Herbsttagung 2021
Elektronische Ausweise

Stephan Verbücheln
Zürich, 8. September 2021

cnlab

Agenda_

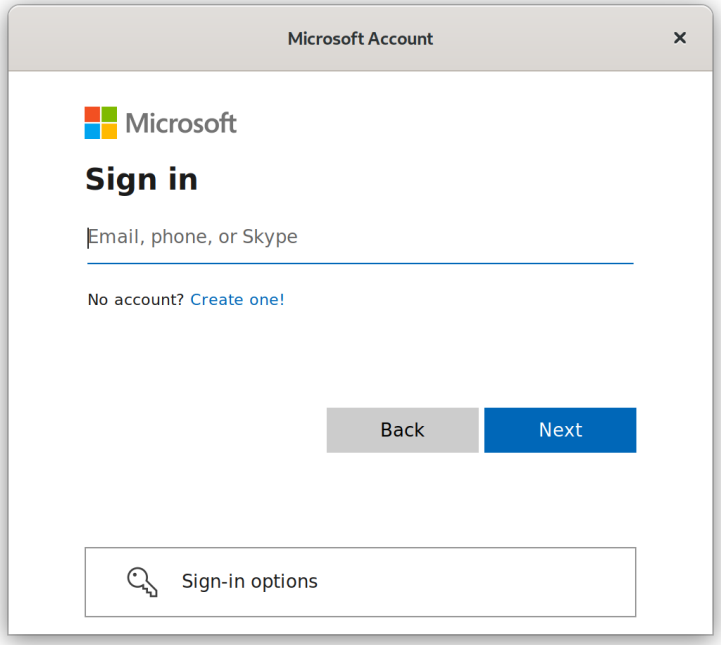
Föderationen

Zertifikate

Chipkarten

Föderationen

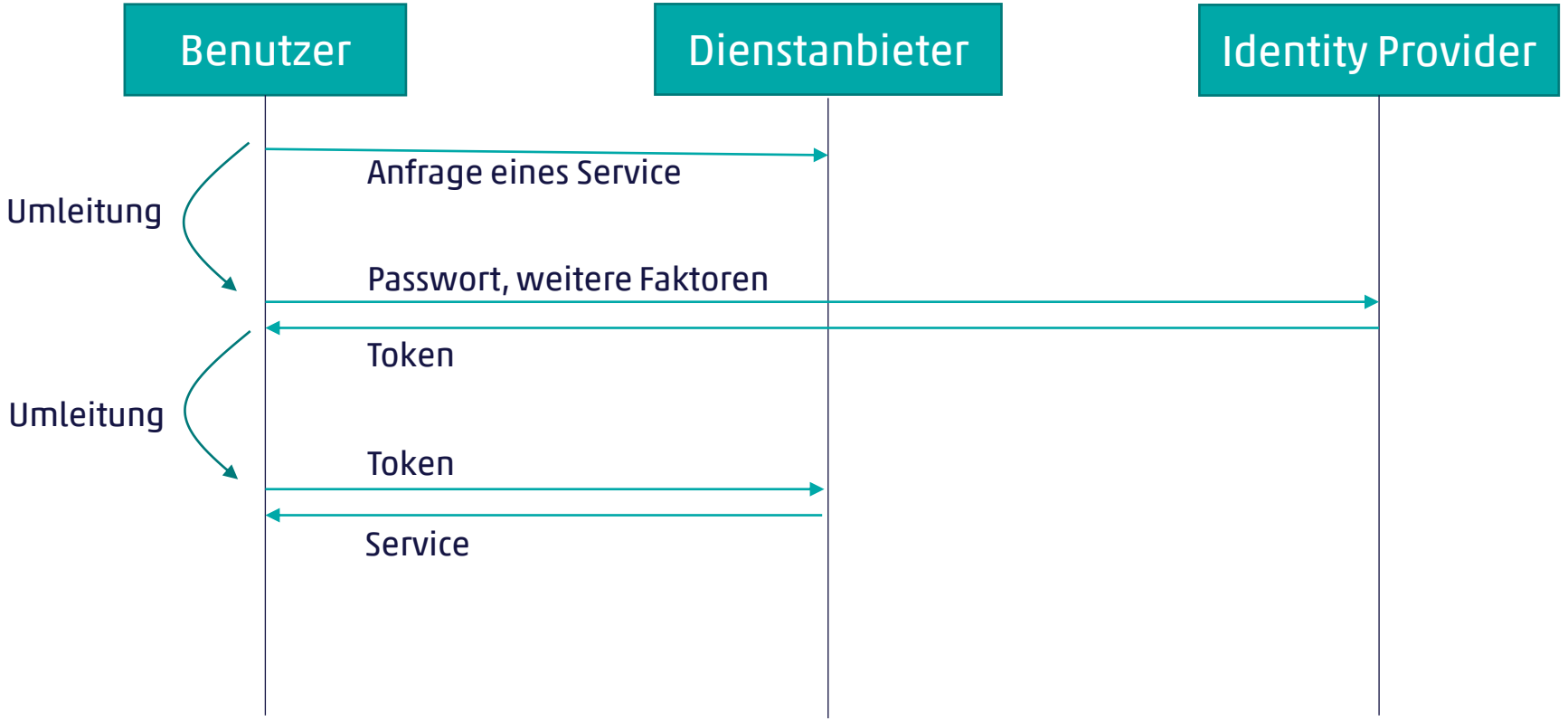
- Web-basierte Authentisierung
- Benutzer authentisiert sich bei seinem Identity Provider
- Identity Provider stellt ein Token für den Dienstanbieter aus



