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: Technische Übersicht, Perigon Authentication Service (Perigon Hello)	Dokumententyp: Systeminformationen
Dokumentennummer: SI-20211221	Programmversion: ab 2022.1
Ausgabedatum: 21. Dezember 2021	Letzte Aktualisierung: 17. Januar 2022

Systeminformationen

Technische Übersicht, Perigon Authentication Service (Perigon Hello)

Wie funktionierte die Anmeldung bisher am Perigon?

Jede Perigon-Datenbank (SAP SQL Anywhere) verfügte über einen Benutzerstamm. Neben dem Benutzername wurde ein Passworthash gespeichert. Eine Anmeldung an Perigon funktionierte nur mit Perigon Benutzername und Kennwort. Eine Verknüpfung mit einem Windows Benutzer war möglich. Eine Nutzung des Windows Logins war jedoch nur möglich, wenn Perigon Desktop auf einem Windows Rechner in der entsprechenden Domäne mit angemeldetem Benutzer gestartet wurde.

Diese bisherige Lösung erlaubt keine fortgeschrittenen Anmeldeszenarien sowie eine sichere und einfach Vernetzung mit verteilten Systemen.

Was ist Perigon Hello?

Perigon Hello ist ein Authentication Service nach OpenId Connect Standard (OIDC). OIDC ist eine Erweiterung des OAuth2 Standards. Viele bekannte Anmeldedienste wie Microsoft Azure, Google, Facebook, SwissId usw. erfüllen diesen Standard ebenfalls. Die Einhaltung dieses Standards erlaubt die Delegation von einem Anmeldedienst zu einem anderen. Somit wird es möglich sich bei Perigon auch mit einem Microsoft Azure AD Account anzumelden. Auch MFA wird durch Perigon Hello möglich.

Der Anmeldedienst ist genau genommen ein Authorisierungsdienst.
Unter Anmeldung verstehen wir implizit, dass ein Benutzer einen Benutzername und Kennwort wissen muss. Auf Basis dieser Anmeldeinformationen erhält der Benutzer Zugriff für ein bestimmtes System. Genau genommen erhält der Benutzer für diese Informationen einen Authorisierungscode, der in ein Zugriffstoken getauscht wird. Das Zugriffstoken erlaubt den Zugriff auf Daten von Perigon. Es gibt jedoch auch weitere sogenannte Authorisierungsflows. Immer häufiger wird es notwendig, dass Systeme automatisiert Vorgänge erledigen, ohne dass ein Benutzer involviert ist. Solche «Machine to Machine» Szenarien können mit dem neuen Anmeldedienst gezielt authorisiert werden.

