Zugangsdaten aus und tragen einen Gerätenamen ein
- Klicken Sie auf „Registrieren“
- Ihr Gerät fragt an, ob die Webseite Ihre Face/Touch ID verwenden darf. Klicken Sie hier auf „Fortfahren“. Sie erhalten die Info, dass Sie sich erfolgreich registriert haben. Klicken Sie auf den Button „zur Anmeldung“



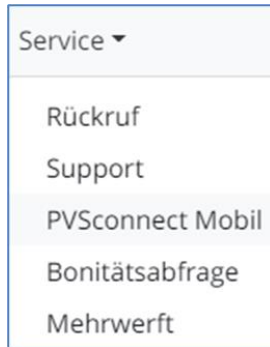
- Tragen Sie Ihre bekannten Zugangsdaten in die Felder „Benutzername“ und „Passwort“ und klicken auf „Anmelden“. Hier müssen Sie sich wieder mit der Face/Touch ID authentifizieren
- Der Registrierungsprozess ist abgeschlossen. Sie können sich ab sofort jederzeit bei dem registrierten Endgerät anmelden und PVSconnect nutzen
- Die PVSconnect Webseite können Sie sich bei Bedarf auf den Home-Bildschirm legen. Klicken Sie den Sharebutton an und wählen „zum Home-Bildschirm“ aus



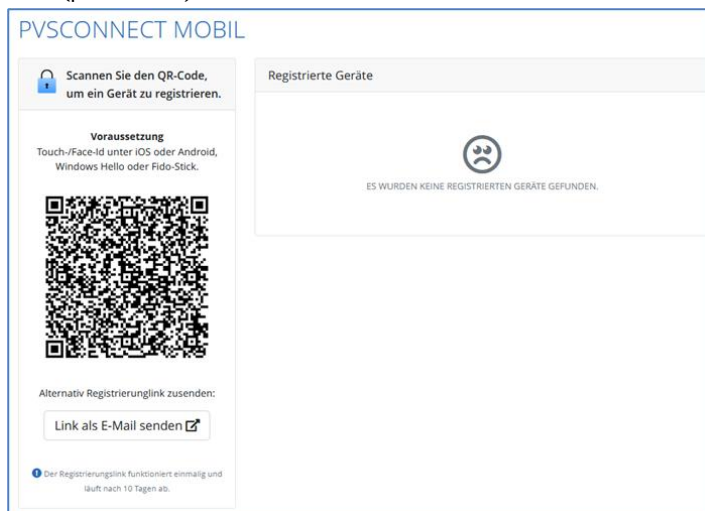
## Installation von Softzertifikaten / Einrichtung von 2-Faktor-Authentifizierung

### 3.2 2-Faktor-Authentifizierung/Registrierung Android-Geräten

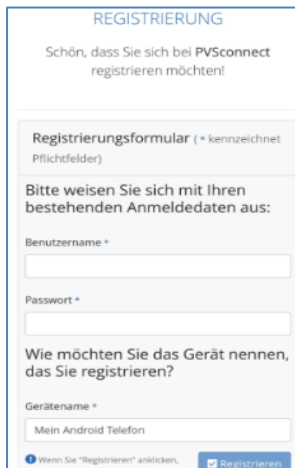
- Melden Sie sich mit Ihren PVScconnect Zugangsdaten bei PVScconnect auf einem PC an, bei dem das Zertifikat bereits installiert wurde
- Wählen Sie den Menüpunkt Service aus und klicken auf „PVScconnect Mobil“



- Scannen Sie den QR-Code mit Hilfe Ihrer Kamera oder einem Barcode Scanner ab und öffnen den Link (pvs-se.de)



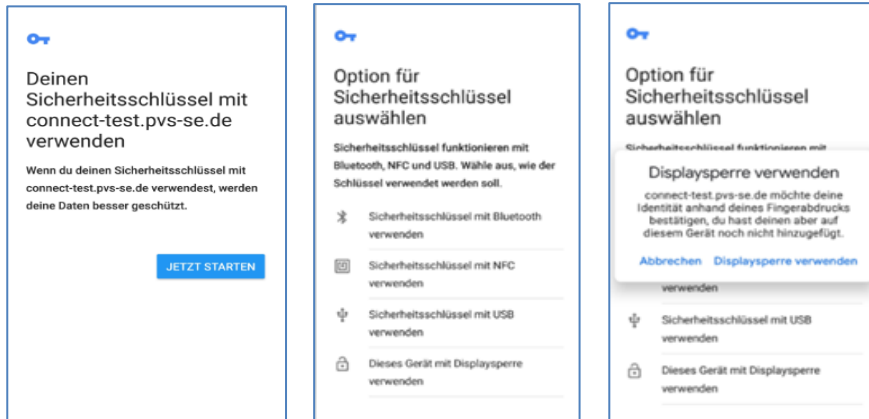
- Auf der Registrierungswebseite weisen Sie sich mit Ihren PVScconnect Zugangsdaten aus und tragen einen Gerätenamen ein



