

# Mehr-Faktor-Authentifizierung

## Open Source MFA mit privacyIDEA

Cornelius Kölbel  
@cornelinux

[cornelius.koelbel@netknights.it](mailto:cornelius.koelbel@netknights.it)  
<https://privacyidea.org>

tübix  
11. Juni 2016

# Identität – Authentifizierung

## Alltag

- Zwischenmenschlich
  - Gesicht
  - Stimme
  - Verhalten



# Identität – Authentifizierung

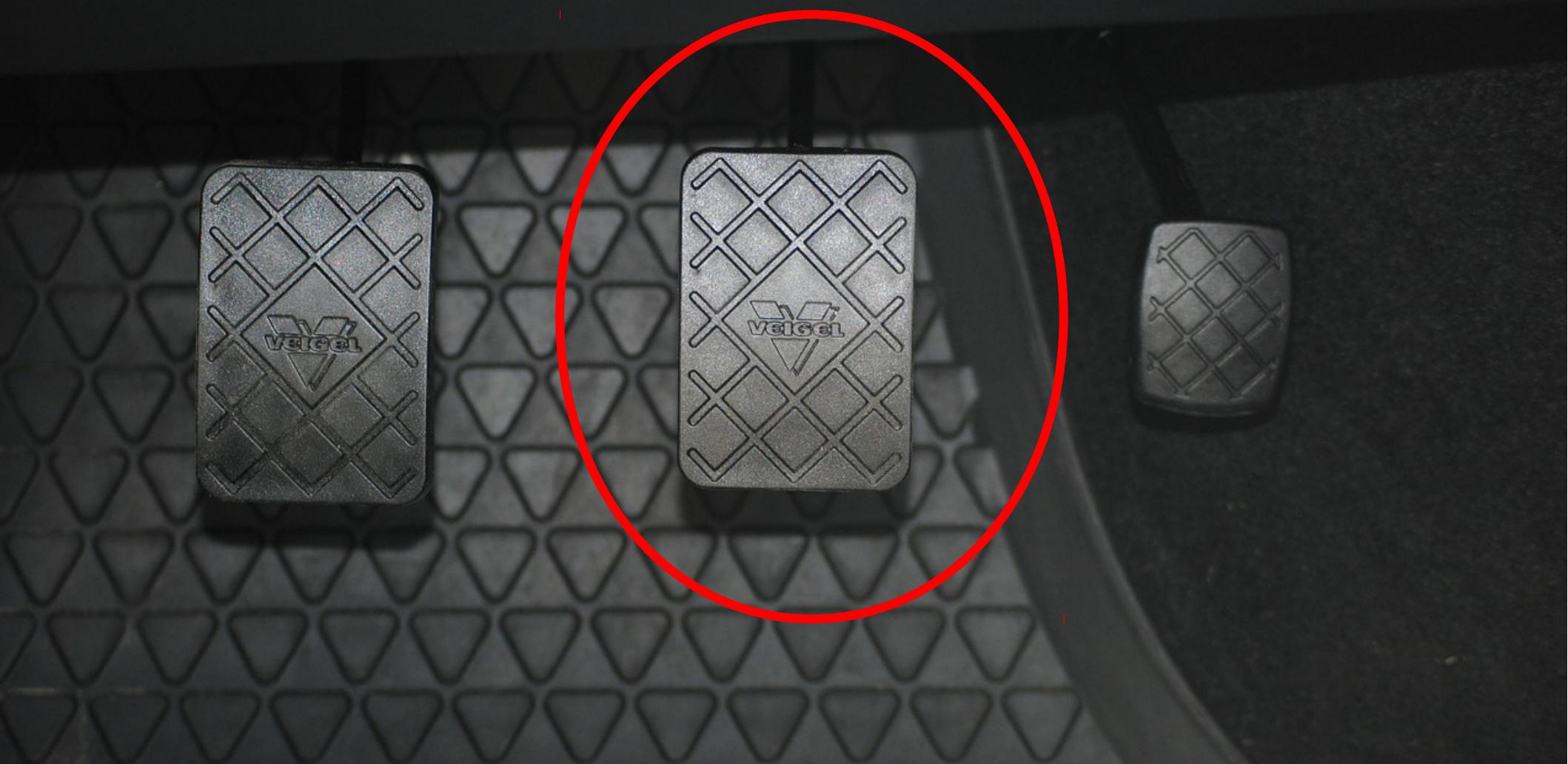
## Auto



- Jedem Deutschen sein Auto
  - Schlüssel

# Identität – Authentifizierung

## Schöne Neue Welt?



# Identität – Authentifizierung Computer

- Benutzerpasswort **(123456)**



