Identität gewährleisten – private Daten schützen

Starke Authentisierung mit privacyIDEA

Datenspuren, 13.09.14, Dresden

Cornelius Kölbel
cornelius@privacyidea.org

Identität - Wikipedia

Bergriffsklärung Wikipedia:

- **Identität**, die Eigentümlichkeit eines Wesens
- Die Eigenschaften einer Person, die der Identitätsfeststellung dienen
- kulturelle Identität von Gruppen (z. B. Gemeinschaften oder Gesellschaften)
- In der Mathematik: Identitätsgleichung, eine Gleichung, die für alle möglichen Parameterwerte erfüllt ist
- Identität (Logik), das Prinzip der Ununterscheidbarkeit
- Identität (Pharmazie), ein Nachweis zur zulassungskonformen Qualität eines Arzneistoffs

https://de.wikipedia.org/wiki/Identität_(Begriffsklärung), 11.09.2014

Identität - Wikipedia

Identität (lateinisch īdem ‚derselbe‘, ĭdem ‚dasselbe‘) ist die Gesamtheit der eine Entität, einen Gegenstand oder ein Objekt kennzeichnenden und als Individuum von allen anderen unterscheidenden Eigentümlichkeiten.

https://de.wikipedia.org/wiki/Identität, 11.09.2014

Identität - Print

Identität, [lat. zu idem „derselbe“], allg. vollkommene Gleichheit oder Übereinstimmung (in Bezug auf Dinge oder Personen); v.a. durch Schriftstücke nachzuweisende Echtheit einer Person **(Identitätspapiere)**.

Meyers großes Taschenlexikon, 5. Auflage, 1995

Identität - Print

Identität, die; (völlige Gleichheit)

Duden, 20. Auflage, 1991

Identität feststellen

- Cornelius Mensch

- Cornelius Account

```
(virtual)cornelius@puckel ~/02_Projekte/01_Messe/Datenspuren_2014 %
```

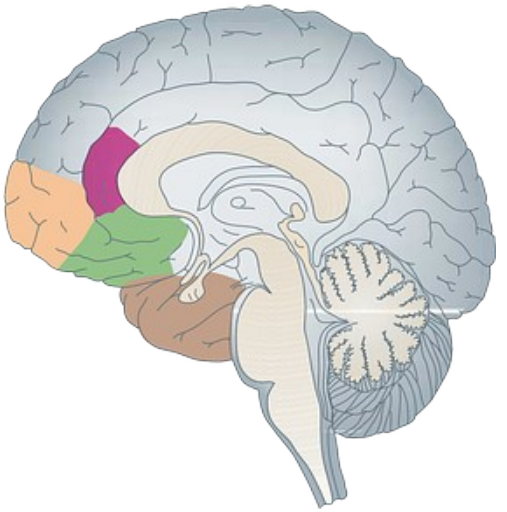
Starke Authentisierung
Zwei-Faktor-Authentisierung

Kombination aus mehreren Faktoren:

- Wissen, das nur ich weiß...
- Besitz, den nur ich habe...
- Eigenschaften, die nur ich habe...

Faktor: Wissen

- Passwort
- Passphrase
- Sicherheitsfragen



- Funktioniert bei dem Account Cornelius

```
(virtual)cornelius@puckel ~/02_Projekte/01_Messe/Datenspuren_2014 %
```

Faktor: Besitz

- SSH Key
- Client Zertifikat
- OTP Token
- Smartcard
- Smartphone...

- Funktioniert bei dem Account Cornelius

```
(virtual)cornelius@puckel ~/02_Projekte/01_Messe/Datenspuren_2014 %
```

Aspekt - Besitz

Besitz wird i.d.R. durch einen geheimen/privaten kryptografischen Schlüssel abgebildet:

- Einzigartigkeit
  - Wo wurde er erzeugt?
- Kopierbarkeit
  - Wie wird er geschützt?

