Perigon Hello

Login via Authentication Service

GEMEINSAM SCHÜTZEN
WIR IHRE DATEN

root-service ag | Weinfelderstrasse 32 | 8575 Bürglen | T +41 (0)71 634 80 40 | info@root.ch | www.root.ch

Einleitung


Gesundheitsdaten besonders schützen
erhöhte Ansprüche an den Datenschutz
Perigon Hello
effiziente Pflege
zunehmende Digitalisierung
Schutz der Privatsphäre

Was ist Perigon Hello?

Perigon Hello ist ein Authentication Service (Anmeldedienst), der Login-Informationen empfängt und mit diesen Informationen die Identität des Benutzers bestätigt oder verneint.

Was ist der Authentication Service?

- Zugriff/Berechtigung wird weiterhin vom Perigon Ihrer Spitex definiert
- Zentrale Datenbank auf einem Rechenzentrum in der Schweiz
- Benutzernamen, Kennwort als Hash werden in der zentralen Datenbank gespeichert
- **Es werden keine Mitarbeiter- oder Kundendaten in der Perigon Hello Datenbank gespeichert.**

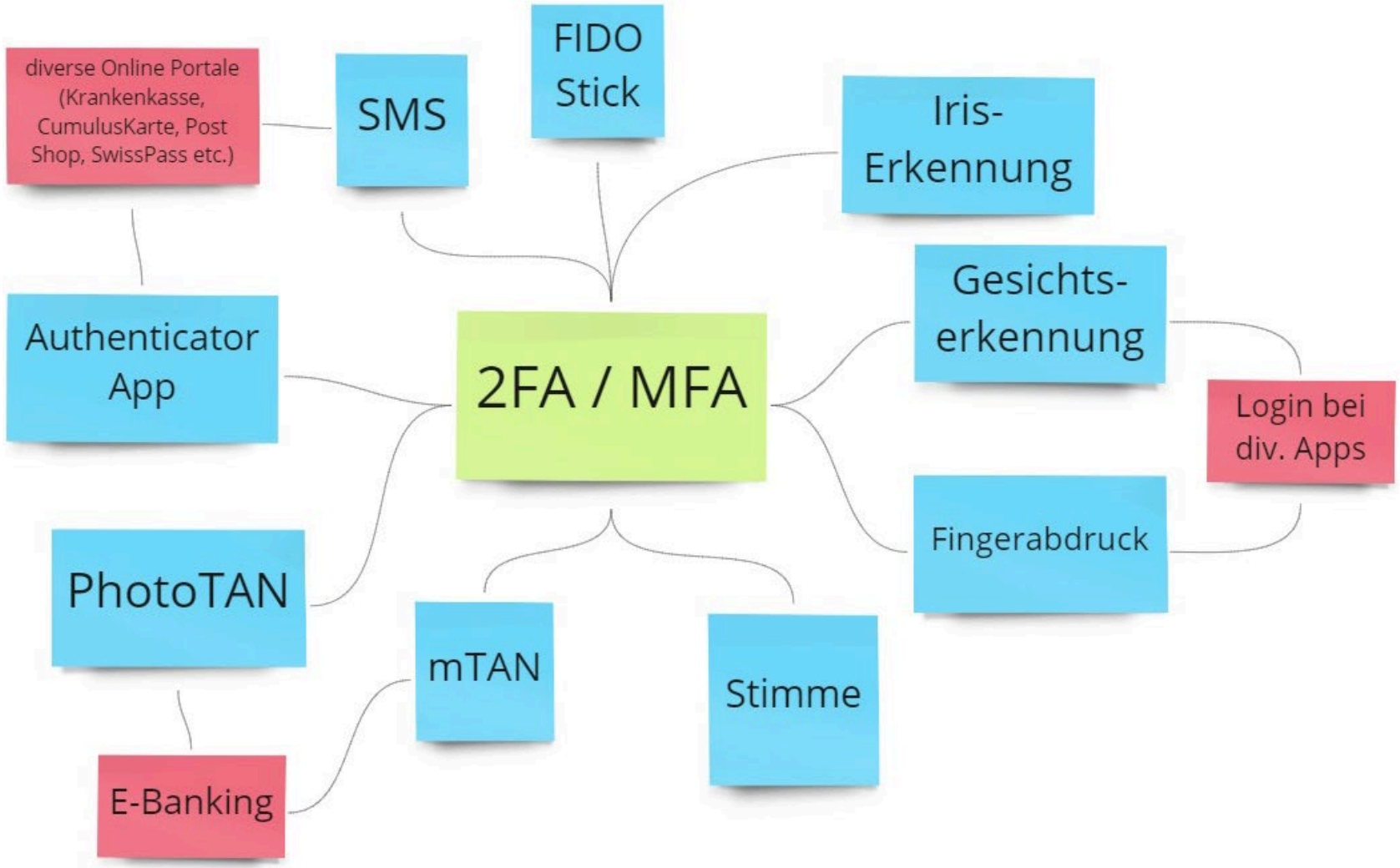
Was sind die Vorteile des Authentication Service?

- Grundstein für eine zeitgemässe und flexible Anmeldung
- Vereinfachung vom Login-Prozess mittels Delegationen
- Delegation aufgrund vom OpenID Connect Standard (OIDC) an verschiedene Anmeldedienste möglich.
- Multifaktor-Authentifizierung wird möglich
- Vereinfachter Login auch beim Personalaustausch

Was ist eine Multifaktor-Authentifizierung (MFA)?

