



keyon

Die **suisseID** in der Praxis

- ▶ Einführung in die SuisseID
- ▶ SuisseID spezifische Registrierprozesse
- ▶ SuisseID Erfahrungsbericht der VRSG
- ▶ Sicherung von Web Applikationen

V R S G **AIRLOCK**
Vertrauen verbindet. by ergon

Über Keyon **keyon**

information security?

just relax.

plan
implement
enforce
control



keyon for security reasons
www.keyon.ch / info@keyon.ch



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Volkswirtschaftsdepartement EVD
Staatssekretariat für Wirtschaft SECO



SuisselD

Das SuisselD Zertifikat

1. September 2010, Zürich




René G. Eberhard
Dipl. Ö.-Ing. HTL
Betriebswirtschafts-Ing. FH NDS
CEO, Partner

keyon AG
Schlossstrasse 6
8640 Jona
Switzerland
www.keyon.ch

Tel. +41 55 220 64 03
Mobile +41 79 490 00 45
Fax +41 55 220 64 01
eberhard@keyon.ch

3

eberhard@keyon.ch





SuisselD: Kurz-Steckbrief



Die SuisselD ist:

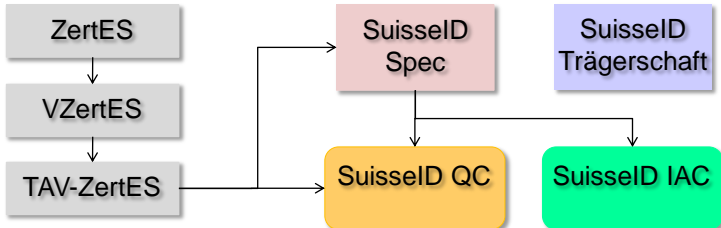
- ein ZertES-konformes **Signatur-Token** mit entsprechendem Signatur-Zertifikat,
mit zusätzlich
- einem standardisierten **Authentisierungs-Zertifikat**,
- einer einmaligen **SuisselD-Nummer**
- und einem **SuisselD-Identity-Provider-Service**
- bereitgestellt von einer nach ZertES **zertifizierten Zertifizierungsdienste-Anbieterin**

4

 **Grundsatz** 

Basis der SuisselD ist die TAV-ZertES



Sofern die technischen und administrativen Bestimmungen der SuisselD keine ergänzenden oder einschränkenden Angaben machen, gelten die Bestimmungen der TAV-ZertES.



```

graph TD
    ZertES[ZertES] --> VZertES[VZertES]
    VZertES --> TAV_ZertES[TAV-ZertES]
    TAV_ZertES --> SuisselD_Spec[SuisselD Spec]
    TAV_ZertES --> SuisselD_QC[SuisselD QC]
    SuisselD_Spec --> SuisselD_QC
    SuisselD_Spec --> SuisselD_IAC[SuisselD IAC]
    SuisselD_Trägerschaft[SuisselD Trägerschaft] --> SuisselD_IAC
  
```

5

 **Grundsatz** 

Die SuisselD Zertifikate sind vertrauenswürdig, weil

- das SuisselD QC gesetzlich geregelt ist
- das SuisselD IAC
 - Die gleiche Benennung der Person hat wie das SuisselD QC
 - Der private Schlüssel sicher, auf dem gleichen Token wie das SuisselD QC, generiert und gespeichert ist

6



Definitionen



Subject DN (Namensgebung)

- Name oder Pseudonym plus
- SuisseID Nummer plus optional
- spezifische Attribute der Inhaberin oder des Inhabers

Der Subject DN eines SuisseID IAC ist immer identisch mit dem Subject DN des korrespondierenden SuisseID QC

SuisseID QC	SuisseID IAC
CN=Hans Muster (Qualified Signature) serialNumber=0001-0000-0000-0001 emailAddress=h.muster@mail.xy	CN=Hans Muster (Authentication), serialNumber=0001-0000-0000-0001, emailAddress=h.muster@mail.xy

7



Definitionen



SuisseID Nummer 1/2


Eine eindeutige, durch den CSP vergebene Nummer, die einem Zertifikatsinhaber zugeordnet ist.