Faktor: Eigenschaft

- Fingerabdruck
- Stimme
- Retina
- Tippverhalten (continuous authentication)
- Gang
- Funktioniert bei dem Mensch Cornelius

Next Level Authentication

International Journal of Engineering Trends and Technology (IJETT) – Volume 11 Number 5 - May 2014

ATM Client Authentication System Using Biometric Identifier & OTP

Jaydeep Shamdasani[#1], Prof. Pravin Matte[*2]

#M.E., Department of E & TC, G.H. Raisoni COE,Wagholi, Pune University, Pune ,Maharashtra, India.
#HOD, Department of E & TC, G.H. Raisoni COE,Wagholi, Pune University, Pune ,Maharashtra, India.

***Abstract*— In this paper we propose a design, to add more security to the current ATM systems by using biometric and GSM technology. In conventional method identification is done based on ID cards and static 4 digit password. Whereas in our purposed system, Bankers will collect the customer fingerprints and mobile number at the time of opening the accounts then only customer will be able to access ATM machine. The primary step of this project is to verify currently scanned fingerprint with the fingerprint which is registered in the bank during the account opening time. If the two fingerprints get matched, then a message will be delivered to the user's mobile which is the random 4 digit pin number to access the account. For every transaction new pin numbers will be send to the user's mobile thus there will not be fixed pin number for every transaction. Thus, Pin number will vary during each transaction.**

Keywords*— *ATM Terminal, Fingerprint Recognition, GSM Module, LINUX.

I. INTRODUCTION

The Modern banking technology has altered the way banking activities are usually done. One banking technology that has impacted to banking activities is the automated teller machine (ATM). Due to ATM technology, a customer is able to perform different banking activities such as cash withdrawal, transferring money, paying phone bills and discussions on the results and conclusion.

II. KEY COMPONENTS OF SYSTEM

The proposed ATM client authentication system depends on fingerprint recognition which is developed after analysing existing ATM systems. The ARM 9 microcontroller (Friendly ARM) is used as the brain of these embedded systems along with fingerprint recognition module and GSM Module.

The primary components are shown as follows:

ARM 9 Microcontroller: It is the central controlling unit of the system. It controls all the peripherals.

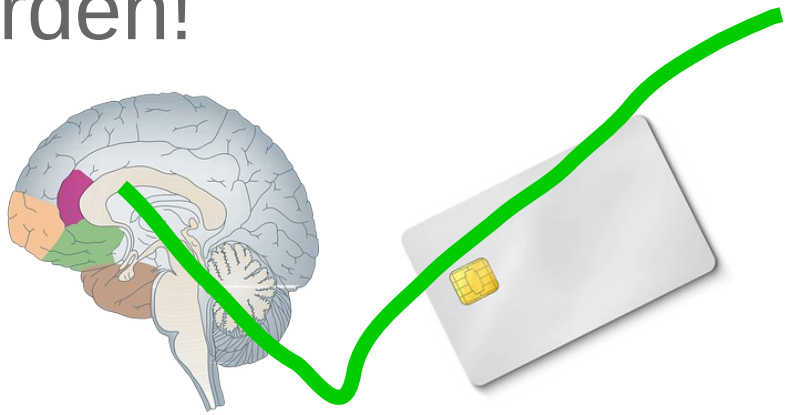
Fingerprint recognition Module: The user's fingerprint was used as the standards of identification. It must verify the feature of the customer fingerprint before using ATM terminal.

GSM Module: It sends different 4-digit code as message to the registered mobile number of the customer for accessing the ATM.

Identität?

- Nutzung von biometrischen Eigenschaften scheint für die Identität eines Accounts wenig geeignet!

- Faktoren Wissen und Besitz sollten weiterhin kombiniert werden!



Privat? Cloudservices!

Cloudservices für die Identitätsentscheidung nicht nur für Privatanwender sondern auch für Geschäftskunden...

XXX Authentication Service

salesforce

Sign in with Google

Privat?