- Die Multifaktor-Authentifizierung ist eine Sicherheitsprozedur, bei der ein Anwender zwei unterschiedliche Merkmale bereitstellt, um sich zu identifizieren.

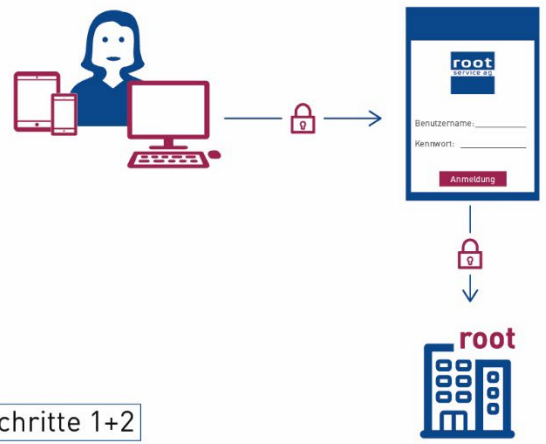
Beispiele weiterer Faktoren?



Login mit MFA (Vereinfachte Darstellung)

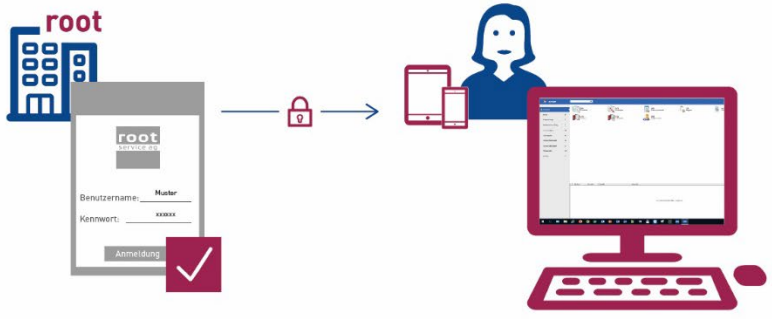
1. Der Benutzer gibt den Benutzernamen und das Kennwort im Perigon Spitex (am PC oder am mobilen Gerät) ein und bestätigt die Eingabe.
2. Benutzernamen und Kennwort werden an den root-Authentication Service gesendet.
3. Der root-Authentication Service prüft den Benutzernamen und das Kennwort.
4. Der root-Authentication Service generiert einen zweiten Faktor (SMS-Code, Push-Meldung usw.) und leitet diesen an den Benutzer weiter.
5. Der Benutzer gibt den zweiten Faktor ein und bestätigt die Eingabe.
6. Der eingegebene zweite Faktor wird an den root-Authentication Service gesendet.
7. Der root-Authentication Service prüft den zweiten Faktor.
8. Der root-Authentication Service leitet die Freigabe an den Benutzer weiter und erlaubt den Zugriff.

✓ Der Benutzer ist angemeldet.