# Begriffsklärung

- Authentisierung vs. Authentifizierung
- Verschiedene Authentisierungsarten



Wissen



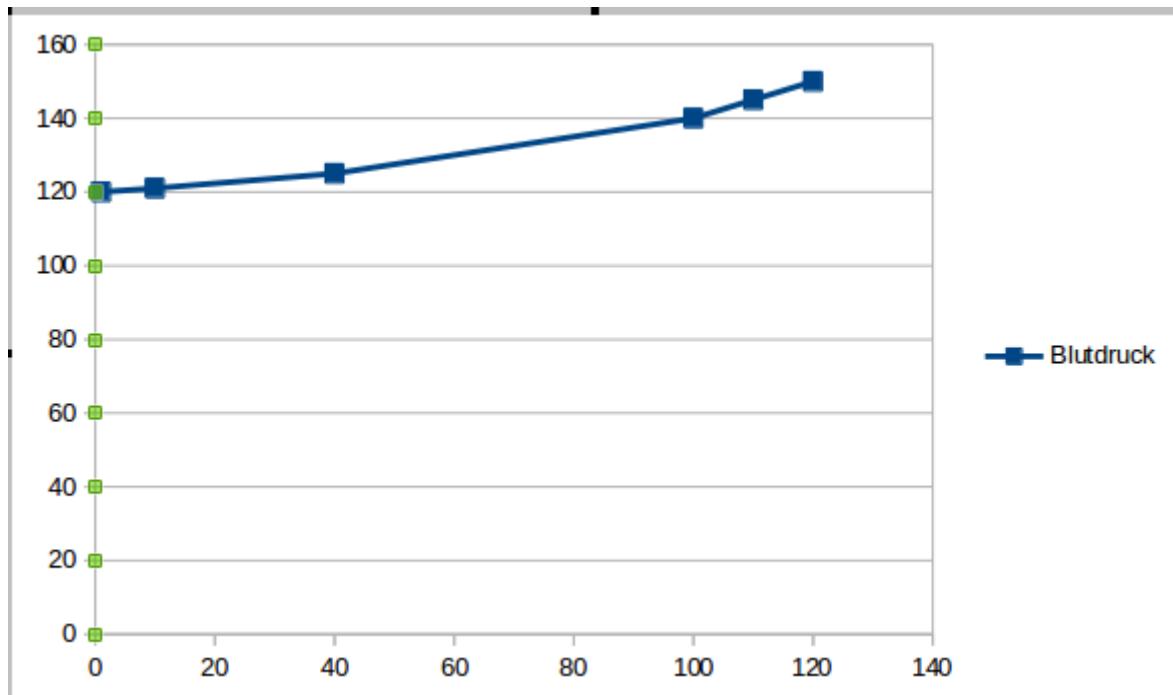
Besitz



Eigenschaft

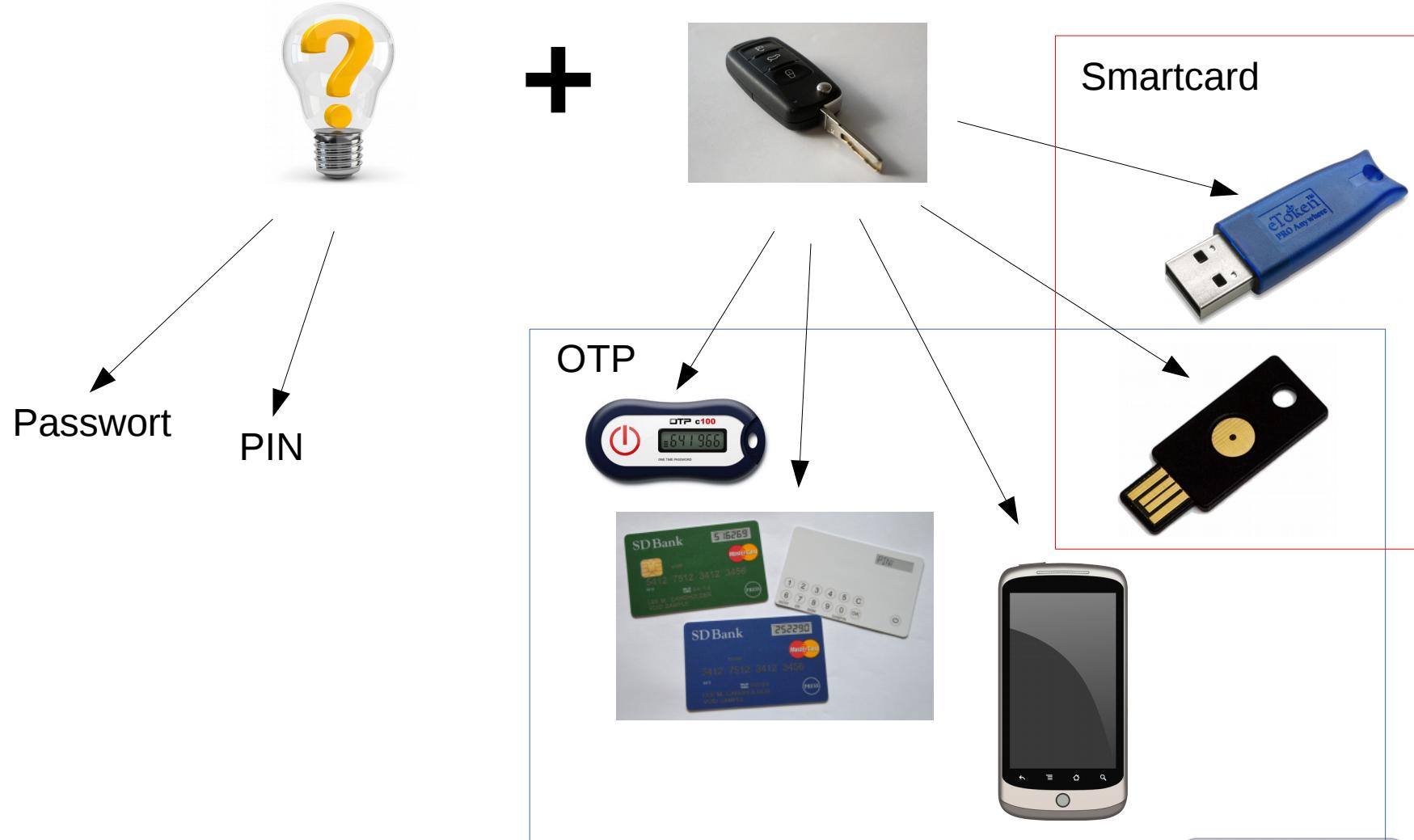
# Passwörter: Komplex und viel

- Tein:ohwenoong7Ao|Sho



- Nur das Passwort reicht nicht aus.