Standards

- SAML, OAuth2, OpenID Connect

Föderationen: Funktionsweise



Föderationen: Google, Facebook und Co.

Facebook

- Zugriff auf Identifikationsmerkmale (Name, E-Mail, ...)
- Zugriff auf Daten (Profilbild, Bilder, ...) durch andere Anwendungen

Google

- Zugriff auf Identifikationsmerkmale (Name, E-Mail, ...)
- Zugriff auf Daten (Mail, Docs, Drive, ...)

Föderationen: SwissID

Fokus auf Identität

- Verifizierte Identifikationsmerkmale (Name, Geburtsdatum, …)
- Weitere Identifikationsmerkmale (E-Mail, …)

Dies sollte mit dem eID-Gesetz zum gesetzlichen Standard werden.

Föderationen: Nachteile

Dem Identity Provider muss absolut vertraut werden:

- Er muss die Daten bei Registrierung korrekt prüfen
- Er muss die Authentisierung korrekt prüfen
- Er kann jederzeit falsche Token ausstellen

Ähnlichkeit zu bekannten Methoden:

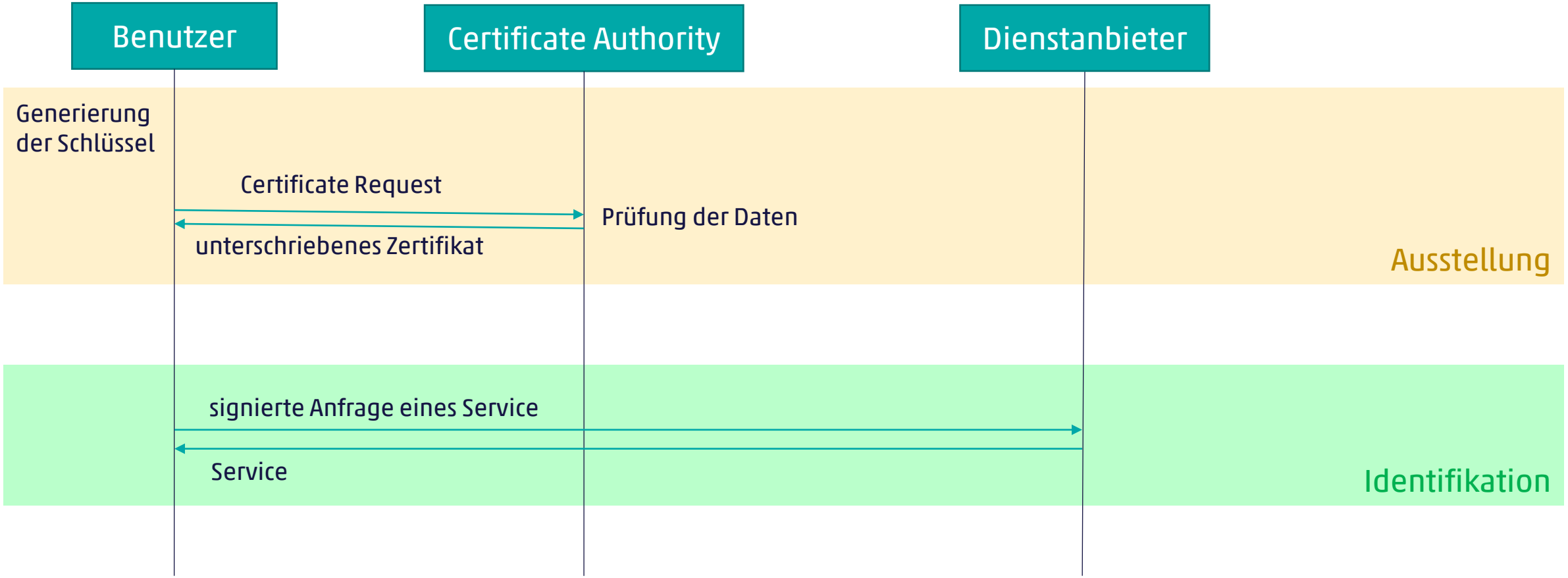
- PostIdent

Zertifikate

- Zertifikate binden Daten an einen öffentlichen Schlüssel
- Nur der Benutzer hat den geheimen Schlüssel des Zertifikats
- Mit diesem kann der Benutzer beweisen, dass er Inhaber ist

- Typische Anwendungen:
  - Verbindungen zwischen Clients und Servern
  - Verschlüsselung von Mails
  - Signierung von Mails, Dokumenten, Software, Git-Commits, usw.