Schritte 1+2

Schritte 3-7

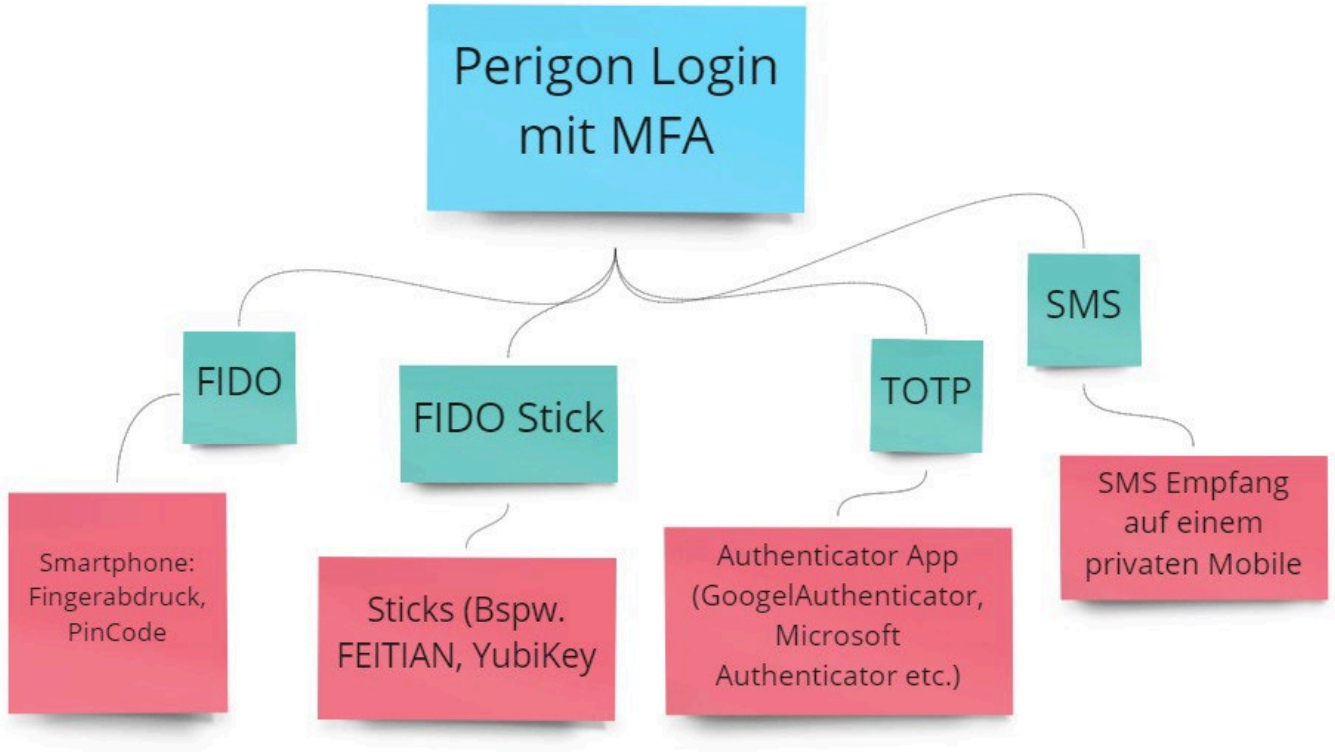


Schritt 8

Was sind die Vorteile von MFA?

- Es kann ein einfacheres Kennwort verwendet werden
- Gelangt ein Kennwort in falsche Hände ist der Login dennoch sicherer.
- Für einen unbefugten Zugriff muss auch der 2. Faktor im Besitz dieser Person sein.
- Benutzer kann sein eigenes Perigon Kennwort selbständig zurücksetzen sofern nebst MFA auch eine E-Mailadresse hinterlegt ist.

Perigon Login mit MFA



Was versteht man unter Login Delegation?

- Prüfung der Identität erfolgt durch den Anmeldedienst der Delegation.

- Solche Anmeldedienste sind beispielsweise HIN, SwissID oder Microsoft Azure.

Wie funktioniert eine Login Delegation?

- Mögliche Delegationen werden pro Organisation festgelegt
- Welcher User wohin sein Login delegieren kann wird pro User festgelegt
- Mischformen sind möglich

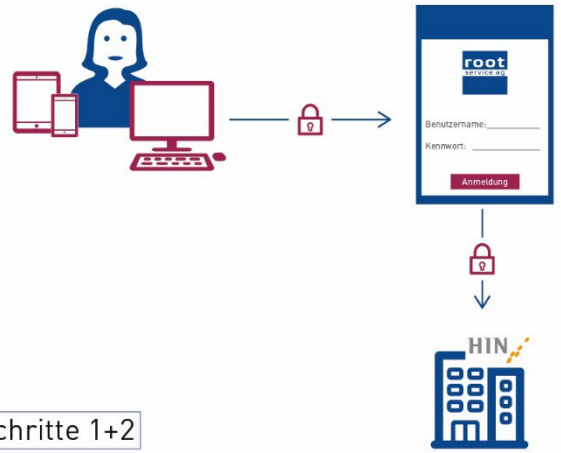
Wie funktioniert eine Login Delegation?

- Auswahl beim Login
- Weiterleitung auf die Seite des Anbieters der Delegation
- Benutzernamen und Kennwort des Anbieters der Delegation werden eingegeben
- Der Anbieter prüft nun die Identität und leitet das Ergebnis an den Perigon Authentication Service zurück.
  - Der Anbieter stellt quasi einen Pass aus «Ja das ist Max». Perigon mappt diesen Benutzer Max, dann zum Perigon Benutzer Max und meldet den Perigon Benutzer Max an.

Login mit Delegation (Vereinfachte Darstellung)

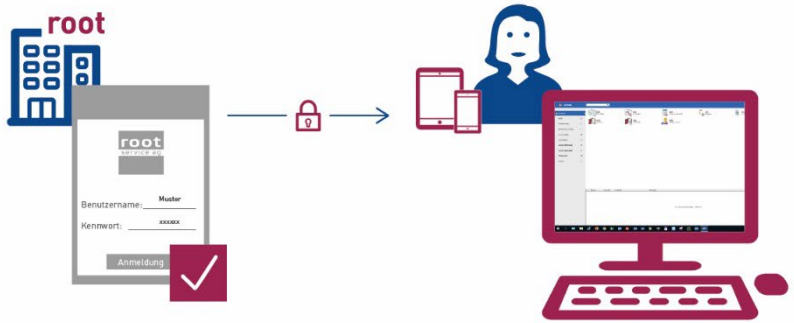
1. Der Benutzer wählt HIN für die Anmeldung am Perigon Spitex (am PC oder am mobilen Gerät) aus und bestätigt diese Auswahl.
2. Der root-Authentication Service leitet die Anfrage für die Anmeldung an HIN weiter.
3. Der Benutzer gibt den Benutzernamen und das Kennwort bei HIN ein.
4. HIN prüft den Benutzernamen und das Kennwort.
5. HIN generiert einen zweiten Faktor und sendet diesen an den Benutzer.
6. Der Benutzer gibt den zweiten Faktor ein und bestätigt die Eingabe.
7. Der eingegebene zweite Faktor wird an HIN gesendet.
8. HIN prüft den zweiten Faktor.
9. HIN sendet die Freigabe für den Zugriff an den root-Authentication Service.
10. Der root-Authentication Service leitet die Freigabe an den Benutzer weiter und erlaubt den Zugriff.

✓ Der Benutzer ist angemeldet.