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

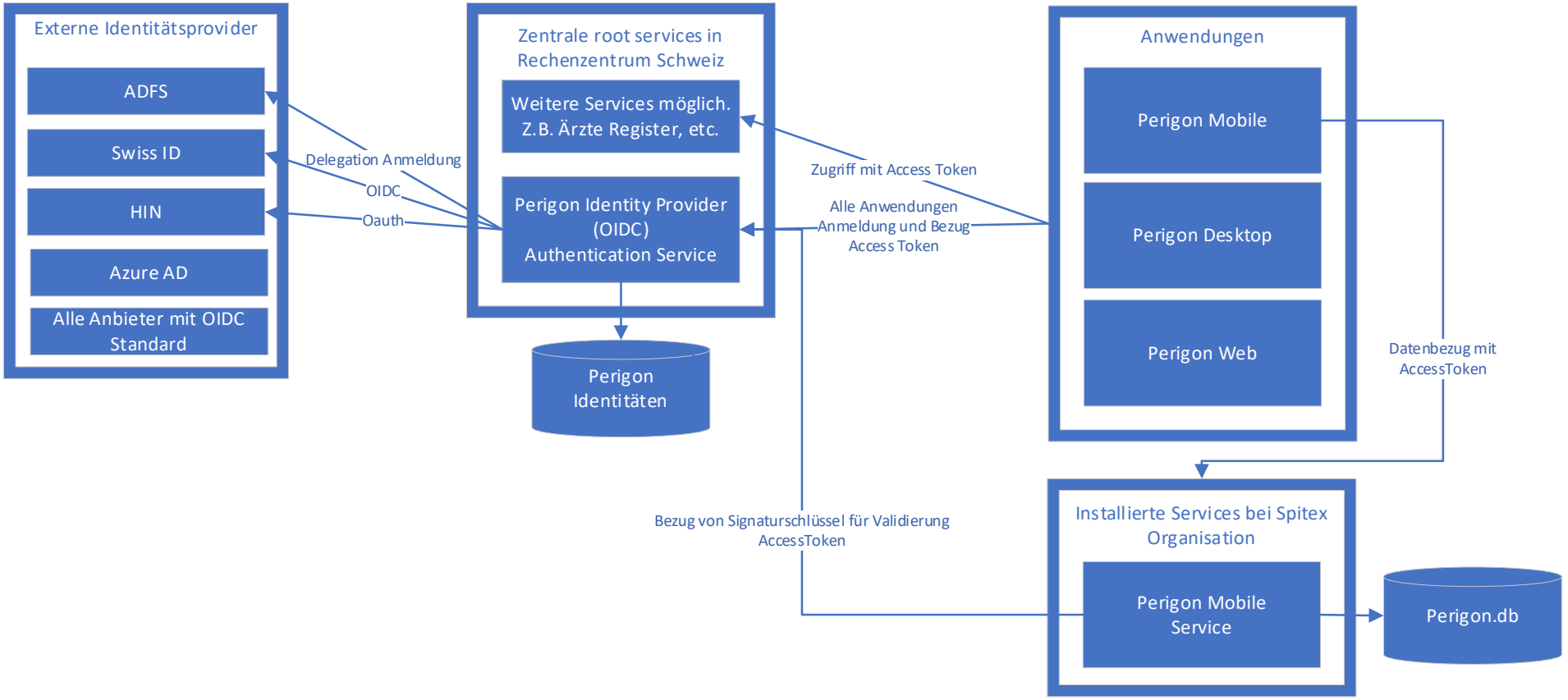
Die neue Perigon Anmeldung ist immer eine Website. Da die Anmeldung nicht mehr nativ in verschiedenen Applikationen separat programmiert ist, wird es möglich, das Perigon Mobile beispielsweise genau gleich von der neuen Anmeldung mit Delegationsmöglichkeit profitieren kann wie das Perigon am PC.

Da der neue Anmeldedienst zentral ist und nicht mehr nur ein Benutzerstamm lokal existiert, werden neue Szenarien zur vernetzten Zusammenarbeit möglich.

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

Schematische Übersicht



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

Datenhaltung

Alle bisherigen Daten und auch Kundenbezogene Daten bleiben weiterhin ausschliesslich in der Perigon SAP SQL Anywhere Datenbank.

Der Anmeldedienst verfügt über eine eigene zentrale Datenbank. Diese wird auf einem Schweizer Rechenzentrum gehostet. Wir sind uns bewusst, wie sensibel eine Schweizer Datenhaltung für unsere Kunden ist.

Folgende Informationen werden zentral in dieser Perigon Identity Datenbank erfasst:

- Organisation
  - Name
  - Kürzel
  - Anmeldedienste-Delegationsinformationen
- Mandanten (von Organisationen)
  - Name
  - Typ (Test, Produktivsystem)
  - Logo
- Benutzer von Organisationen
  - Benutzername
  - E-Mail (optional, für flows notwendig wie Passwordreset)
  - PasswordHash
  - Telefonnummer (optional, für flows notwendig wie Passwordreset)
  - Vor- Nachname
  - Bevorzugte Sprache
  - Status aktiv/passiv
  - Evt. Profilbilder (Stand Okt 2020 noch nicht)
  - Mappinginformation von Perigon Benutzer zu externem Anmeldedienst. Je nach Dienst eine E-Mail-Adresse oder Zeichenkombination.
  - Anmeldehistorie
- Verknüpfung von Benutzer zu Mandanten mit Zugriff bis Datum
- Informationen bezüglich zwei Multifaktor-Authentifizierung
  - Private Schlüssel für TOTP Authenticator oder FIDO Sicherheitsschlüssel
- Berechtigungen in Bezug auf Organisation, Mandant und Benutzer verwalten
- Protokollierung von Veränderungen
- Weitere für den Dienst relevante nicht personenbezogene Daten
  - Kryptografische Schlüssel
  - Ausgestellte Tokens
  - Log Informationen
  - Etc.