Beispiel: 0001-9384-9341-8453


Zielsetzung

- Eindeutige Zuordnung eines Zertifikats zu einer Person unabhängig von der Lebensdauer des Zertifikats.
- Für die Applikation transparente Erneuerungsprozesse

8

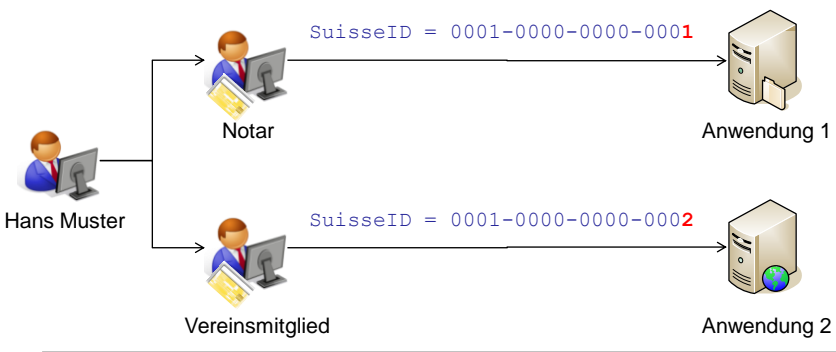


Definitionen



SuisseID Nummer 2/2

Ein Zertifikatsinhaber kann mehrere SuisseID Zertifikate mit unterschiedlichen SuisseID-Nummern beantragen, um diese in unterschiedlichen Kontexten zu nutzen.



9



Definitionen



SuisseID Token

- Das SuisseID QC und das SuisseID IAC befinden sich auf dem **gleichen** Hardware Token.



10

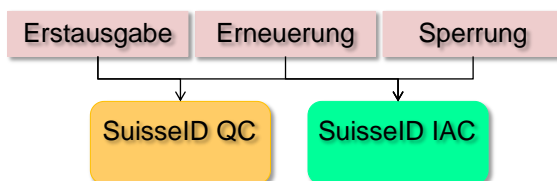


Definitionen / Prozesse



SuisseID Zertifikateset

- Ein SuisseID QC und ein SuisseID IAC, welche jeweils zusammen im Rahmen eines Zertifikatantrags im Bereich der SuisseID ausgegeben werden.
- Alle administrativen Operationen wie z.B. die Erstausgabe, das Sperren und die Erneuerung von SuisseID Zertifikaten, werden immer auf ein SuisseID Zertifikateset angewendet.



11

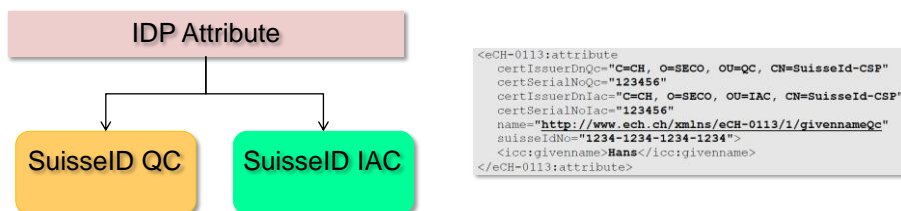


Definitionen / Prozesse



SuisseID Zertifikateset

- Die User-Attribute des IDPs beziehen sich auf das SuisseID QC und das SuisseID IAC. Die IDP Attribute sind von der jeweiligen CA qualifiziert signiert.
- 1:1 Beziehung zwischen den IDP Attributen und dem SuisseID QC / IAC



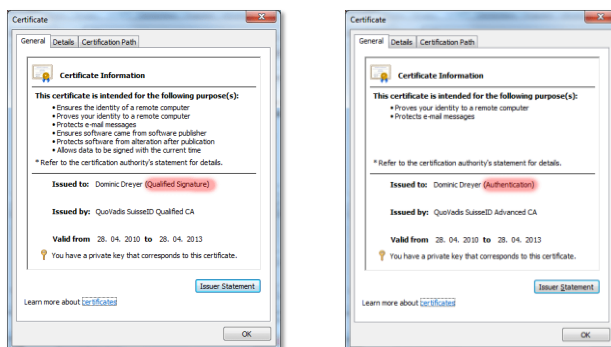
12



Kennzeichnung der SuisseID Zertifikate

Kennzeichnung

- SuisseID qualified certificate
- SuisseID identity & authentication certificate



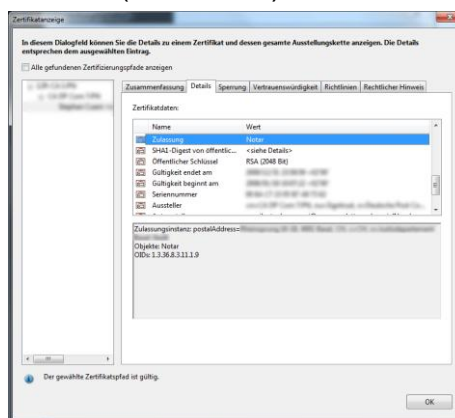
13



Berufszertifikat für Urkundspersonen

Standardisierter Eintrag: Berufliche Befähigung

- Bezeichnung der Urkundsfunktion (z.B. Notar)
- Bezeichnung der bestätigenden Stelle
- Verweis auf den Eintrag im Register der Urkundspersonen
- Unterstützt von gängigen Applikationen



