root-service ag
Weinfelderstrasse 32
Postfach 227
CH-8575 Bürglen

Telefon +41 (0)71 634 80 40
E-Mail: info@root.ch
Internet: www.root.ch

Dokument: Perigon Login via Authentication Service (Perigon Hello)	Dokumententyp: Systeminformationen
Dokumentennummer: PS-SI-20211019	Programmversion: ab 2022.1
Ausgabedatum: 19. Oktober 2021	Letzte Aktualisierung: 09. Februar 2022

Systeminformationen Perigon Spitex

Perigon Login via Authentication Service (Perigon Hello)

Einleitung

Mit der zunehmenden Digitalisierung unserer Gesellschaft werden auch die Ansprüche an den Datenschutz und vor allem die Datensicherheit laufend höher. Dabei gehören speziell Gesundheitsdaten zu den Daten, für welche ein erhöhtes Schutzbedürfnis besteht. Sie müssen mit allen möglichen Mitteln vor unbefugten Zugriffen geschützt werden. Neben einer qualitativ hochwertigen Pflege ist die Privatsphäre der Kunden/Klienten das wichtigste Gut. Um den gestiegenen Ansprüchen an den Schutz der Daten vor unbefugten Zugriffen Rechnung zu tragen, ist neu für das Perigon Spitex der Authentication Service verfügbar. Damit wird der Zugang zum Perigon Spitex, egal ob am PC oder im Perigon Mobile, zusätzlich mit den neusten und sichersten Technologien abgesichert.

Was ist Perigon Hello?

Ein Authentication Service (Anmeldedienst) ist ein Dienst, der Login-Informationen empfängt und mit diesen Informationen die Identität des Benutzers prüft. Abhängig vom Resultat der Prüfung und von den Berechtigungen des Benutzers werden danach entsprechende Zugriffe gewährt oder verweigert. Der Authentication Service wird auf einem Rechenzentrum in der Schweiz betrieben und hat Zugriff auf eine zentrale Datenbank. Entscheidet sich eine Spitex-Organisation, ihre Anmeldung am Perigon via Authentication Service vorzunehmen, werden die Benutzerdaten in der zentralen Datenbank gespeichert. Gespeichert werden nebst dem Benutzernamen nicht das Kennwort, sondern eine verschlüsselte Version, die nur mit der Kennworteingabe vom Benutzer verglichen werden kann. In dieser Datenbank werden ausschliesslich Daten der Benutzer gespeichert. Kunden- oder Mitarbeiterdaten usw. bleiben nach wie vor in der persönlichen Datenbank pro Spitex-Organisation.

Was sind die Vorteile des Authentication Service?

Mit dem Authentication Service legen wir den Grundstein für eine zeitgemässe und flexible Anmeldung an der Software. Da der Authentication Service auf dem OpenID Connect Standard

root-service ag
Weinfelderstrasse 32
Postfach 227
CH-8575 Bürglen

Telefon +41 (0)71 634 80 40
E-Mail: info@root.ch
Internet: www.root.ch

(OIDC) basiert, können wir Logins an bekannte Anmeldedienste delegieren (HIN, SwissID, Microsoft Azure usw.). Dadurch kann ein Anwender das gleiche Login für mehrere Anwendungen verwenden. So wird das Login-Prozedere massiv vereinfacht. Mit der Delegation an weitere Anmeldedienste ist je nach Anmeldedienst auch bereits die Multifaktor-Authentifizierung möglich.

Da sich die Benutzerdaten verschiedener Spitex-Organisationen in der zentralen Datenbank befinden, ist es möglich, dass ein Anwender auf verschiedene Perigon-Datenbanken zugreifen kann. Dies ist vor allem im Personalaustausch oder einem überregional organisierten Nachtdienst hilfreich. Der Anwender kann sich mit dem gleichen Login an mehreren Datenbanken anmelden und hat so Zugriff auf die notwendigen Kundendaten. Welchen Anwendern Sie Zugriff auf Ihre Perigon-Datenbank gewähren, entscheiden weiterhin Sie.

Was ist eine Multifaktor-Authentifizierung (MFA) und wo wird diese bereits verwendet? Was sind die Vorteile?