Zertifikate: Funktionsweise



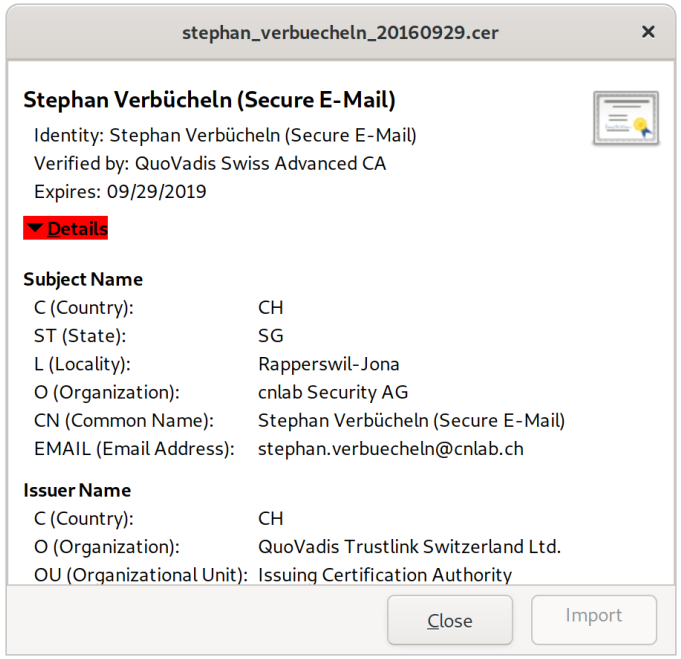
Zertifikate: Public CAs, PGP

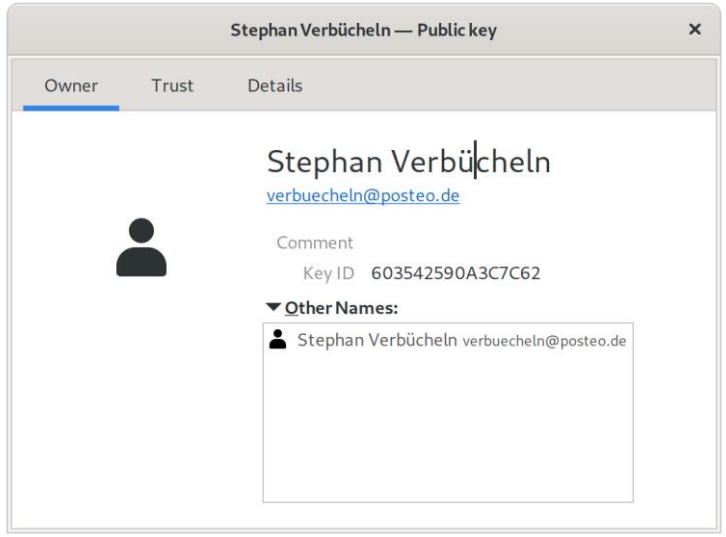
X.509-Zertifikate

- X.509-Zertifikate sind von einer CA unterschrieben
- Liste akzeptierter CAs werden von Betriebssystemen und Anwendungen definiert

PGP

- PGP-Nutzer unterschreiben sich gegenseitig
- PGP-Zertifikat werden vom Nutzer oder von Dritten transitiv unterschrieben (Web of Trust)