- Durch Cloudservices wandert auch die Identitätsentscheidung in die Cloud
- Somit auch der Zugang zu
    - Privaten Diensten, die nicht in der Cloud liegen
    - Privaten Daten, die nicht in der Cloud liegen


privacyIDEA

privacyIDEA

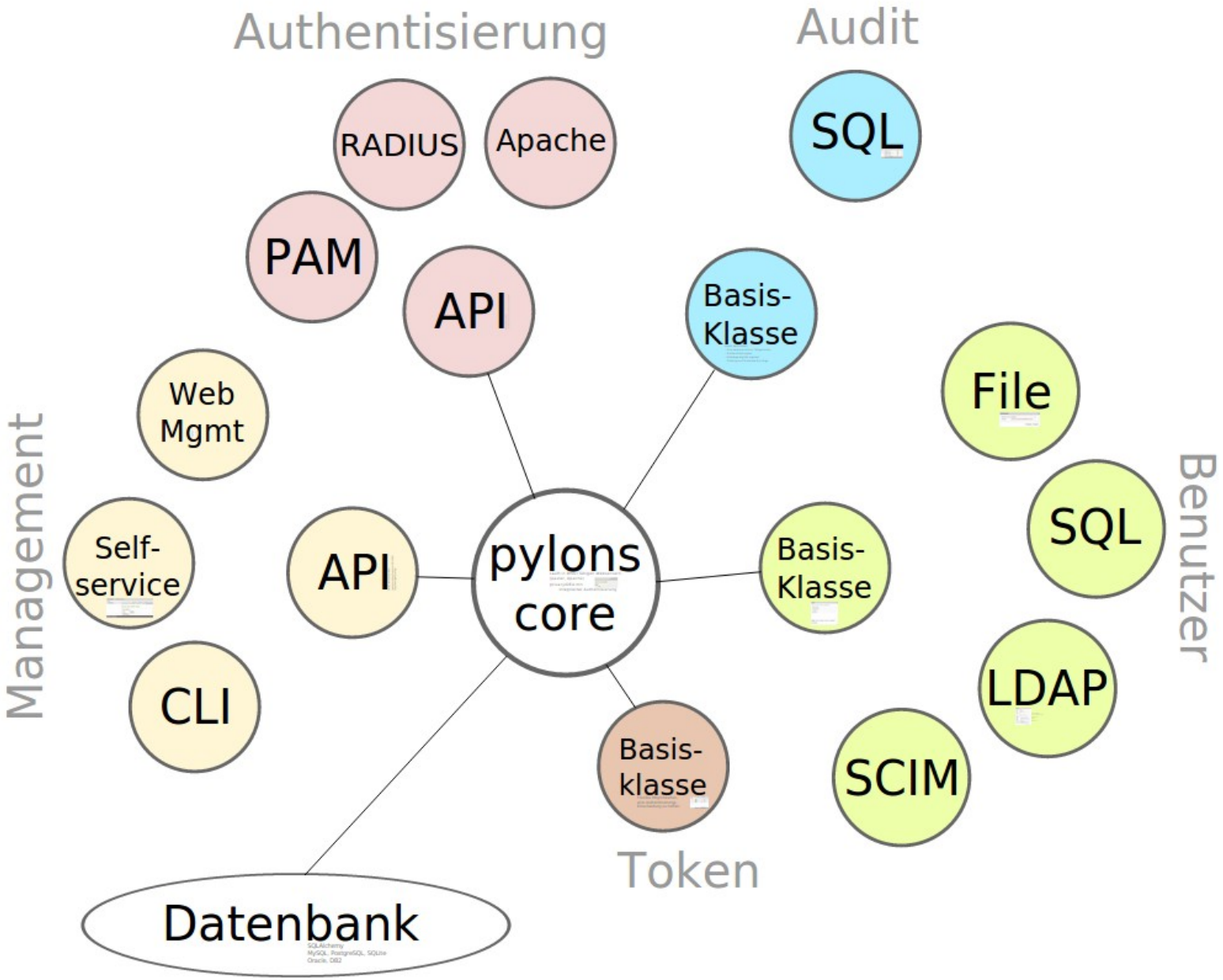
Wie Identitäten überprüfen?

- Keine Biometrie
  - Wir authentisieren nicht mit unserer Persönlichkeit.
- Eigenes Schlüsselmaterial
  - Geheime Schlüssel können selber erzeugt werden und bleiben geheim.
  - → Wahl der Hardware!
- Eigene Entscheidung
  - Über die Authentisierung entscheidet nicht ein beliebiger Provider.

privacyIDEA

- Authentisierungsserver und Managementsystem für Besitzfaktor
- OSS auf github.com/privacyidea
- Webapplikation in Python
- Modularer Aufbau
- Fork von LinOTP (seit 2010)

privacyIDEA Struktur



Authentisierungsgeräte

privacyIDEA bietet bereits verschiedene Möglichkeiten der Authentisierung.