Unter Multifaktor-Authentifizierung (MFA) versteht man alle Varianten, bei welchen zusätzlich zum Kennwort eine weitere Bestätigung erfasst werden muss. Beispielsweise wird beim Login im E-Banking bereits heute ein zweiter Faktor verlangt. Nachdem der Anwender sein Benutzername und Kennwort eingegeben hat, wird die Bestätigung durch den zweiten Faktor gefordert. Bekannte Formen hierfür sind: SMS-Code, Pushmeldung auf dem Smartphone zum Bestätigen, mTAN oder auch PhotoTAN, Gesichtserkennung im Smartphone, Fingerabdruckleser, FIDO-Sticks usw. Erst wenn auch der zweite Faktor erfolgreich bestätigt werden konnte, erhält der Anwender Zugriff.

Eine Multifaktor-Authentifizierung macht den Login-Vorgang um einiges sicherer. Erbeuten, erraten oder gelangen Unbefugte auf anderen Wegen an ein einzelnes Kennwort, reicht das nicht mehr aus, um sich Zugriff zum System zu verschaffen. Dafür müsste auch der zweite Faktor überlistet werden. Das bedeutet für den Anwender, dass Kennwörter an sich einfacher definiert werden können, sobald ein weiterer Faktor im Login-Vorgang involviert ist. Ein einfacheres Kennwort ist wohl etwas, das sich viele Benutzer wünschen. Die Multifaktor-Authentifizierung muss im Umgang mit sensiblen Daten zum State of the Art werden.

Was versteht man unter Login Delegation?

Bei einer Login Delegation wird nicht durch das Perigon entschieden, ob die Anmeldedaten korrekt sind, sondern ein Anmeldedienst. Solche Anmeldedienste sind beispielsweise HIN, SwissID oder Microsoft Azure.

Wie funktioniert eine Login Delegation?

Haben Sie ihre Benutzerverwaltung vom Perigon auf den Authentication Service migriert, können Sie pro Perigon-Benutzer festlegen, ob sein Login delegiert werden soll oder nicht. Es ist also möglich, dass einige Perigon-Benutzer weiterhin Kennwort und Benutzername beim Perigon Start eingeben müssen und andere über ein delegiertes Login Zugriff erhalten. Wurde einem Anwender

root-service ag
Weinfelderstrasse 32
Postfach 227
CH-8575 Bürglen

Telefon +41 (0)71 634 80 40
E-Mail: info@root.ch
Internet: www.root.ch

eine Delegation hinterlegt, kann er bei der Anmeldung am Perigon wählen, ob er sich mit seinem Perigon Login oder über die hinterlegte Delegation anmelden möchte.

Wählt der Anwender Delegation aus, wird er direkt weitergeleitet und gelangt zum Anmeldedienst, der den Login übernehmen soll. Hier gibt er sein Benutzername und Kennwort für den Anmeldedienst ein. Der Anmeldedienst prüft nun, ob diese Angaben korrekt sind und gewährt oder verweigert den Zugriff. Wird der Zugriff gewährt, kann der Anwender definieren, ob er auf dem gleichen Gerät angemeldet bleiben möchte oder nicht.

Falls der Anwender angemeldet bleiben möchte, muss beim Start eines weiteren Perigons erneut ausgewählt werden, wie man sich anmelden möchte (via Delegation oder mit dem Perigon Login). Wird die Delegation gewählt, muss der Anwender das Kennwort jedoch nicht erneut eingeben. Die Logindaten werden für einen begrenzten Zeitraum auf dem Gerät gespeichert. Hierbei wird nicht das Kennwort gespeichert, sondern nur, dass der Zugriff gewährt wurde. Ist der Zeitraum vom automatischen Zugriff abgelaufen, muss der Anwender seine Logindaten erneut eingeben bei einer Neuanmeldung.

Was ist der Vorteil einer Login Delegation?

Der Vorteil einer Login Delegation ist, dass der Anwender die gleichen Login Daten (Benutzername und Kennwort) verwenden kann für verschiedene Anwendungen. Weiter müssen Sie als Organisationen Ihre Kennwortrichtlinien nicht an mehreren Orten pflegen, sondern können diese im Idealfall nur einmal definieren. Ebenfalls wird bei Logins die Multifaktor-Authentifizierung (MFA) immer wichtiger. Diese Multifaktor-Authentifizierung (MFA) ist bei HIN, SwissID und Microsoft Azure möglich und wäre somit auch für das Perigon verfügbar.

Wieso soll ich als Spitex meine Logins via Perigon Hello durchführen?