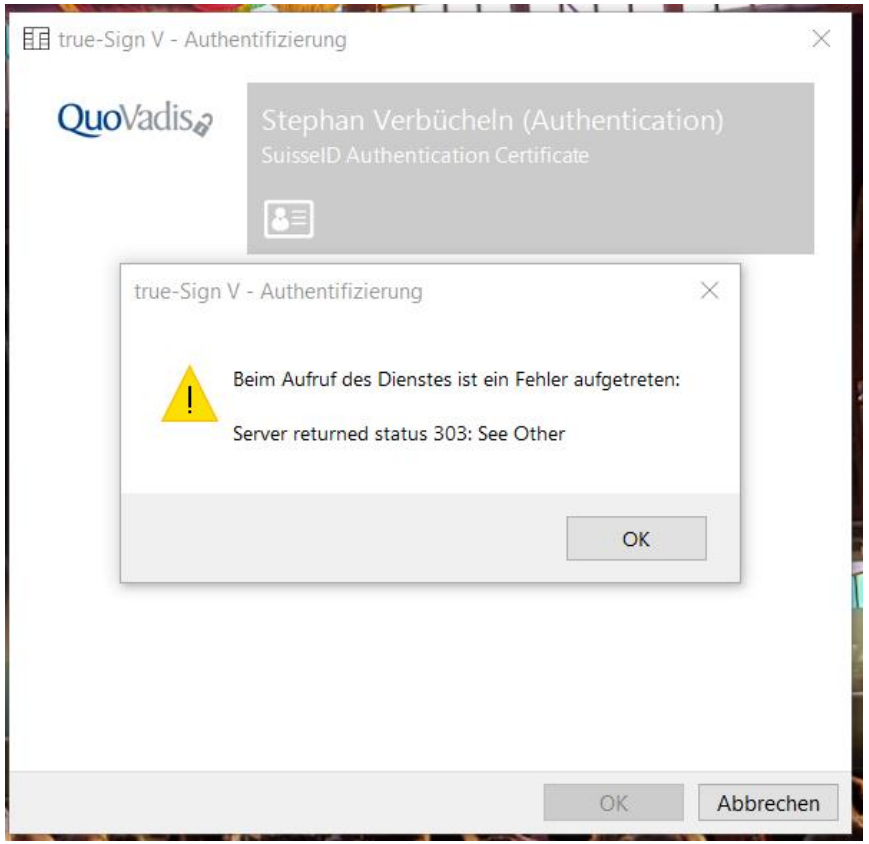




Zertifikate: SuisseID

Offizielles Zertifikat mit verifizierten Informationen

- Erlaubt Ausweisen und Unterschreiben von Dokumenten
- Als Hardwaretoken mit Chipkarte oder Signing Service
- Stirbt aufgrund der geringen Verbreitung aus



Zertifikate: Nachteile

Zertifikate sind lange gültig und müssen gut geschützt werden.