- Click-Token

  sendet credentials

  `(user, password) → Authentisierungsserver`

  privacyIDEA validiert die credentials direkt

- Beispiele
  - Google-Authenticator u.a.
  - Feitian (C100, C200)
  - Yubikey (im Button-Modus)

Authentisierungsgeräte

- Challenge Response Token

  sendet credentials (Passwort optional)

  `(user, [password]) → Authentisierungsserver`

  `Challenge ← Authentisierungsserver`

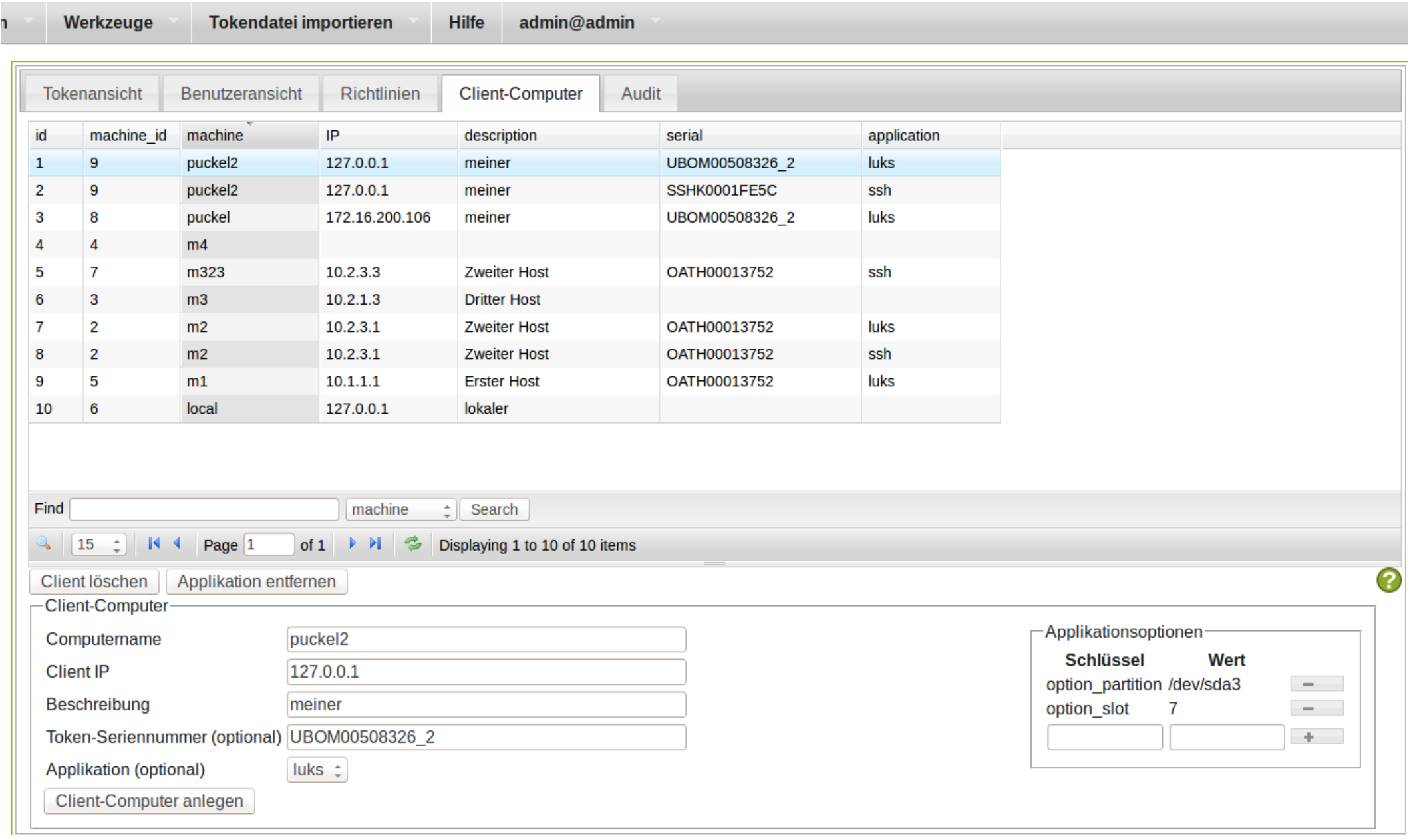
  `Algorithmus(Challenge) → Authentisierungsserver`