# Mehr-Faktor-Authentifizierung: Kombination



# Warum jetzt Mehr-Faktor-Authentifizierung?

- Angriffszenarien und Skill-Profile des Angreifers



- Phishing / Social Engineering
- SQL-Injection
- Cracker / Skript-Kiddie



- Physikalischer Diebstahl
- Zugriff zum Firmengebäude



- Körperkontakt
- Partybesucher / Einwohnermeldeamt

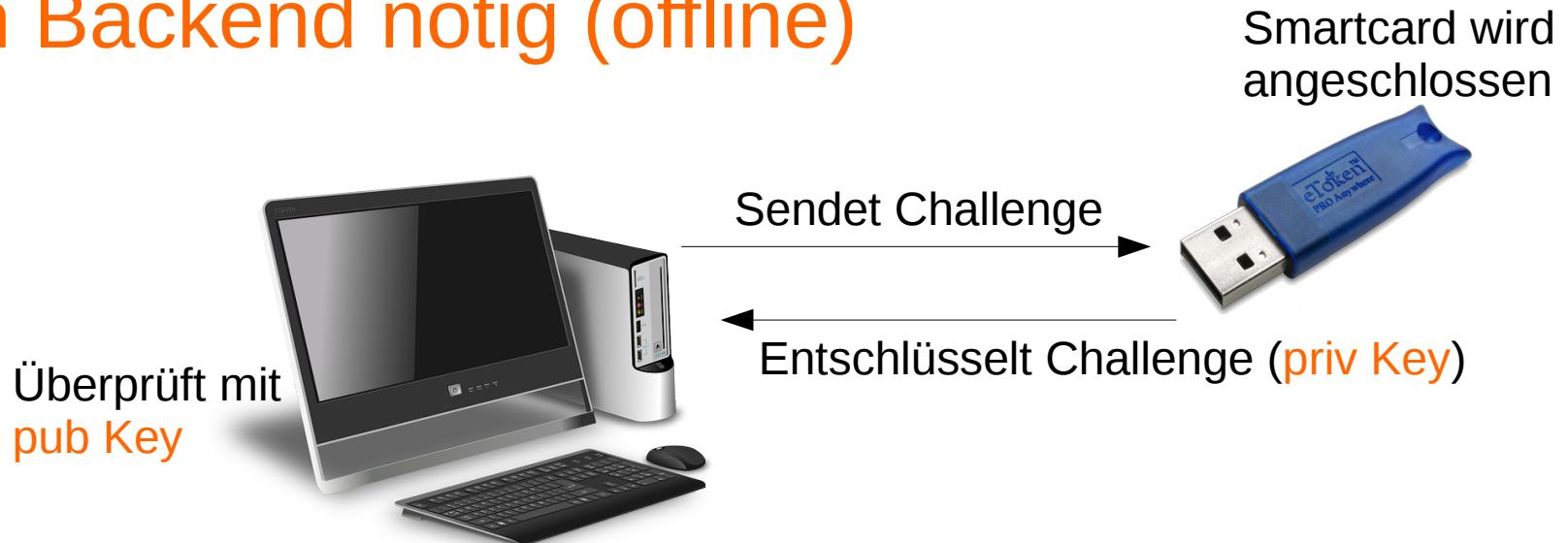
# Anforderungen an 2. Faktor

- Eindeutig → Nicht kopierbar
- Verlust sollte bemerkbar sein
- Revozierbar / Neu ausstellbar



# Smartcard

- Assymmetrischer Algorithmus (RSA bis 2048/4096 bit)
- Treiber erforderlich
- Kein Backend nötig (offline)