14



Windows Logon




Weltweit eindeutiger Microsoft UPN

- UPN := SuisseID-Nr@upn.suisseid.ch
Der Fokus war
- SECO Whitepaper
SuisseID Smart Card Logon
Configuration Guide




15





SuisseID look and feel

SuisseID Enabling von Web Applikationen mit Airlock

SuisseID spezifische Registrierprozesse und Anwendungsfälle

keyon



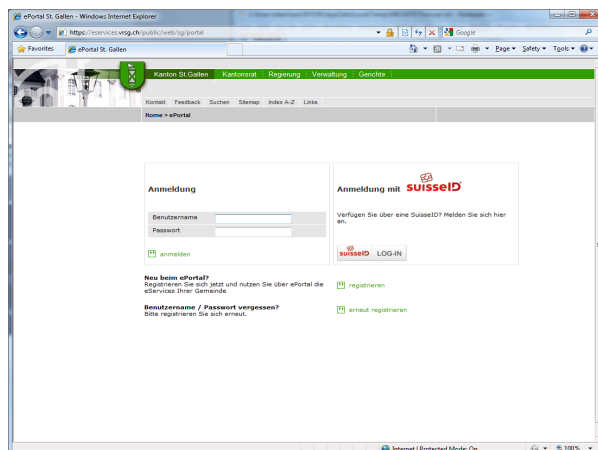
Live Demo

<https://suisseid.keyon.ch>

keyon

Beispiel SuisseID Enabling – look and feel

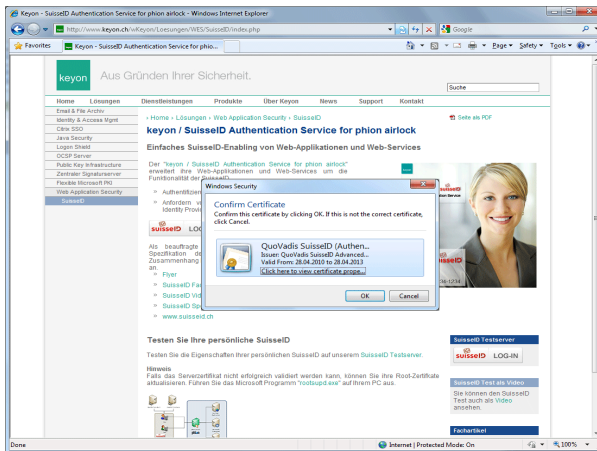
Beispiel Login (Username / Passwort oder SuisseID)