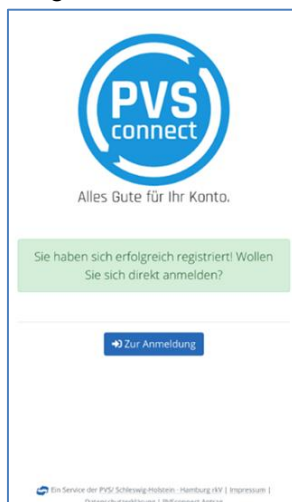
- Klicken Sie auf „Registrieren“


## Installation von Softzertifikaten / Einrichtung von 2-Faktor-Authentifizierung

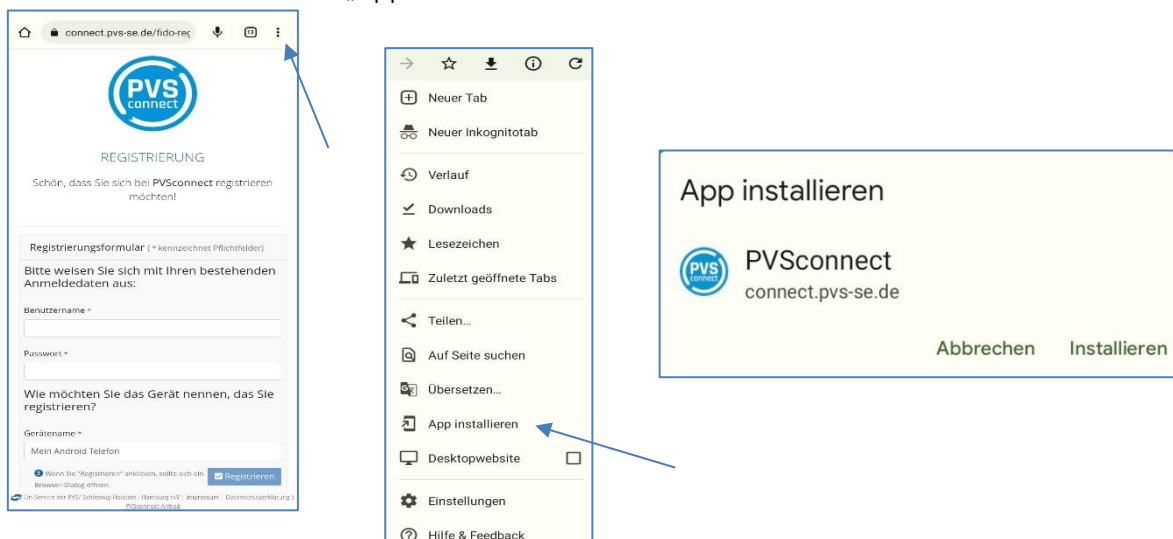
- Ihr Gerät fragt an, welchen Sicherheitsschlüssel die Webseite verwenden darf z.B. Displaysperre, Face-ID



- Der Registrierungsprozess ist abgeschlossen. Sie können sich ab sofort jederzeit bei dem registrierten Endgerät anmelden und PVScconnect nutzen



- Die PVScconnect Webseite können Sie sich bei Bedarf auf den Start-Bildschirm legen. Klicken Sie hierfür oben rechts auf die Einstellungen  Wählen Sie die Schaltfläche „App installieren“ aus



## Installation von Softzertifikaten / Einrichtung von 2-Faktor-Authentifizierung

### 3.3 2-Faktor-Authentifizierung Windows Hello-Fingerabdruck Einrichtung

- Sollten Sie Windows Hello bisher noch nicht eingerichtet haben, führen Sie bitte folgende Schritte durch:  
Schritt 1:

Informationen zu Windows Hello und zur Einrichtung

Windows 11, Windows 10

**Windows 11    Windows 10**

Windows Hello ist eine persönlichere und sicherere Möglichkeit, um mithilfe einer PIN, Gesichtserkennung oder eines Fingerabdrucks sofort auf Ihre Windows 10-Geräte zugreifen zu können. Sie müssen eine PIN als Teil der Anmeldung mit Fingerabdruck oder Gesichtserkennung einrichten. Sie können sich auch nur mit Ihrer PIN anmelden.