Schritte 1+2

Schritte 3-9

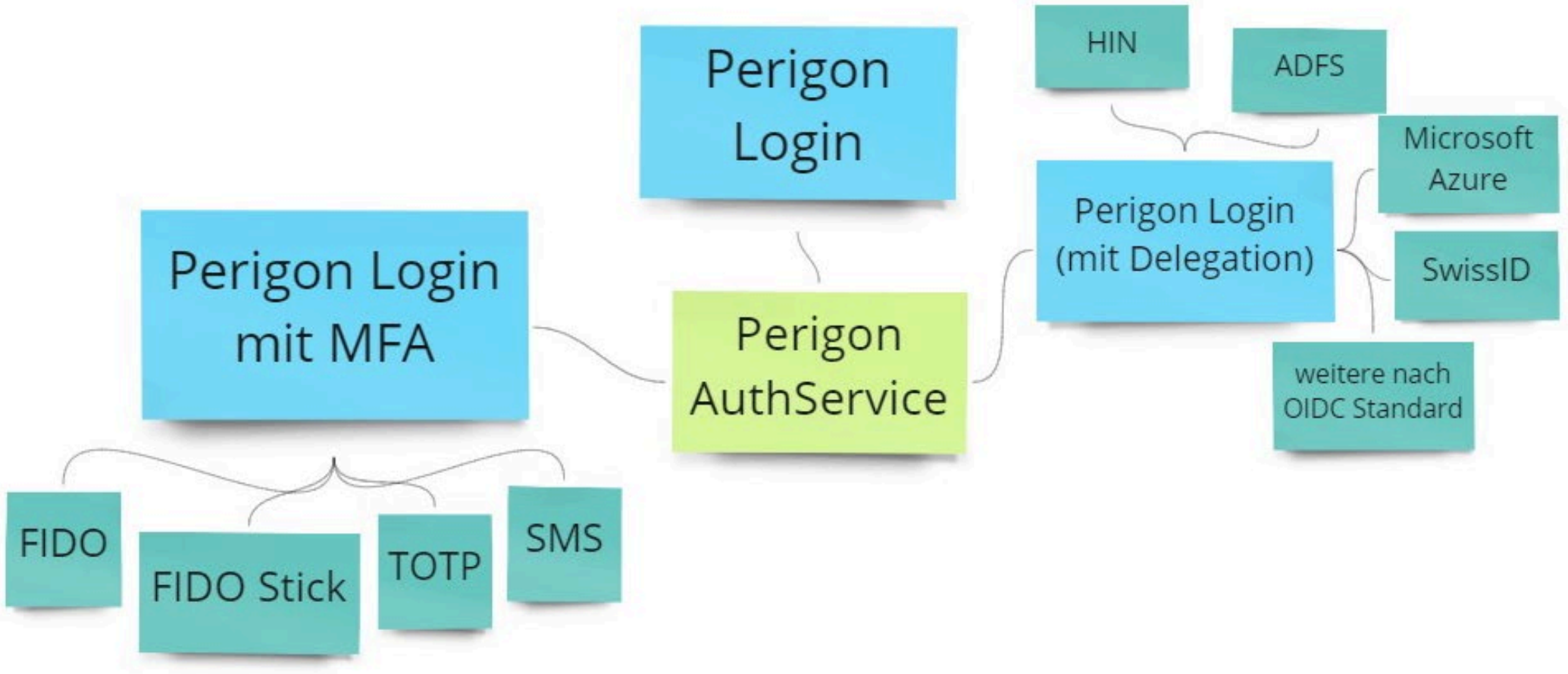


Schritt 10

Was ist der Vorteil einer Login Delegation?

- Gleiches Login für verschiedene Anwendungen
- Kennwortrichtlinien sind einheitlich und können zentral verwaltet werden
- MFA ist bei Azure, SwissID und HIN möglich und somit auch für das Perigon einsetzbar.

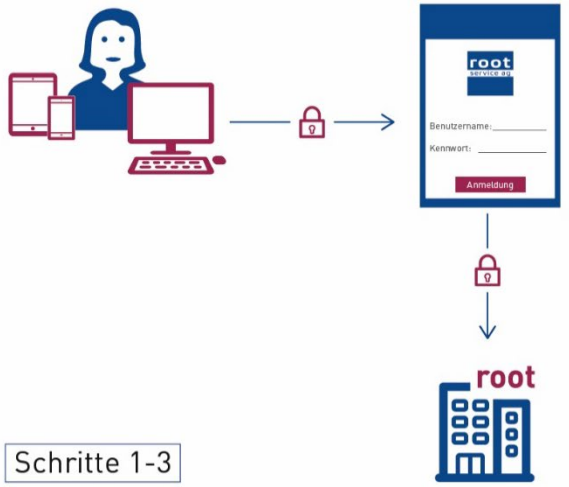
Möglichkeiten & Varianten Perigon Hello



Login mit root-Authentication Service
(Vereinfachte Darstellung)

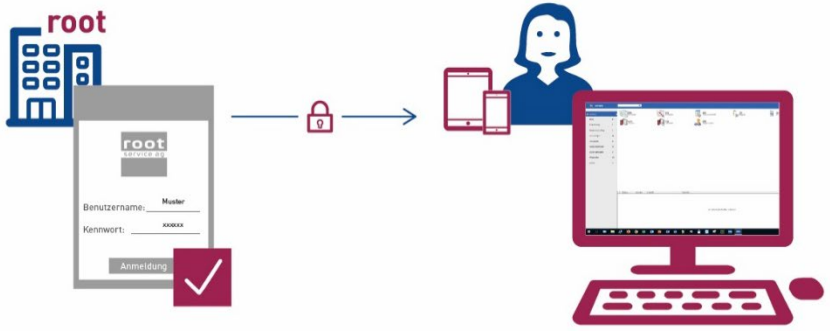
1. Der Benutzer gibt den Benutzernamen und das Kennwort im Perigon Spitex (am PC oder am mobilen Gerät) ein und bestätigt die Eingabe.
2. Benutzernamen und Kennwort werden an den root-Authentication Service gesendet.
3. Der root-Authentication Service prüft den Benutzernamen und das Kennwort.
4. Der root-Authentication Service leitet die Freigabe an den Benutzer weiter und erlaubt den Zugriff.