Verwaltungsrechenzentrum AG St.Gallen (VRSG), www.vrsg.ch



Beispiel SuisseID Enabling – look and feel

Beispiel SuisseID Login

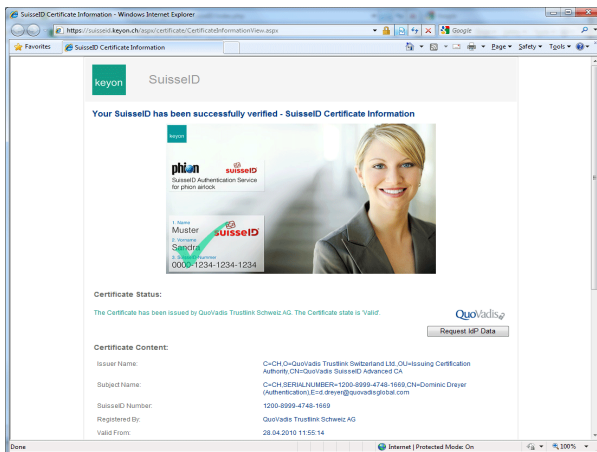


keyon – SuisseID Testserver, <https://suisseid.keyon.ch>



Beispiel SuisseID Enabling – look and feel

Beispiel SuisseID Login - Success

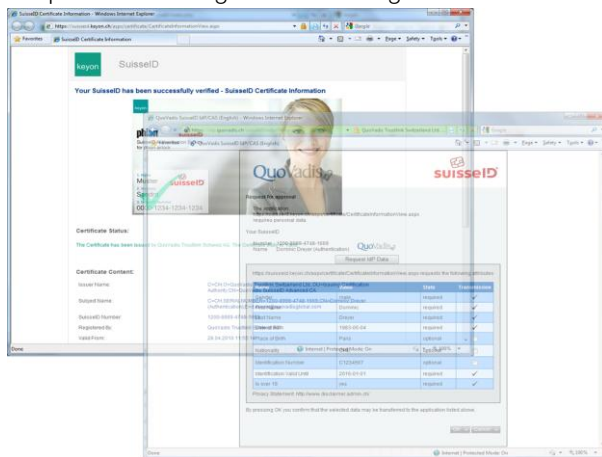


keyon – SuisseID Testserver, <https://suisseid.keyon.ch>



Beispiel SuisseID Enabling – look and feel

Beispiel SuisseID Login mit IDP Anfrage