Mithilfe dieser Optionen wird die Anmeldung bei Ihrem PC erleichtert und sicherer, da Ihre PIN nur einem Gerät zugeordnet und für eine Wiederherstellung mit Ihrem Microsoft-Konto gesichert ist.

**Einrichten von Windows Hello**

Wählen Sie die Schaltfläche oben, um direkt zu den **Einstellungen** zu gelangen, oder folgen Sie diesen Schritten, um Windows Hello einzurichten.

1. Wählen Sie **Start** > **Einstellungen** > **Konten** > **Anmeldeoptionen**.
2. Unter **Verwalten, wie Sie sich bei Ihrem Gerät anmelden** werden Ihnen drei Optionen zur Anmeldung mit Windows Hello angezeigt:
  - Wählen Sie **Windows Hello-Gesichtserkennung** aus, um die Gesichtserkennungsanmeldung mit der Infrarotkamera Ihres PCs oder einer externen Infrarotkamera einzurichten.
  - Wählen Sie **Windows Hello-Fingerabdruckerkennung** aus, um die Anmeldung mit einem Fingerabdruckleser einzurichten.
  - Wählen Sie **Windows Hello-PIN** aus, um die Anmeldung mit einer PIN einzurichten.

#### Schritt 2:

Startseite

Einstellung suchen

**Konten**

Ihre Infos

E-Mail und Konten

Anmeldeoptionen

Auf Arbeits- oder Schulkonto zugreifen







Einstellungen synchronisieren

### Anmeldeoptionen

\*Einige dieser Einstellungen sind ausgeblendet oder werden von Ihrer Organisation verwaltet.

#### Vorgehensweise für die Anmeldung an Ihrem Gerät verwalten

Wählen Sie eine Anmeldeoption aus, um sie hinzuzufügen, zu ändern oder zu entfernen.

-  **Windows Hello-Gesichtserkennung**  
Diese Option ist zurzeit nicht verfügbar. Klicken Sie hier, um weitere Informationen zu erhalten.
-  **Windows Hello-Fingerabdruckerkennung**  
Mit Fingerabdruckscanner anmelden (empfohlen)
-  **Windows Hello-PIN**  
Mit PIN anmelden (empfohlen)
-  **Sicherheitsschlüssel**  
Mit physischem Sicherheitsschlüssel anmelden
-  **Kennwort**  
Mit Ihrem Kontokennwort anmelden
-  **Bildcode**  
Wischen und tippen Sie auf ihr Lieblingsfoto, um Ihr Gerät zu entsperren

## Installation von Softzertifikaten / Einrichtung von 2-Faktor-Authentifizierung

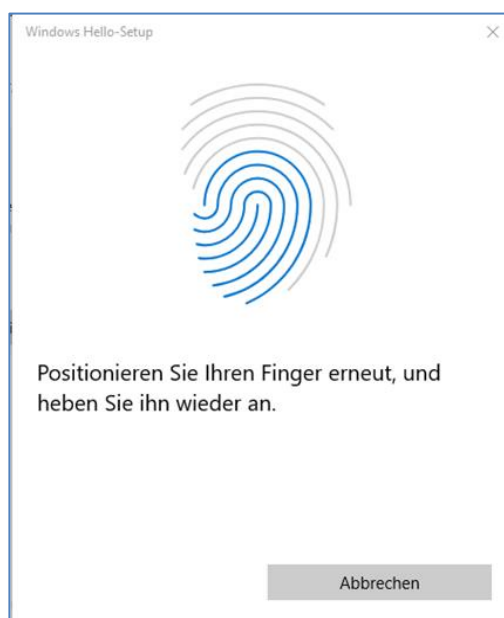
### Schritt 3:



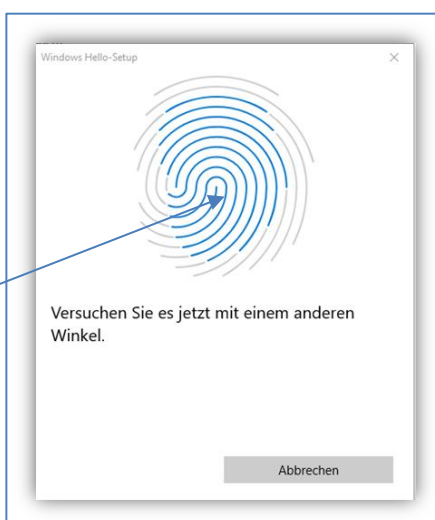
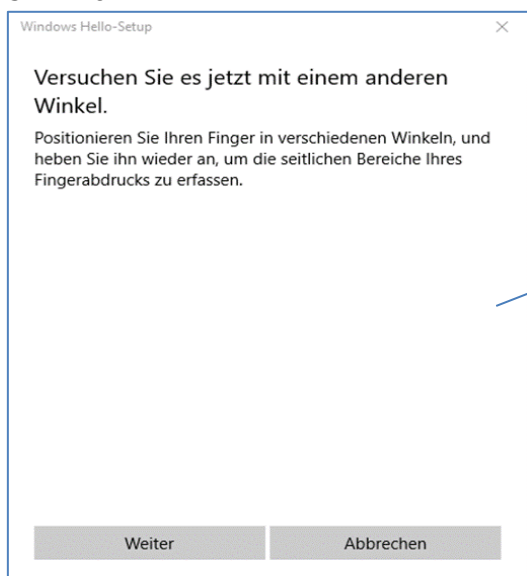
### Schritt 4:



### Schritt 5:

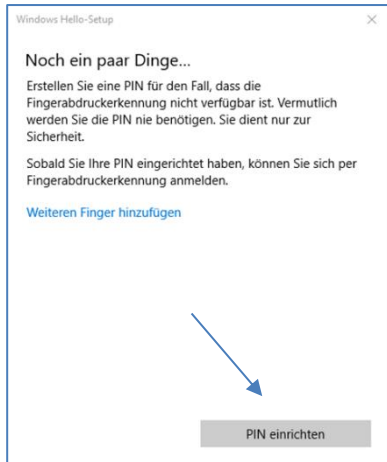


### Schritt 6:

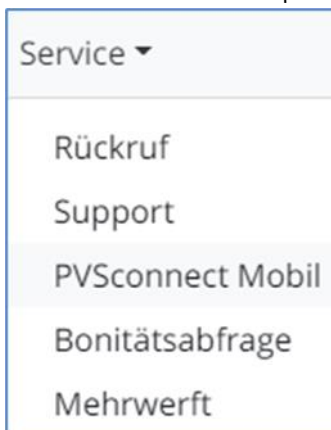


## Installation von Softzertifikaten / Einrichtung von 2-Faktor-Authentifizierung

### Schritt 7:



- Registrierung für PVSconnect Mobil PC vornehmen
- Melden Sie sich mit Ihren PVSconnect Zugangsdaten bei PVSconnect auf einem PC an, bei dem das Zertifikat bereits installiert wurde
- Wählen Sie den Menüpunkt Service aus und klicken auf „PVSconnect Mobil“



- Wählen Sie den Button „Link als E-Mail senden“ aus. Die E-Mail wird an die E-Mail-Adresse versendet, mit der Sie sich das erste Mal bei PVSconnect registriert haben. Sollte die E-Mail an eine andere E-Mail-Adresse gesendet werden, können Sie diese selbstständig in Ihrem PVSconnect Zugang ändern





- Öffnen Sie Ihr E-Mail-Programm und klicken auf die neue E-Mail. Wählen Sie „PVScconnect aktivieren“ aus

**Betreff: PVScconnect aktivieren**

Bitte klicken Sie hier:

[PVScconnect aktivieren](#)

um PVScconnect zu aktivieren.