Revocation ist aufwendig und unzuverlässig.

Chipkarten (auch: Smartcards)

Eine Chipkarte ist ein kleiner Rechner:

- Kryptographie wird auf der Chipkarte ausgeführt
- Geheime Schlüssel bleiben dabei auf der Karte

Beispiele:

- Kreditkarten mit Chip, SIM-Karten, SuisseID
- TPMs, Secure Enclave, USB-Tokens

Chipkarten: Zertifikate

Chipkarten können zur Speicherung von Zertifikaten verwendet werden

- Beispiel: SuisseID mit USB-Token
- Anwendung ähnlich wie mit Softwarezertifikat
- Statt Passphrase wird PIN verwendet

Chipkarten: elektronischer Pass

- Elektronischer Pass enthält Mechanismen, um Echtheit zu prüfen
  - modifizierte Angaben
  - falsches Foto

- Elektronischer Pass weist **nicht** nach, dass man Inhaber ist
  - Vergleich des Fotos notwendig

Chipkarten: elektronischer Ausweis

- Mit dem elektronischen Ausweis kann der Benutzer sich ausweisen
- Die Echtheit des Ausweises ist überprüfbar
- Die Identität des Benutzers wird durch eine geheime PIN garantiert
- Der Ausweis kann interaktiv arbeiten
  - Vermeidung signierter Datensätze für Händler

Chipkarten: Nachteile

- Aufwand für den Nutzer
- Kartenlesegerät wird benötigt
  - Smartphone mit NFC möglich
- Aufwand bei Verlust der PIN
- Inhaber kann Chipkarte mit PIN unerlaubt weitergeben

nPA: Elektronischer Ausweis in Deutschland

- Elektronische Funktionen über NFC
- Jeder Personal- und Ausländerausweis in D hat die Funktion
- Bezüglich Sicherheit und Privatsphäre sehr durchdacht
  - PIN identifiziert Inhaber und schützt Daten
  - Nutzung von Pseudonymen
  - Alterskontrolle ohne Geburtsdatum

nPA: Beispiel

Benutzer will ein Videospiel kaufen, das nicht jugendfrei ist.

Welche Daten braucht der Dienstanbieter?

- Name?
- Wohnadresse?
- Geburtsdatum?

Was braucht er wirklich?

- Die Information, ob der Benutzer vor dem 8. September 2003 geboren ist.
- Ggf. ein Pseudonym, um den Benutzer wiederzuerkennen.

nPA: Verbreitung in Deutschland

Trotz der Verbreitung wird die Funktion in Deutschland wenig eingesetzt

- Lesegerät am PC aufwendig
  - Smartphones mit NFC anfangs nicht verbreitet
- Henne-Ei-Problem?
  - PIN vergessen?

Kritik

- Nutzen Händler die Funktion datensparsam?
- Wer will Software von der Regierung installieren?

Fazit

- Eigentlich gibt es schon alles, was man haben will, seit den 90ern.
- Aufgrund der geringen Akzeptanz werden zunehmend schlechtere Lösungen präsentiert.
  - Videoidentifikation statt Kryptographie
  - Föderationen statt Zertifikate
  - Smartphone statt Chipkarte
- Welche Variante am Ende Akzeptanz findet, lässt sich schwer sagen.

Vielen Dank für Ihre Aufmerksamkeit_

Stephan Verbücheln
stephan.verbuecheln@cnlab.ch
+41 55 214 33 36

info@cnlab-security.ch
+41 55 214 33 33

cnlab security AG
Obere Bahnhofstrasse 32b
CH-8640 Rapperswil-Jona
Switzerland

cnlab