- Beispiele
  - SMS
  - Email
  - OCRA (Feitian C300, Smartdisplayer e3xxx, t3xxx)
  - (Smartcards/Pubkey)

Anwendungsfälle
Click-Token und Chall/Resp

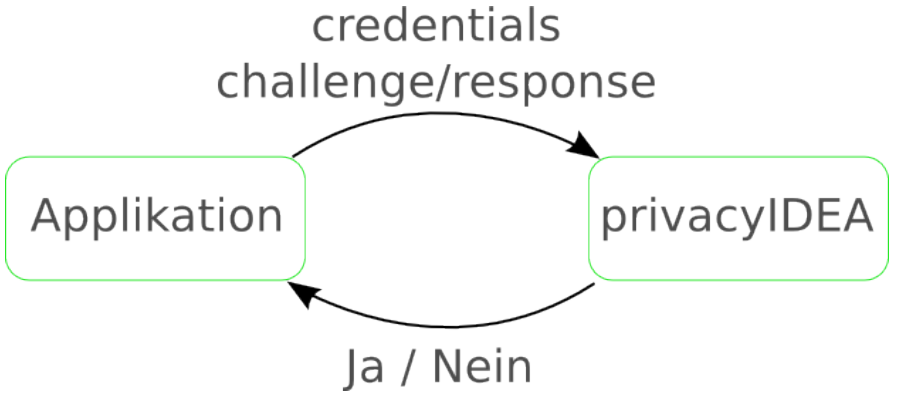
- SSL VPN
- Webapplikationen (OTRS, django, Wordpress, contao...)
- Serverfarm/SSH
- ...
    - Alle Applikationen die im Netzwerk stehen und auf einen Authentisierungsserver zugreifen können.

Clients und Applikationen

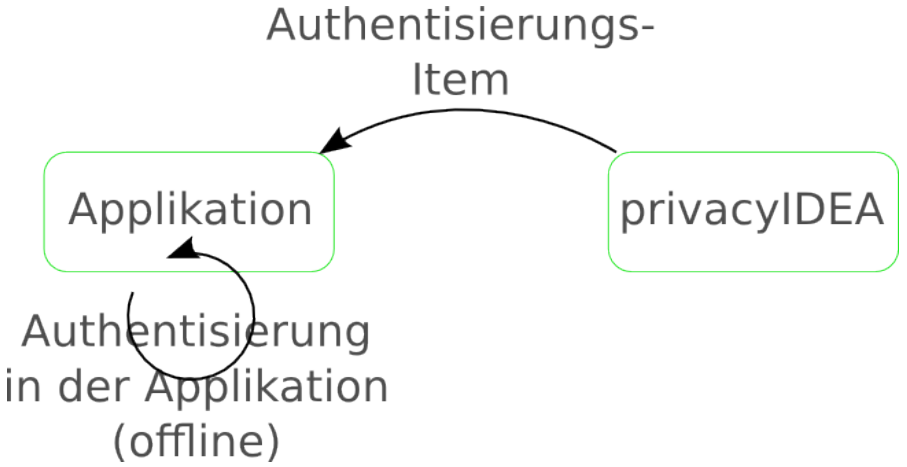


Authentisierung
mit und ohne Clients

- Mit Click-Token und Challenge Response



- Mit Machinen/Clients und Applikationen



Anwendungsfälle
Clients / Applikationen

- LUKS und Yubikey
- SSH-Server und SSH-Token
- ...
    - privacyIDEA verteilt die notwendigen Authentisierungsinformationen an die Applikationen.
    - Die Applikationen müssen zur Authentifizierung nicht mehr mit privacyIDEA kommunizieren.

privacyIDEA Ideen

- Look@ github issues und wiki!
  - Infrastruktur verbessern
    - (Repos, RPM, „Appliance“)
  - Weitere Token-Typen
  - Client-Zertifikate ausrollen und verwalten

Danke

http://www.privacyidea.org

Cornelius Kölbel

cornelius@privacyidea.org