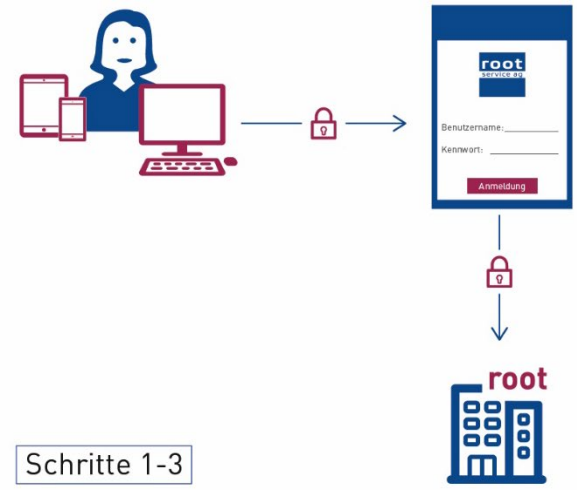
Die Sicherheit der Kundendaten muss Ihnen als Organisation und auch allen Mitarbeitern genauso wichtig sein wie persönliche Logindaten, beispielweise für das E-Banking oder zu Webplattformen von Krankenversicherungen. Mit diesen Logindaten gehen wir bereits sehr vorsichtig um und sichern sie zusätzlich mit einem zweiten Faktor ab. Wir behalten solche Logindaten für uns und geben diese auch einem guten Arbeitskollegen nicht weiter. Genau gleich muss es sich mit den Kennwörtern für das Perigon verhalten. Der Schaden bei Missachtung dieser Sicherheitsmassnahmen kann gross sein und das Vertrauen ihrer Kunden in die Spitex tief erschüttert werden. Aus diesem Grund ist es wichtig, die organisationsinterne Strategie bezüglich Datenschutz und Datensicherheit im Perigon zu überdenken und auf den aktuellen Stand der Technik zu aktualisieren. Wir unterstützen Sie dabei mit Perigon Hello.

root-service ag
Weinfelderstrasse 32
Postfach 227
CH-8575 Bürglen

Telefon +41 (0)71 634 80 40
E-Mail: info@root.ch
Internet: www.root.ch

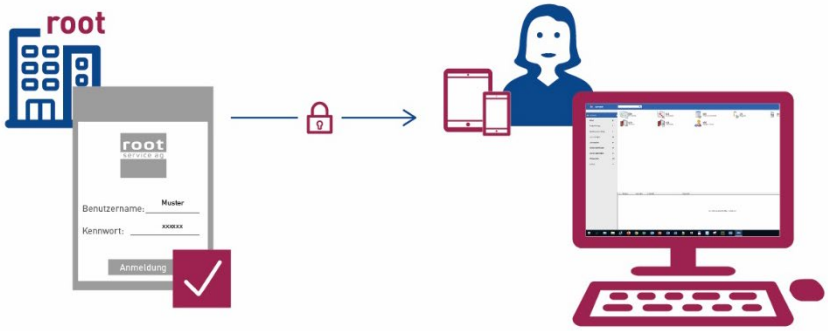
Beispiele für die Anmeldung mit einem Authentication Service

Anmeldung mit root-Authentication Service



Schritte 1-3

Schritt 4



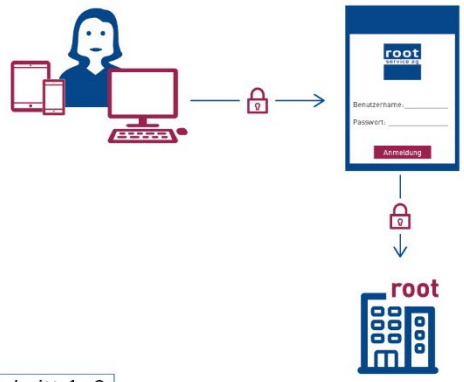
1. Der Benutzer gibt den Benutzernamen und das Kennwort im Perigon Spitex (am PC oder am mobilen Gerät) ein und bestätigt die Eingabe.
2. Benutzernamen und Kennwort werden an den root-Authentication Service gesendet.
3. Der root-Authentication Service prüft den Benutzernamen und das Kennwort.
4. Der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

✓ Der Benutzer ist angemeldet.