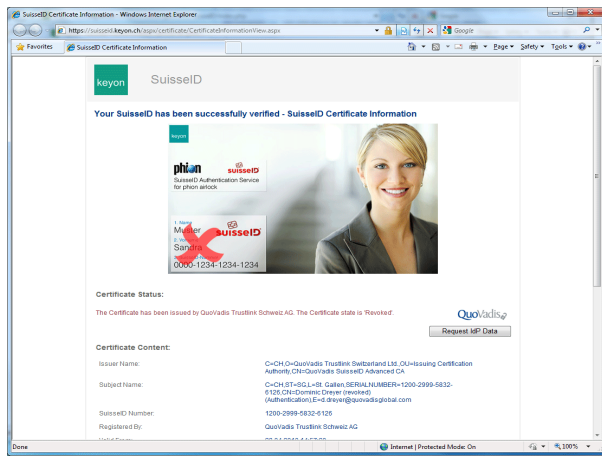


keyon – SuisseID Testserver, <https://suisseid.keyon.ch>



Beispiel SuisseID Enabling – look and feel

Beispiel SuisseID Login – Revoked

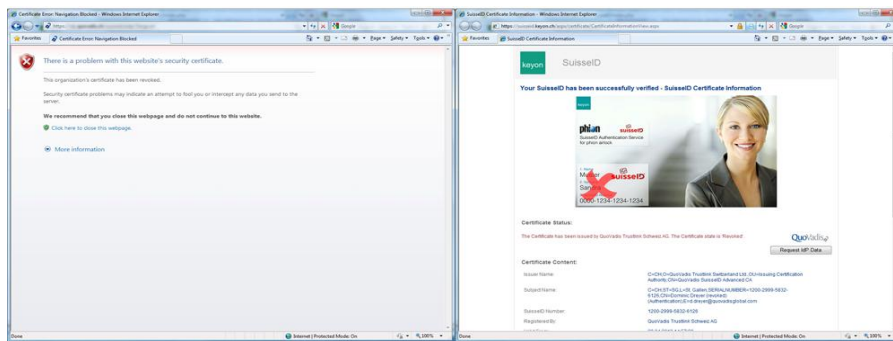


keyon – SuisseID Testserver, <https://suisseid.keyon.ch>

Beispiel SuisseID Enabling – look and feel

keyon

Benutzerfreundliche Fehlermeldungen



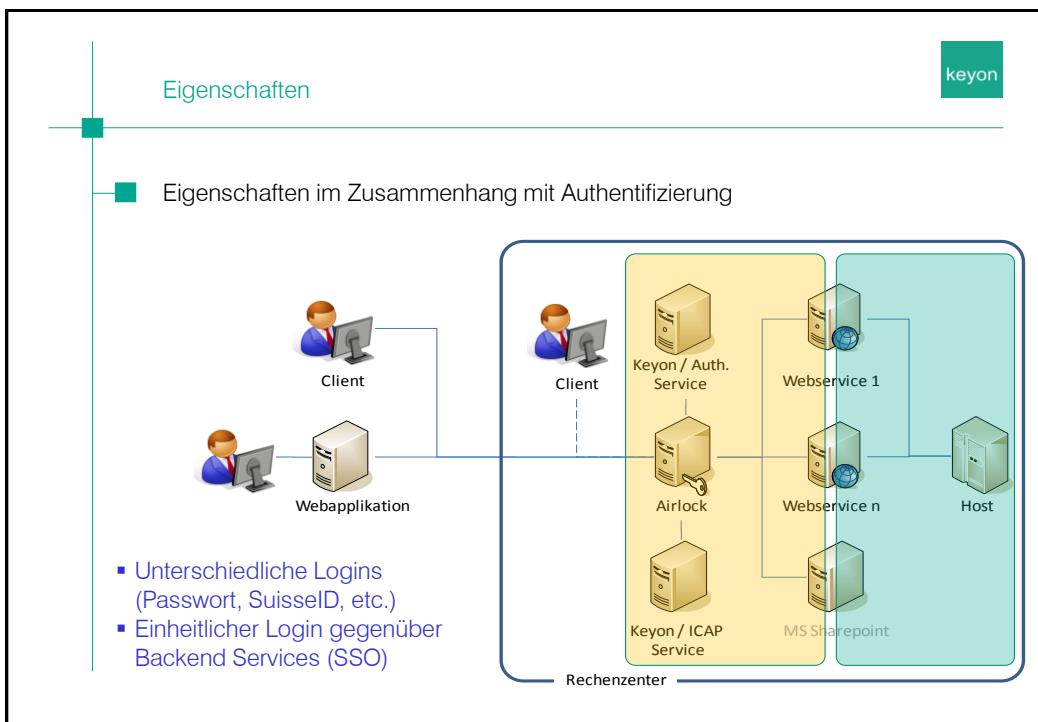
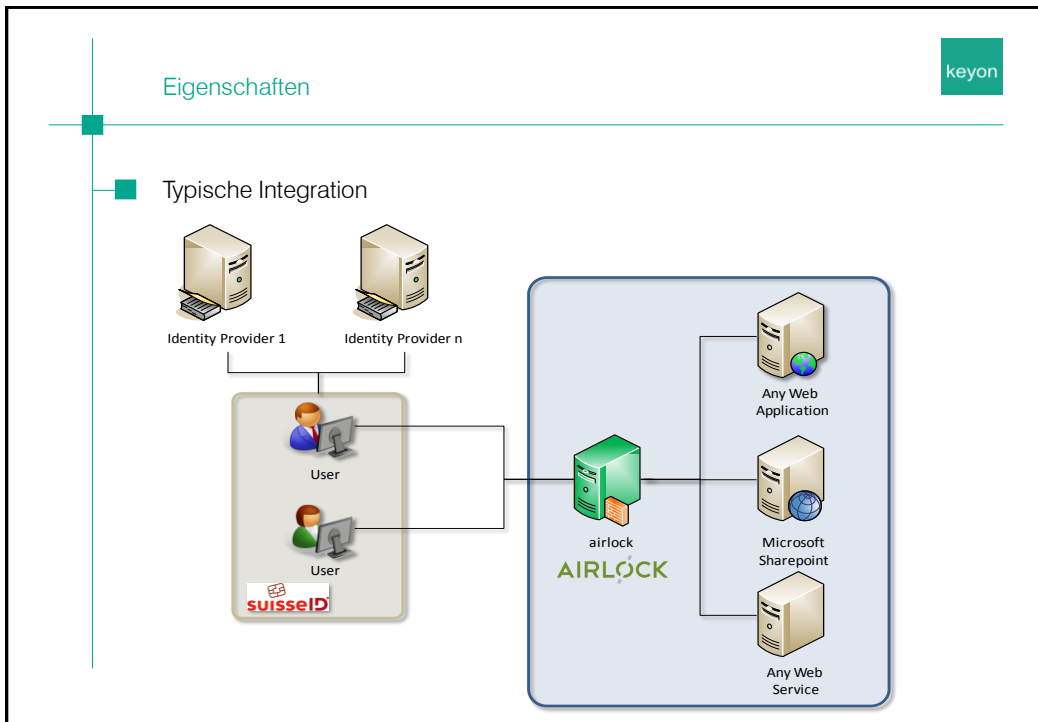
Reduktion der Supportkosten