✓ Der Benutzer ist angemeldet.



Schritte 1-3

Schritt 4



Perigon Login

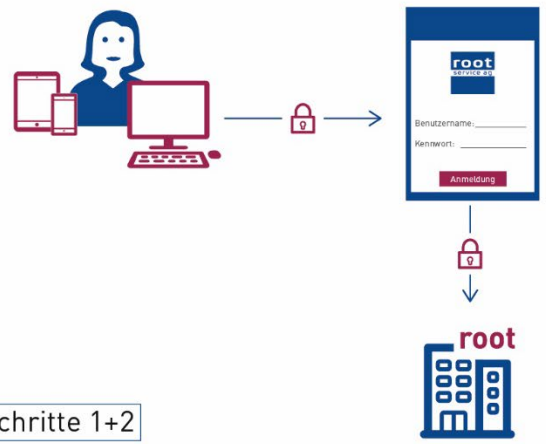
Perigon AuthService

root-service ag | Weinfelderstrasse 32 | 8575 Bürglen | T +41 (0)71 634 80 40 | info@root.ch | www.root.ch

Login mit MFA (Vereinfachte Darstellung)

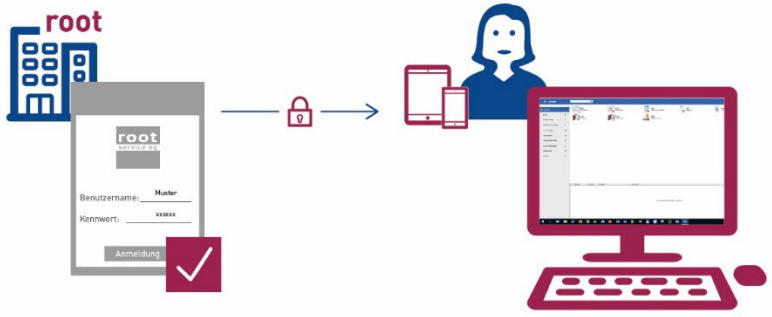
1. Der Benutzer gibt den Benutzernamen und das Kennwort im Perigon Spitex (am PC oder am mobilen Gerät) ein und bestätigt die Eingabe.
2. Benutzernamen und Kennwort werden an den root-Authentication Service gesendet.
3. Der root-Authentication Service prüft den Benutzernamen und das Kennwort.
4. Der root-Authentication Service generiert einen zweiten Faktor (SMS-Code, Push-Meldung usw.) und leitet diesen an den Benutzer weiter.
5. Der Benutzer gibt den zweiten Faktor ein und bestätigt die Eingabe.
6. Der eingegebene zweite Faktor wird an den root-Authentication Service gesendet.
7. Der root-Authentication Service prüft den zweiten Faktor.
8. Der root-Authentication Service leitet die Freigabe an den Benutzer weiter und erlaubt den Zugriff.

✓ Der Benutzer ist angemeldet.

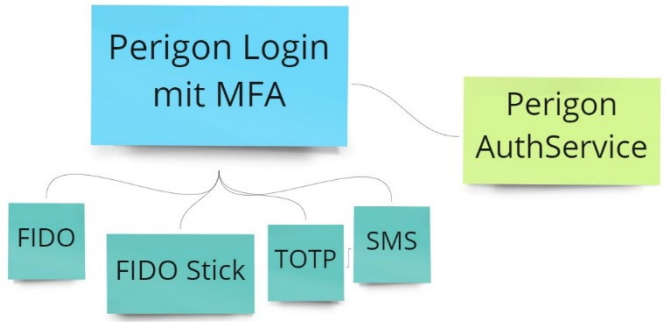


Schritte 1+2

Schritte 3-7



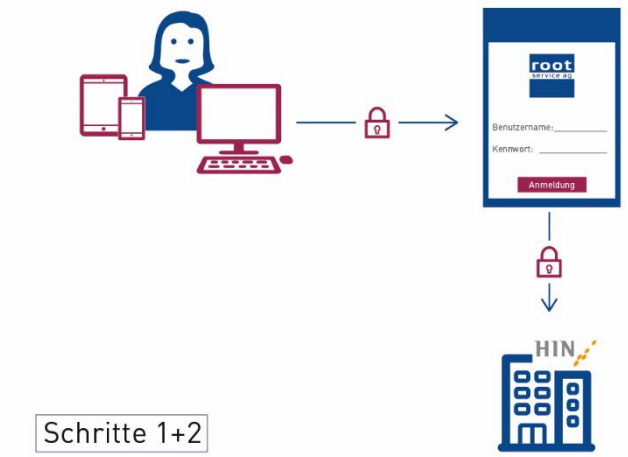
Schritt 8



Login mit Delegation (Vereinfachte Darstellung)