- Auf der Registrierungswebseite weisen Sie sich mit Ihren PVScconnect Zugangsdaten aus und tragen einen Gerätenamen ein

- Sobald die Registrierung abgeschlossen wurde, öffnet sich ein weiteres Fenster „Windows-Sicherheit“. Scannen Sie Ihren Fingerabdruck mit dem Fingerabdruckleser

- Die Authentifizierung ist somit abgeschlossen und Sie können sich mit Ihren bekannten PVScconnect Zugangsdaten anmelden

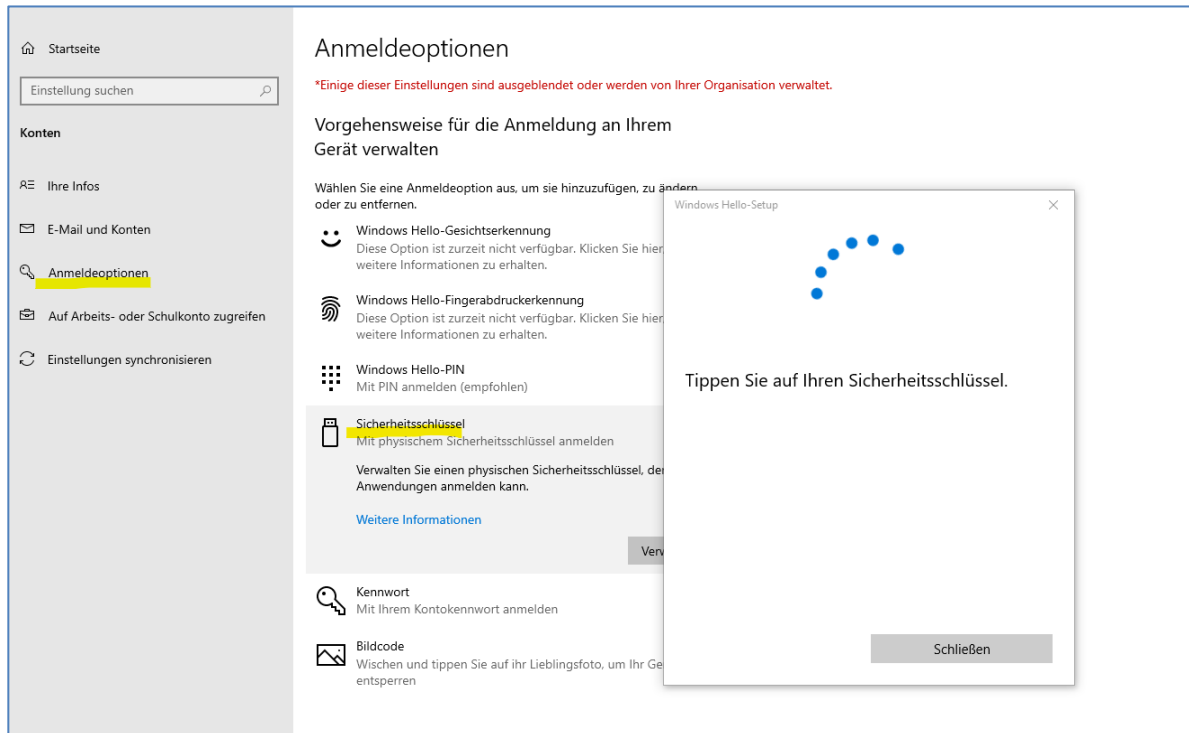


## Installation von Softzertifikaten / Einrichtung von 2-Faktor-Authentifizierung

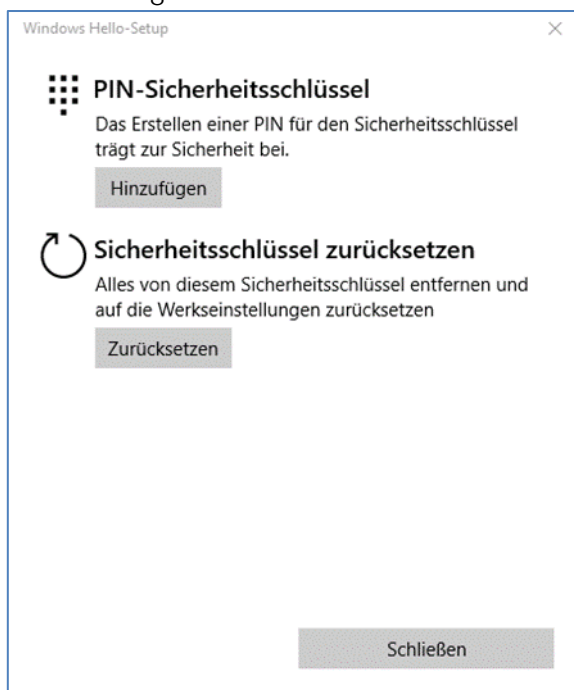
### 3.4 2-Faktor-Authentifizierung Einrichtung Fido-Stick

- Sollten Sie den Fido-Stick bisher noch nicht eingerichtet haben, führen Sie bitte folgende Schritte durch:

Schritt 1: Wählen Sie die „Einstellungen“ Ihres PC's aus und klicken auf „Konten“ -> „Anmeldeoptionen“ -> „Sicherheitsschlüssel“



Schritt 2: Fügen Sie den PIN-Sicherheitsschlüssel hinzu

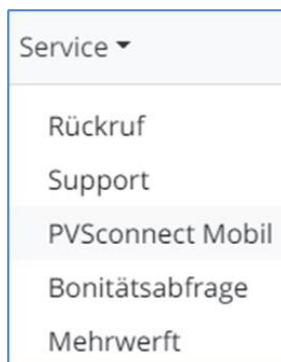


## Installation von Softzertifikaten / Einrichtung von 2-Faktor-Authentifizierung

Schritt 3: Vergeben Sie einen persönlichen Sicherheitsschlüssel-PIN



- Registrierung für PVScconnect Mobil vornehmen
- Melden Sie sich mit Ihren PVScconnect Zugangsdaten bei PVScconnect auf einem PC an, bei dem das Zertifikat bereits installiert wurde
- Wählen Sie den Menüpunkt Service aus und klicken auf „PVScconnect Mobil“

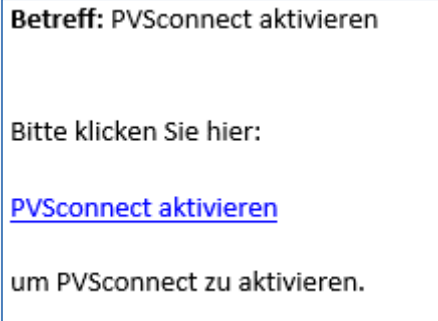


- Wählen Sie den Button „Link als E-Mail senden“ aus. Die E-Mail wird an die E-Mail-Adresse versendet, mit der Sie sich das erste Mal bei PVScconnect registriert haben. Sollte die E-Mail an eine andere E-Mail-Adresse gesendet werden, können Sie diese selbstständig in Ihrem PVScconnect Zugang ändern

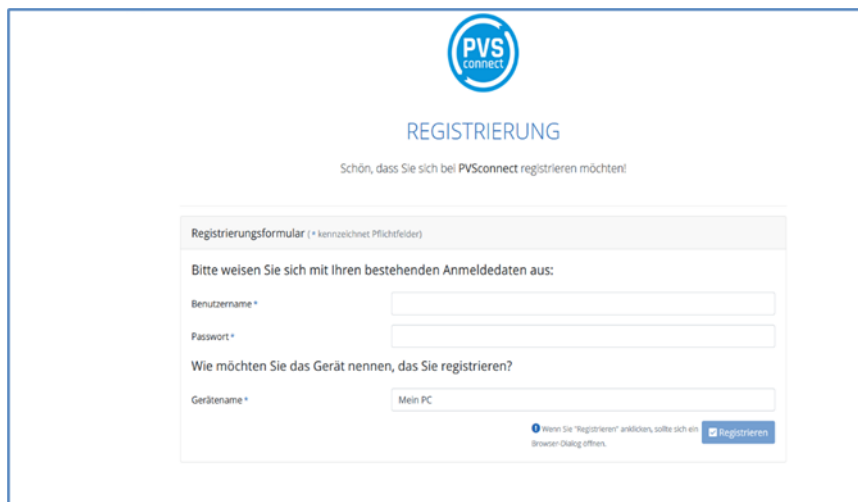


## Installation von Softzertifikaten / Einrichtung von 2-Faktor-Authentifizierung

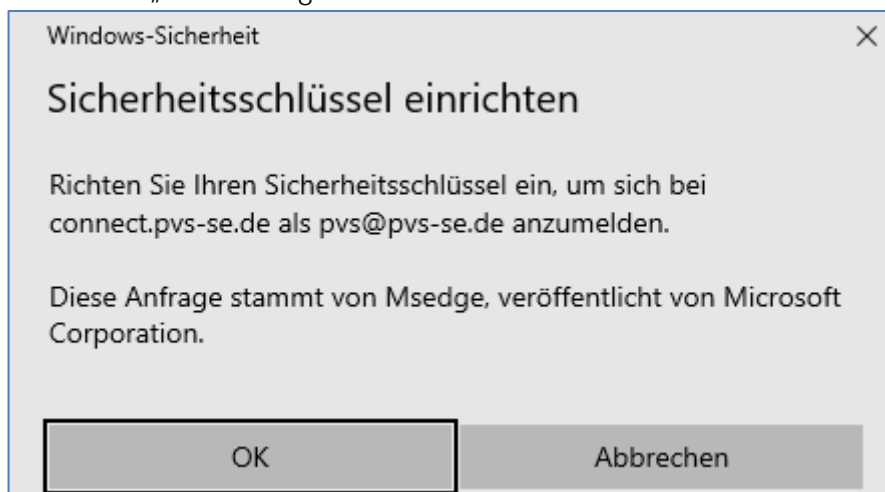
- Öffnen Sie Ihr E-Mail-Programm und klicken auf die neue E-Mail. Wählen Sie „PVScconnect aktivieren“ aus