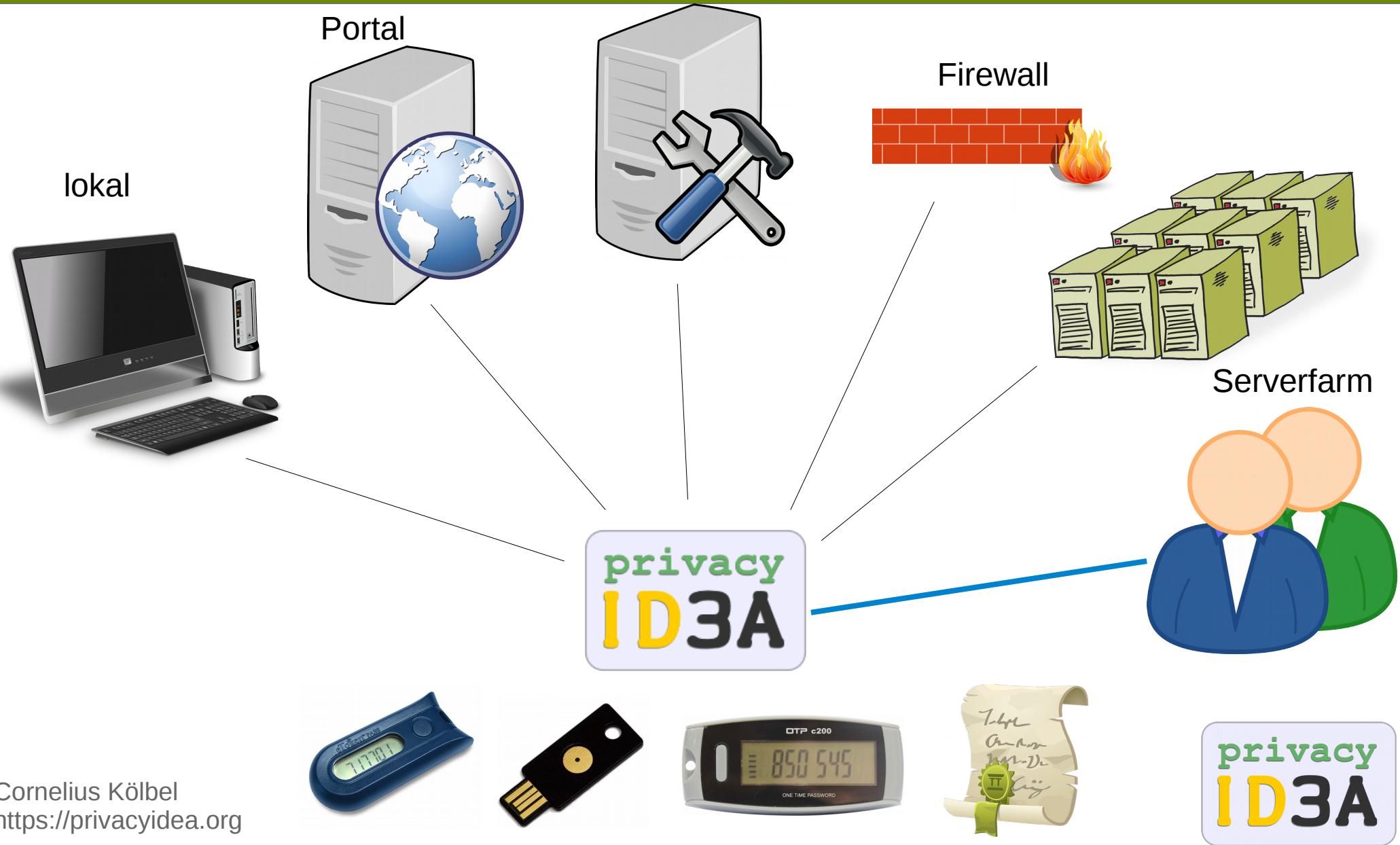
# OTP: Einmal-Passwörter

- Symmetrischer Algorithmus (RFC 4226, 6238...)
- Keine Treiber
- Backend erforderlich



# privacyIDEA

## Überblick



# privacyIDEA

## Features

- Offen, Open Source, Kein Vendor-Lock-In,
- Auth-Devices: Yubikey, U2F, HOTP/TOTP, TiQR, SMS, Email, Google Auth, SSH-Key, X.509 u.v.m.
  - Zertifizierungsstelle
- Policies → *Migration (2.11)*
- Event Handler Framework → *Email Notification (2.12)*
- API → Automatisierbar (*Token Enrollment*)
- Audit
- Benutzer lokal, LDAP, AD, SQL, SCIM...
- Anbindung von Linux und Windows Desktop, PAM, RADIUS, SAML, Wordpress, OTRS, Dokuwiki, TYPO3, Contao, ownCloud/Nextcloud u.v.m.