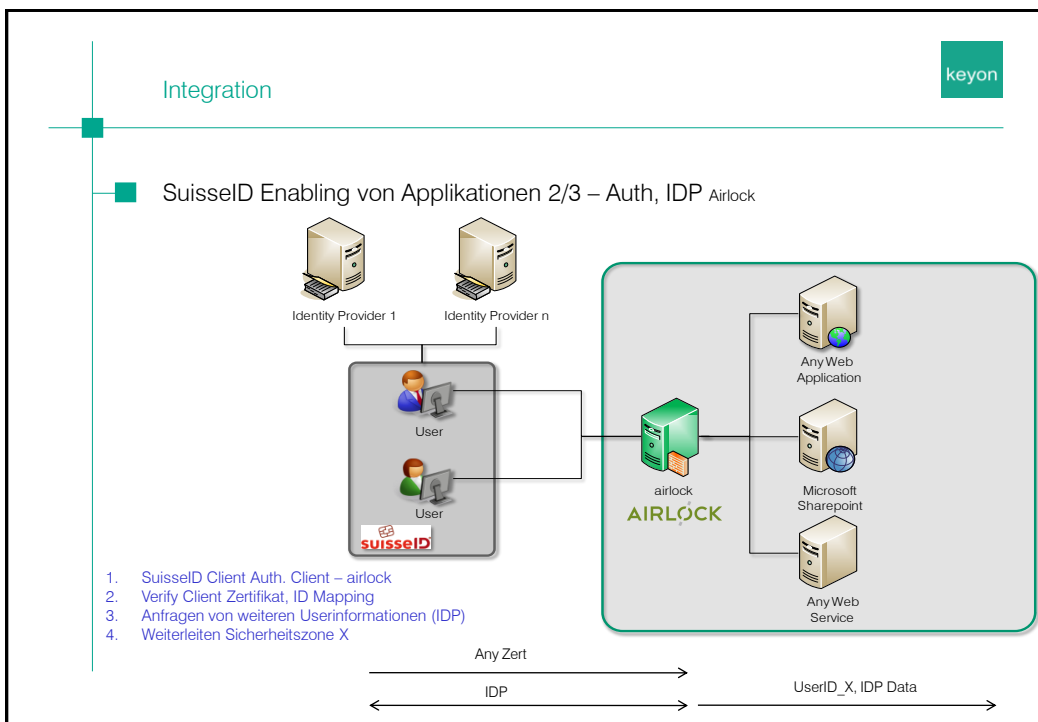
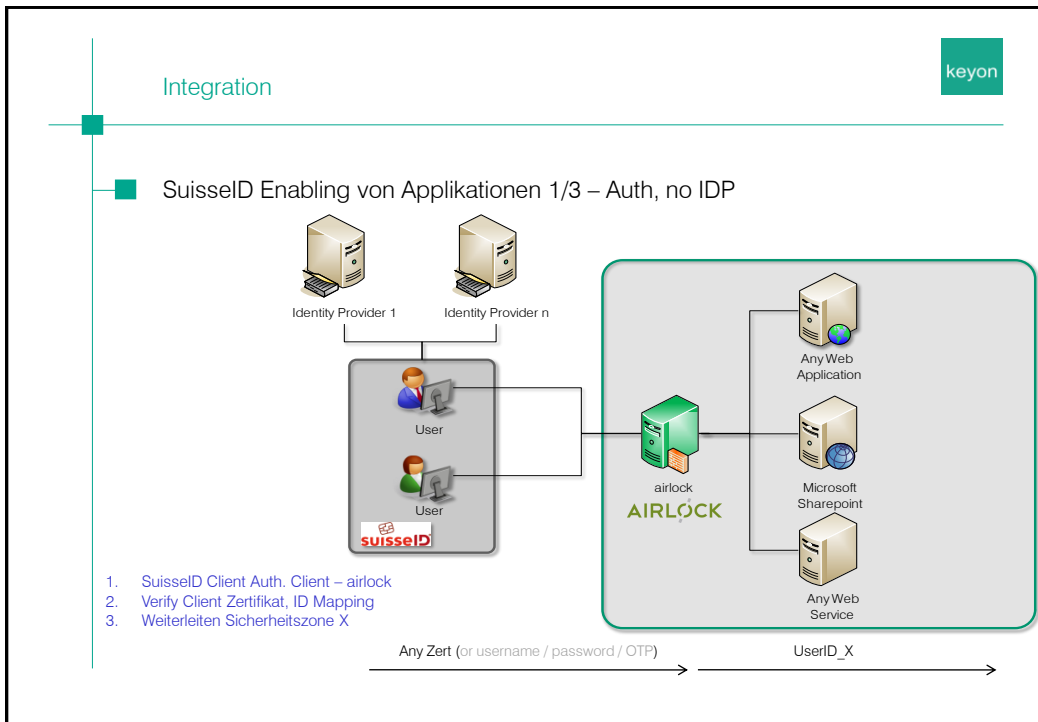
keyon