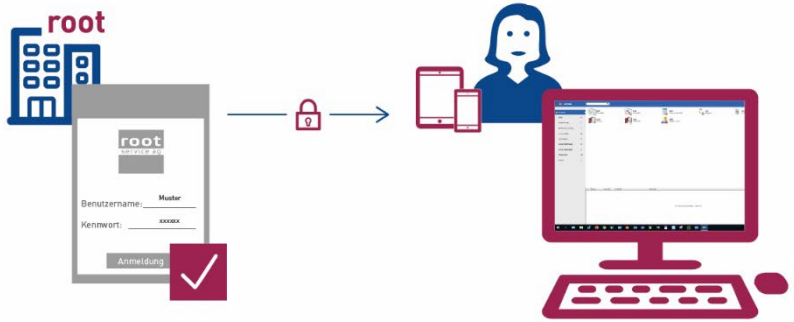
1. Der Benutzer wählt HIN für die Anmeldung am Perigon Spitex (am PC oder am mobilen Gerät) aus und bestätigt diese Auswahl.
2. Der root-Authentication Service leitet die Anfrage für die Anmeldung an HIN weiter.
3. Der Benutzer gibt den Benutzernamen und das Kennwort bei HIN ein.
4. HIN prüft den Benutzernamen und das Kennwort.
5. HIN generiert einen zweiten Faktor und sendet diesen an den Benutzer.
6. Der Benutzer gibt den zweiten Faktor ein und bestätigt die Eingabe.
7. Der eingegebene zweite Faktor wird an HIN gesendet.
8. HIN prüft den zweiten Faktor.
9. HIN sendet die Freigabe für den Zugriff an den root-Authentication Service.
10. Der root-Authentication Service leitet die Freigabe an den Benutzer weiter und erlaubt den Zugriff.

✓ Der Benutzer ist angemeldet.