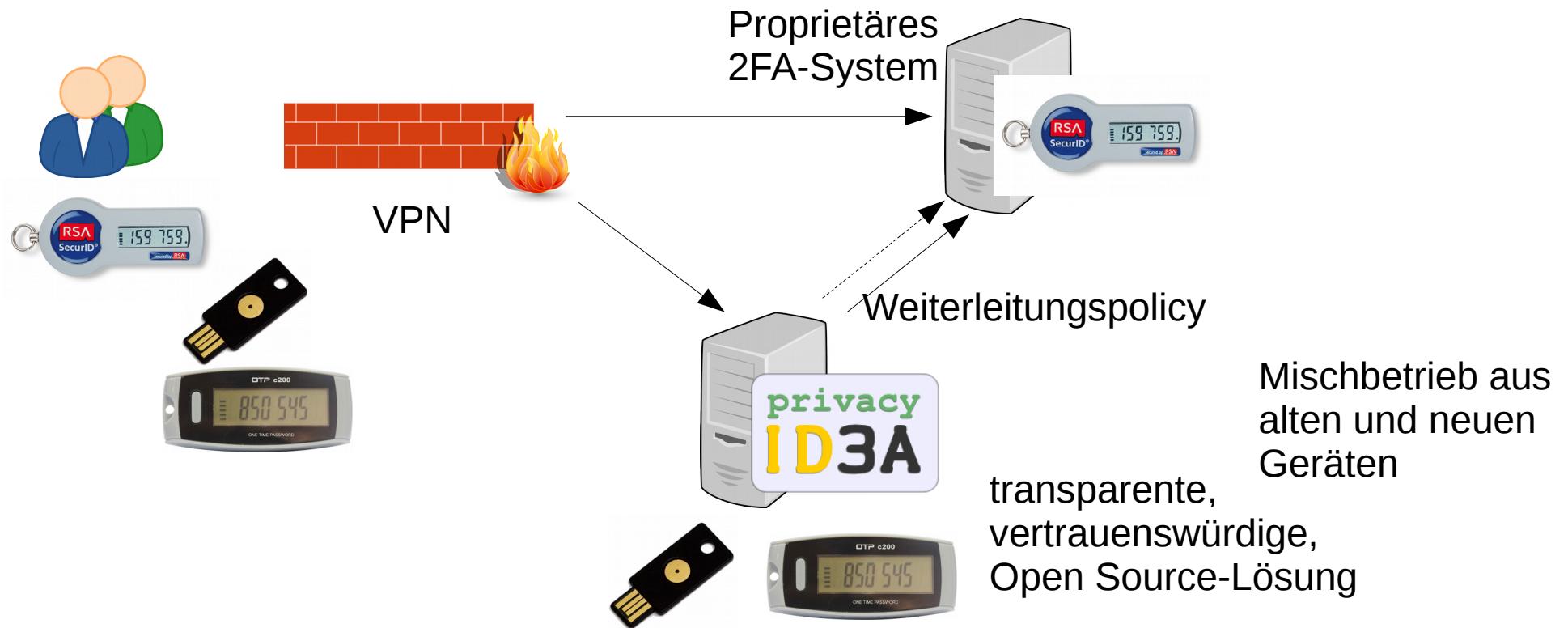
# privacyIDEA

## Features

- Beispiele:
  - Migration / Policies
  - Event Handler
  - Token Enrollment mittels API

# Migration bestehender OTP-Lösungen

- Sanfte Migration



# Migration im UI

- Definition von zentralen RADIUS Servern.
  - Für Migration oder auch für
  - RADIUS-Token

The screenshot shows the privacyIDEA web interface. At the top, there is a navigation bar with links: privacyIDEA, Tokens, Users, Machines, Config (which is highlighted), and Audit. On the far right, it shows the user 'admin @ (admin)' and a dropdown menu.

Below the navigation bar, there is a secondary navigation bar with links: System, Policies, Events, Tokens, Machines, Users, Realms, and CAs.