- Auf der Registrierungswebseite weisen Sie sich mit Ihren PVScconnect Zugangsdaten aus und tragen einen Gerätenamen ein

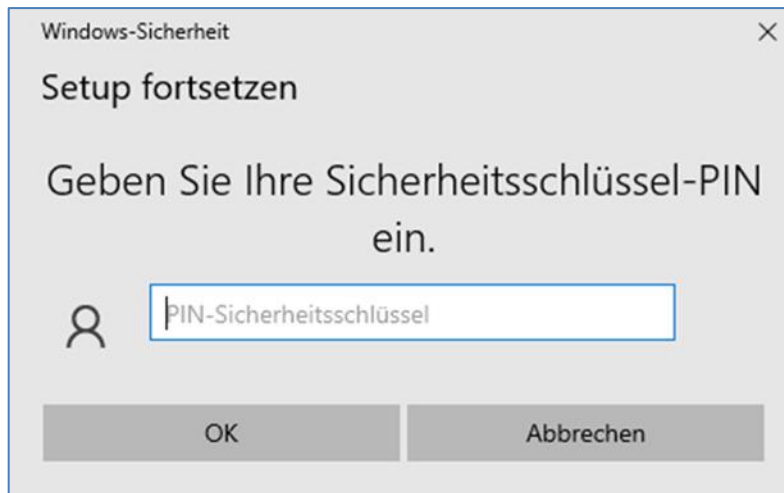


- Sobald die Registrierung abgeschlossen wurde, öffnet sich ein weiteres Fenster „Windows-Sicherheit“. Dieses mit „OK“ bestätigen

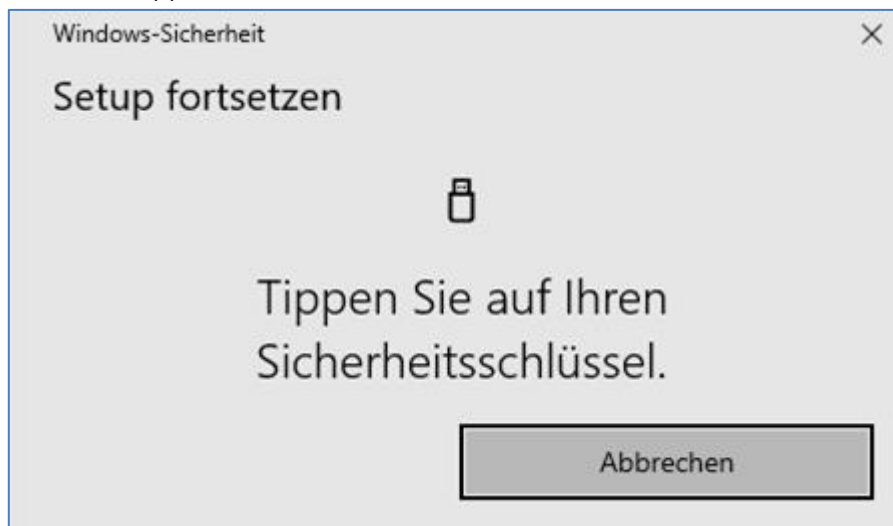


## Installation von Softzertifikaten / Einrichtung von 2-Faktor-Authentifizierung

- Tragen Sie den vorher vergebenen PIN des Fido-Sticks ein



- Beführen/Tippen Sie einmal auf Ihren Fido-Stick



- Durch das Berühren/Tippen auf den Sicherheitsschlüssel ist die Registrierung des Fido Sticks für PVSconnect erfolgreich abgeschlossen und eine Anmeldung mit den Zugangsdaten kann vorgenommen werden