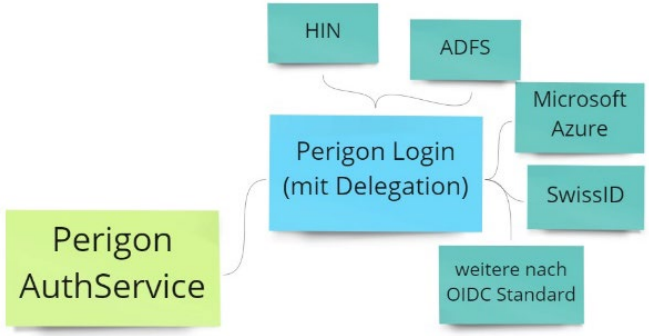


Schritte 1+2

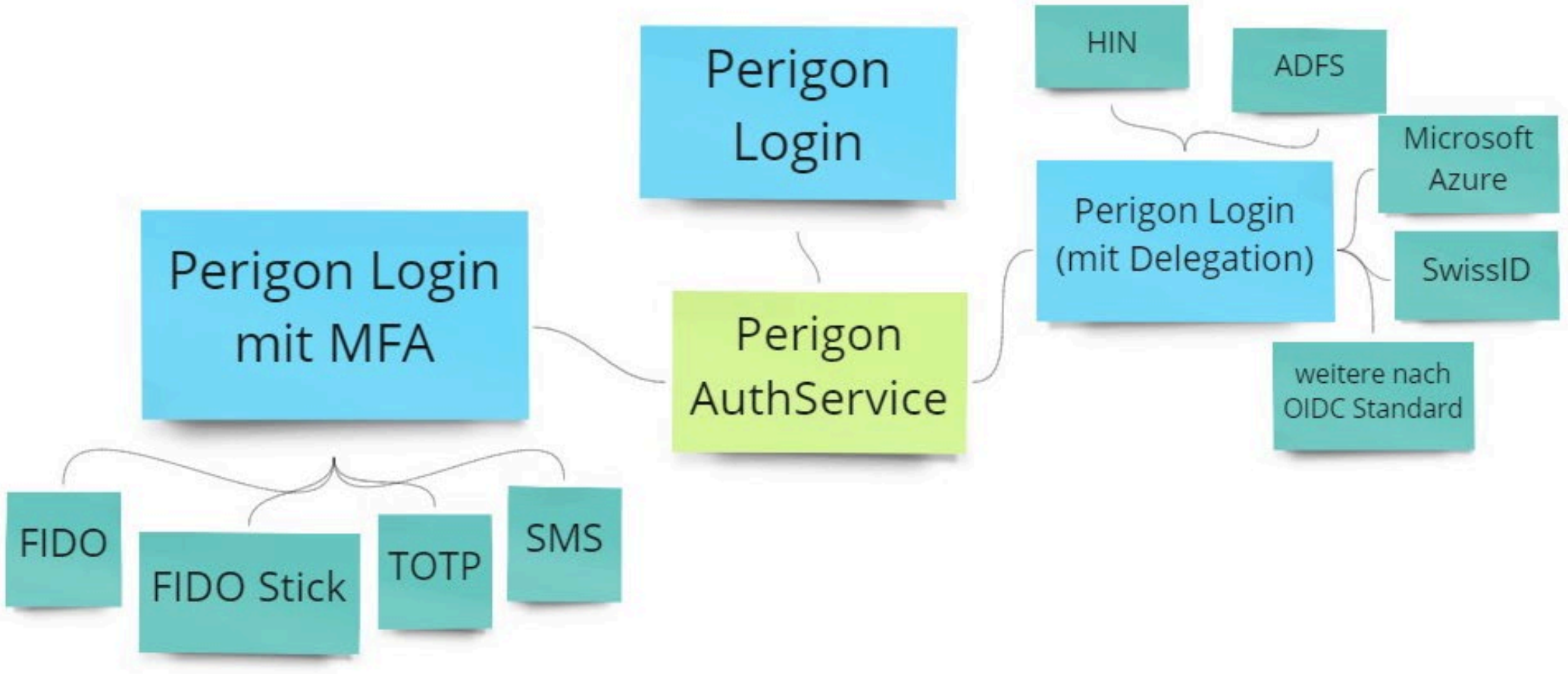
Schritte 3-9



Schritt 10



Möglichkeiten & Varianten Perigon Hello



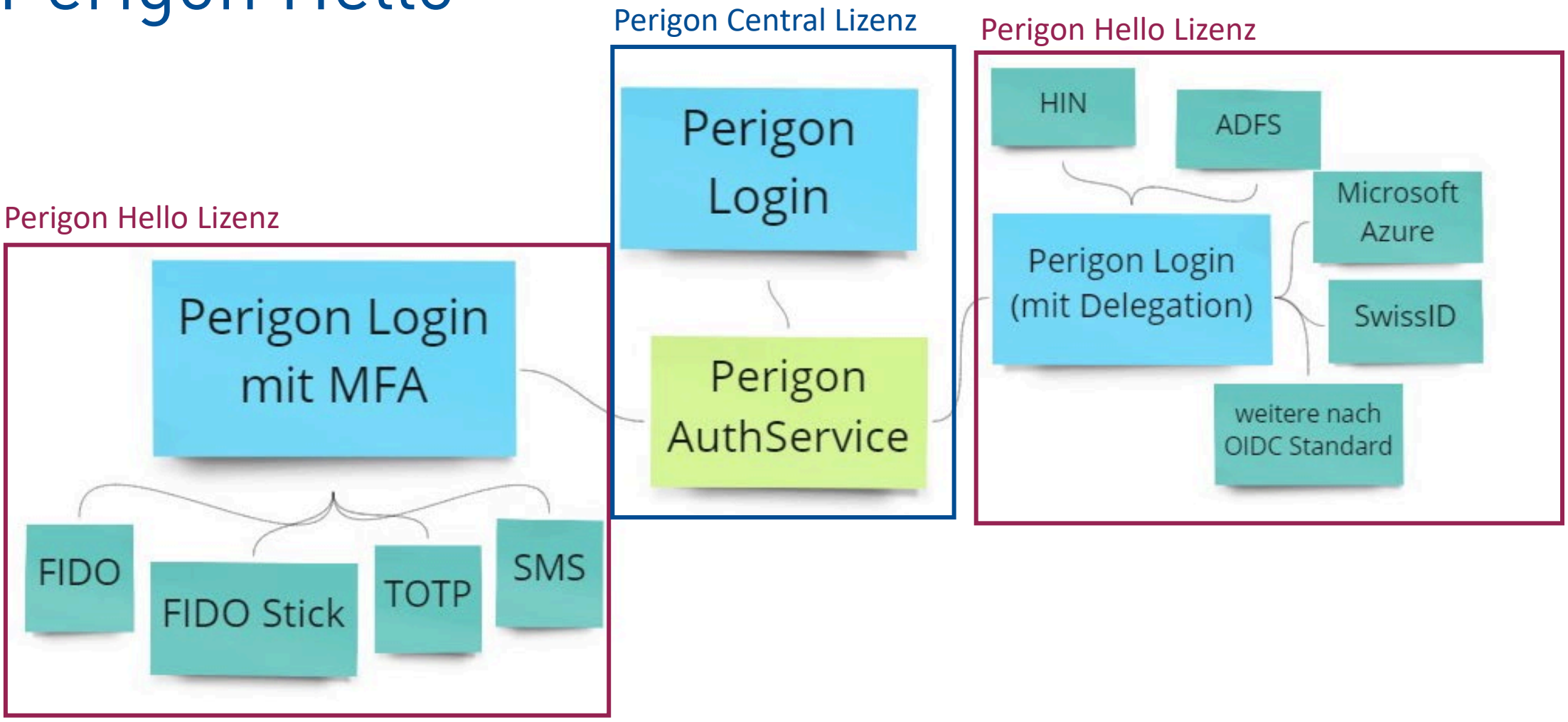
Lizenzierung / Kosten Perigon Hello

	Migration nach Aufwand	Support nach Aufwand	Kosten pro aktive [1] User/Monat Authenticator App	FIDO Stick	FIDO Mobile	Kosten pro versendetem SMS	HIN-ID pro Benutzer	SwissID pro Benutzer	Benutzer bei Microsoft Azure	Active Directory Service	Implementation nach Aufwand
Perigon Login	X	X	-	-	-	-	-	-	-	-	-
Perigon Login mit MFA											
+ TOTP	X	X	X	X	-	(X)[2]	-	-	-	-	-
+ FIDO Stick	X	X	X	-	X	(X)[2]	-	-	-	-	-
+ FIDO Mobile	X	X	X	-	-	X	-	-	-	-	-
+ SMS	X	X	X	-	-	(X)[2]	X	-	-	-	-
Perigon Login mit Delegation											
+ HIN	X	X	X	-	-	-	-	X	-	-	-	-
+ SwissID	X	X	X	-	-	-	-	-	X	-	-	-
+ Microsoft Azure	X	X	X	-	-	-	-	-	-	X	-	-
+ ADFS	X	X	X	-	-	-	-	-	-	-	X	-
+ weitere nach OIDC Standard	X	X	X	-	-	-	-	-	-	-	-	X

- Abrechnung erfolgt quartalsweise
- User mit Delegation und MFA werden nur 1x gezählt
- [1] sofern sich der User mind. 1x angemeldet hat
- [2] alternativer Faktor notwendig falls Login am PC möglich sein muss.