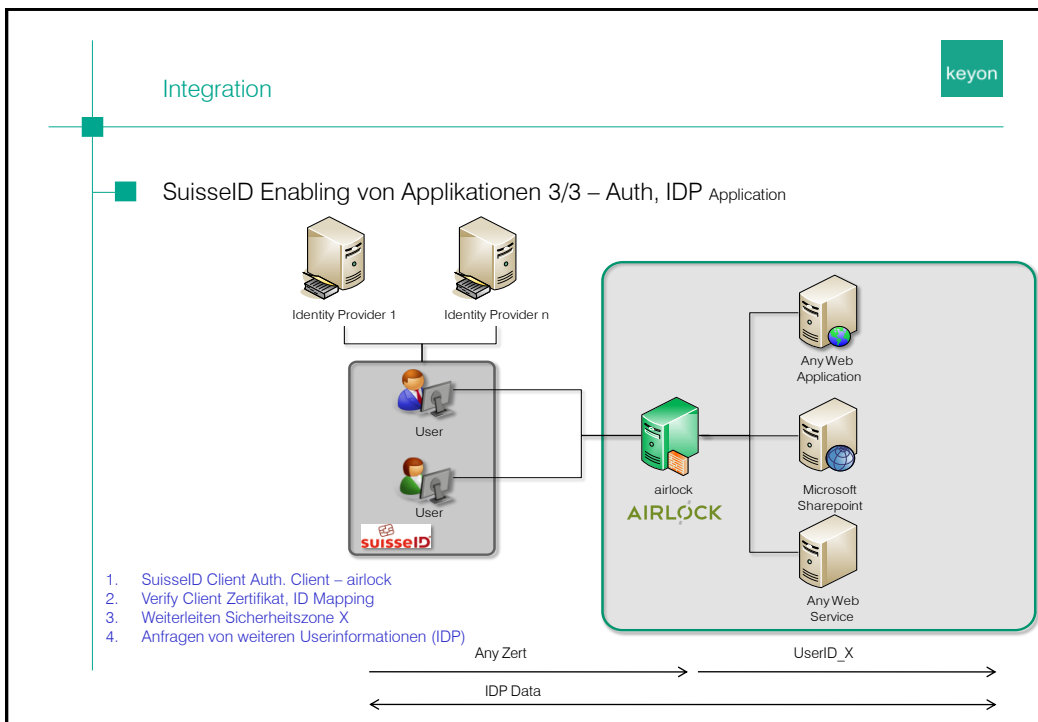
SuisseID look and feel

SuisseID Enabling von Web Applikationen mit Airlock

SuisseID spezifische Registrierprozesse und Anwendungsfälle







keyon

SuisseID look and feel

SuisseID Enabling von Web Applikationen mit Airlock

SuisseID spezifische Registrierprozesse und Anwendungsfälle

Registrierung – Rekapitulation

keyon

Definitionen

Subject DN (Namensgebung)

- Name oder Pseudonym plus
- SuisseID Nummer plus optional
- spezifische Attribute der Inhaberin oder des Inhabers

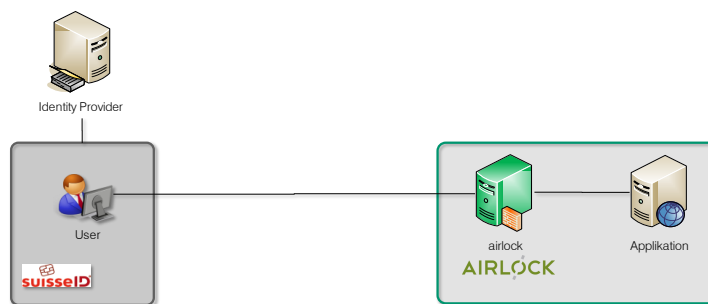
Der Subject DN eines SuisseID IAC ist immer identisch mit dem Subject DN des korrespondierenden SuisseID QC

SuisseID QC	SuisseID IAC
CN=Hans Muster (Qualified Signature) serialNumber=0001-0000-0000-0001 emailAddress=h.muster@mail.xy	CN=Hans Muster (Authentication), serialNumber=0001-0000-0000-0001, emailAddress=h.muster@mail.xy