root-service ag
Weinfelderstrasse 32
Postfach 227
CH-8575 Bürglen

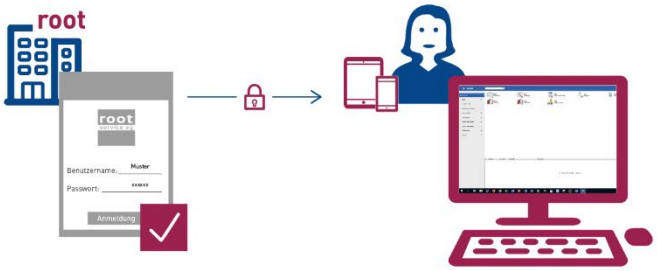
Telefon +41 (0)71 634 80 40
E-Mail: info@root.ch
Internet: www.root.ch

Anmeldung mit root-Authentication Service und Multifaktor-Authentifizierung (MFA)



Schritt 1+2

Schritt 3-7



Schritt 8

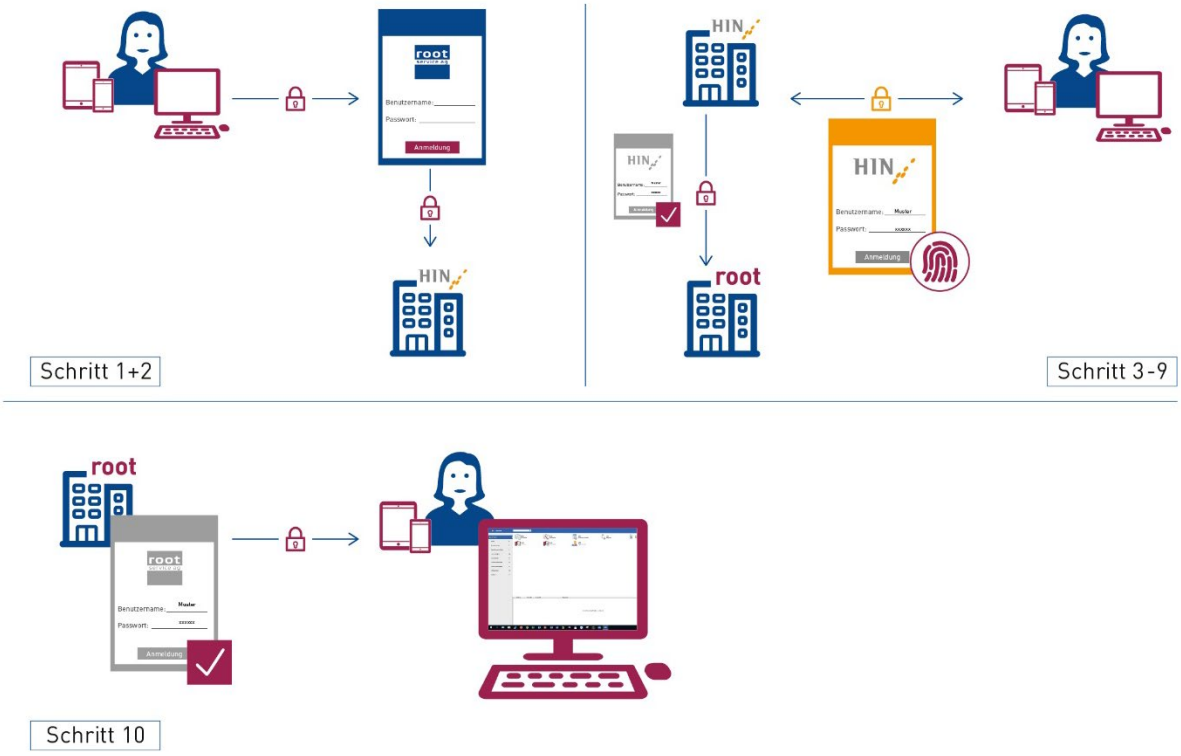
1. Der Benutzer gibt den Benutzernamen und das Kennwort im Perigon Spitex (am PC oder am mobilen Gerät) ein und bestätigt die Eingabe.
2. Benutzernamen und Kennwort werden an den root-Authentication Service gesendet.
3. Der root-Authentication Service prüft den Benutzernamen und das Kennwort.
4. Der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

✓ Der Benutzer ist angemeldet.

root-service ag
Weinfelderstrasse 32
Postfach 227
CH-8575 Bürglen

Telefon +41 (0)71 634 80 40
E-Mail: info@root.ch
Internet: www.root.ch

Anmeldung mit Login Delegation an HIN und mit Multifaktor-Authentifizierung (MFA) durch HIN



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.