Perigon Hello Lizenz

Möglichkeiten & Varianten Perigon Hello



Unsere Empfehlung

- SwissCloud Kunden:
  - Perigon Login mit MFA

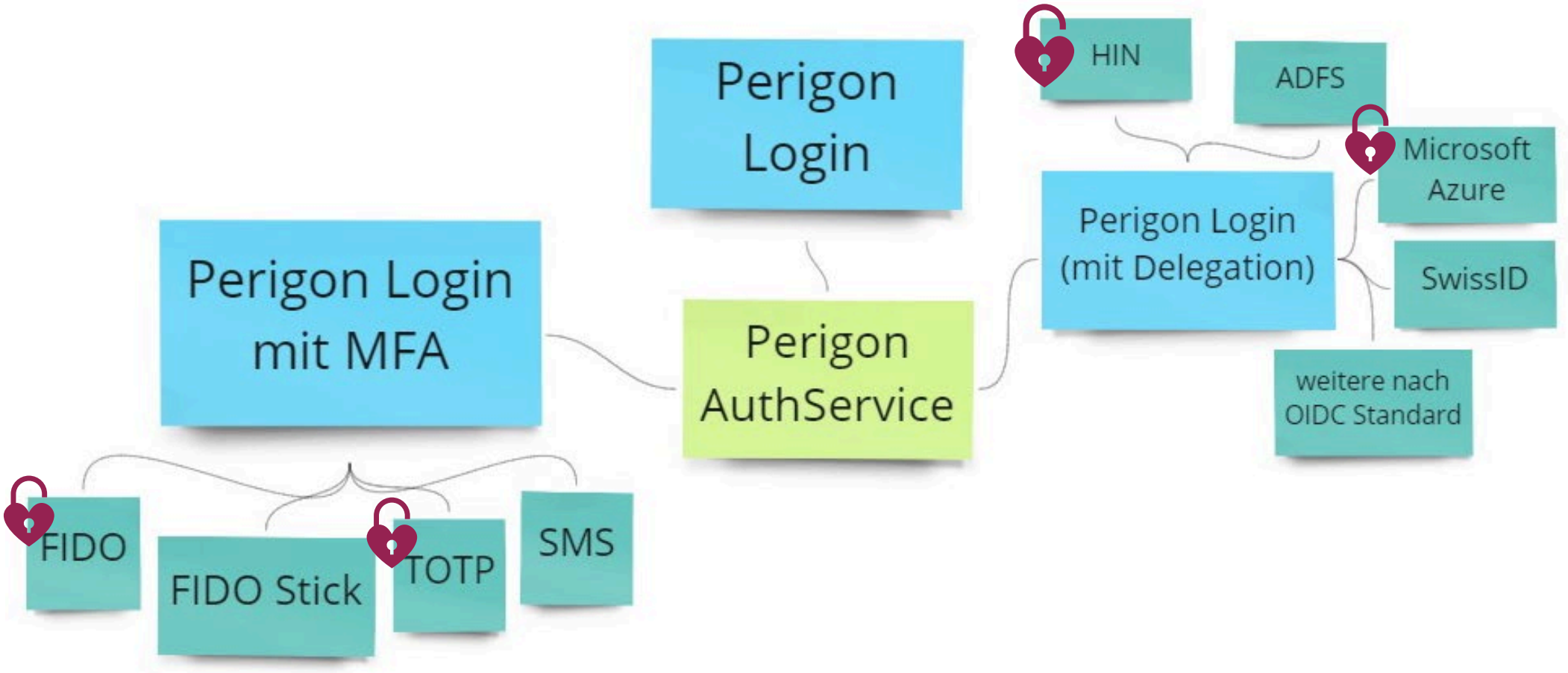
  oder
  - Delegation zu HIN oder bei grossen Organisationen (100 User+) zu SwissID

- Restliche Kunden:
  - Perigon Login mit MFA

  oder
  - Delegation zu HIN, Azure oder bei grossen Organisationen (100 User+) zu SwissID

Perigon Login ohne MFA ist längerfristig nicht mehr zu empfehlen. Die Multifaktor-Authentifizierung muss im Umgang mit sensiblen Daten zum «State of the Art» werden.

Unsere Empfehlung



Wieso?

Wieso soll ich als Spitex meine Logins via Authentication Service durchführen?

- Zeitgemässe Technologie
- Umgang mit Kennwörtern überdenken
- 2. Faktor als zusätzliche Sicherheit ermöglichen
- Vereinfachung der Logins (Stichwort „Delegation“)
- Datenschutz- und Datensicherheit muss von der Organisation gewährleistet werden
- Bereit für künftige Perigon Neuerungen


root
service ag
your data company
GEMEINSAM SCHÜTZEN
WIR IHRE DATEN