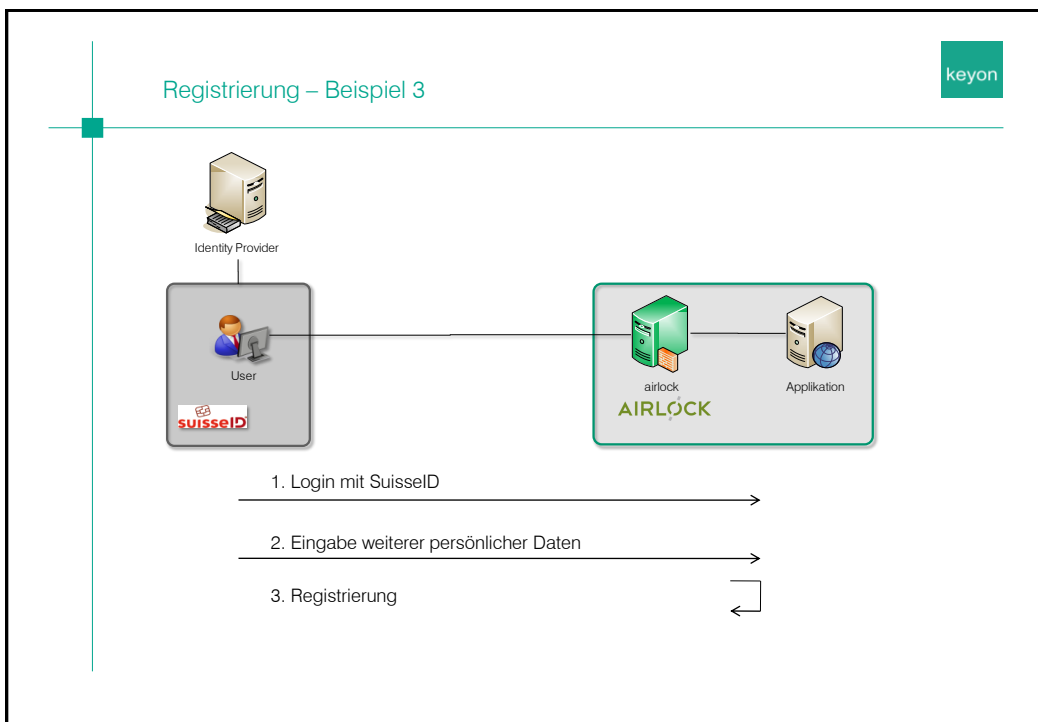
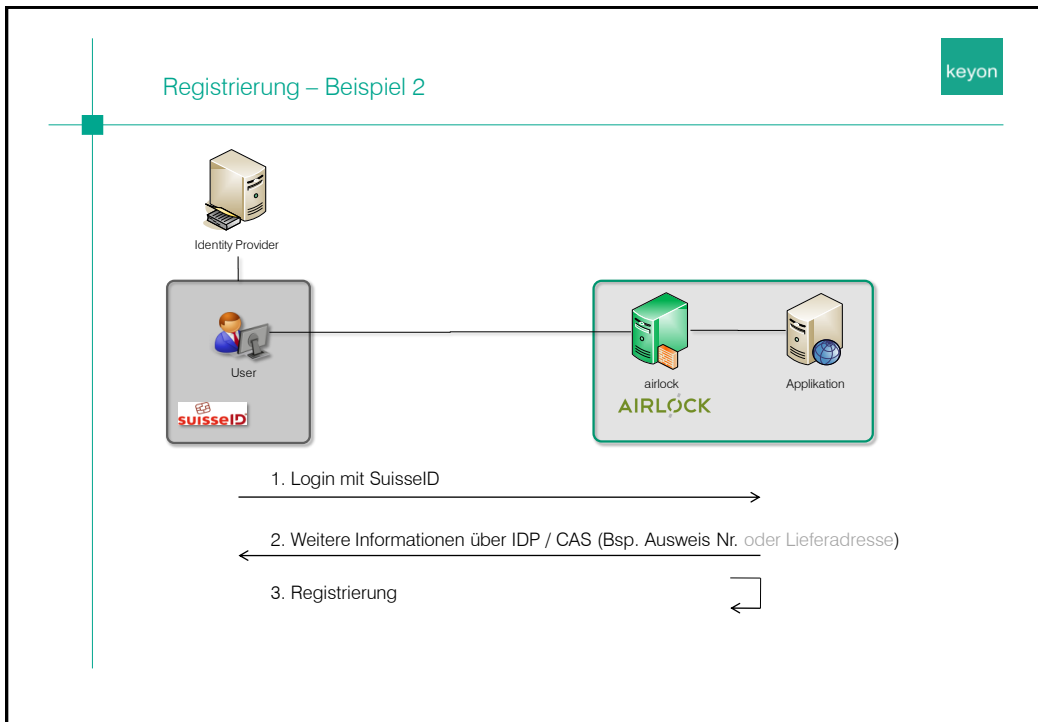
Zuordnung eines konkreten Benutzers zu einer SuisseID

Registrierung – Beispiel 1

keyon

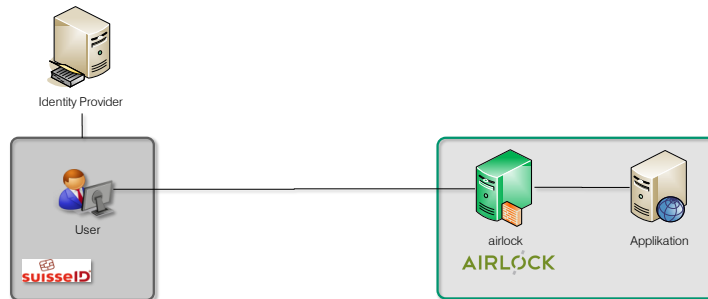


1. Schriftlicher Antrag mit SuisseID Nr., Ausweis Kopie, etc. →
2. Registrierung →
3. Information bez. erfolgter Registrierung ←
4. Login mit SuisseID →



Registrierung – Beispiel 4

keyon



1. Registrierung 1
2. Brief mit spezifischer ID
3. Login mit SuisseID und spezifischer ID
4. SuisseID an spezifische ID / Person Zuordnen
5. Brief mit Challenge (Sichere Bestätigung der Registrierung)
6. Login mit SuisseID und Challenge vom Brief aus Punkt 5.

Vielen Dank für Ihre Aufmerksamkeit

keyon

Bei Fragen stehen ich Ihnen gerne zur Verfügung.



eberhard@keyon.ch

keyon

Aus Gründen Ihrer Sicherheit