The main content area has a blue header 'List RADIUS server definitions'. Below this, there is a button 'New RADIUS server' and a table listing three RADIUS servers:

Identifier	IP/FQDN	Dictionary	Description	Action
2ndRADIUS	10.0.1.3:1812	/etc/privacyidea/dictionary		<button>Delete</button>
SecurID	10.0.1.2:1812	/etc/privacyidea/dictionary		<button>Delete</button>
localhost	127.0.0.1:1812	/etc/privacyidea/dictionary		<button>Delete</button>

# Migration im UI

privacyIDEA    Tokens    Users    Machines    Config    Audit    admin @ (admin) ▾

The screenshot shows the privacyIDEA web interface. At the top, there's a navigation bar with links for System, Policies, Events, Tokens, Machines, Users, Realms, and CAs. The Policies tab is selected. On the left, a sidebar has 'All Policies' and a 'Create new Policy' button. The main content area is titled 'Edit Policy migration'. It shows a policy named 'migration' with a 'Disable' and 'Delete' button. Below the name, a note says: 'If you change the name of the policy, it will create a new policy with the new name!'. There are sections for 'Scope' (set to 'authentication'), 'Action' (checkbox 'passthru' checked), and three configuration options: 'smstext' (text input 'text...'), 'smsautosend' (checkbox), and 'emailsubject' (text input 'text...'). A blue '+Create Policy' button is visible above the action section.

- Definition einer Richtlinie.

# Event Handler - Notification

- Jeder Aktion im UI ist ein API-Call
- Admins und Helpdesk-MA können Token verwalten.

The screenshot shows two panels of the Keycloak administration interface:

**User Management Panel (Left):**

- Details for user cornelius in realm localsql**: Shows user information (Username: cornelius, Given name: Cornelius, Surname: null, Description: null) and tokens (Email: cornelius.koelbel@netknights.it, Phone: null, Mobile: null).
- Tokens for user cornelius**: A table showing two tokens:

serial	type	Active	window	description	failcounter	maxfail	otplen
OATH0014AB4D	hotp	active	10		0	10	6
TOTP00112860	totp	active	10		0	10	6
- Assign a new token**: A search bar for serial numbers.

**Policy Management Panel (Right):**

- Edit Policy superuser**: A form to edit a policy named "superuser". It includes fields for Policy Name (superuser), Scope (admin), Admin-Realm (None Selected), Action (set, revoke, adduser, enrollSMS, policydelete), and descriptions for each action.

# Event Handler - Notification

- Im Rahmen ihrer Rechte (Policies) können Admins neue Token ausrollen  
→ Missbrauchspotential (trotz sign. Audit)
- An Token-Events */token/init* können Aktionen (Notification gebunden werden)
- Aktionen können an alle events (API-calls) gebunden werden.

# Event Handler - UI

The screenshot shows a web-based configuration interface for event handlers. At the top, there is a navigation bar with links: System, Policies, Events (which is the active tab), Tokens, Machines, Users, Realms, and CAs. On the left, a sidebar titled "All Event Handlers" contains a blue button labeled "Create new Event Handler". The main content area is titled "Create a new Event Handler". It includes fields for "Events" (set to "token\_init, token\_assign, token\_unassign, token\_revoke, token\_enable, token\_disable"), "Handlermodule" (set to "UserNotification"), "Condition" (empty), and "Action" (set to "sendmail"). Below this, there is a section titled "Options" with a "body" field containing the following text:

body

```
Hallo {user},  
Der admin {admin} hat an Deinem Token {serial} rumgefummelt!
```

The body of the mail that is sent.

Below the body field, there are other options: "emailconfig" set to "themis" (with a note: "Send notification email via this email server."), and "subject" (an empty field with a note: "The subject of the mail that is sent."). At the bottom right, there is a blue button labeled "+Create Event Handler Definition".

Tracy  
BA

# Handler Module

- Definiert mögliche Aktionen
  - und dazugehörigen Parameter
    - <http://privacyidea.readthedocs.io/en/latest/modules/lib/eventhandler.html>
- Methode *actions* liefert entsprechendes *dict* zurück
- Führt Aktionen entsprechend der zentralen Definitionen aus
  - Methode *do(action, options)* führt Aktion aus.
- UserNotification:
  - 89 Zeilen Python Code!

# Denkbare Event Handler

- Neue Python Klasse von *BaseEventHandler*
  - PIN Notification
  - Clean Up
    - Datenbank
    - Abgelaufene/Tote Token
  - Enrollment/Issuing
- You Choose! → Github

# API – Token Enrollment

- Vollständige REST API  
([readthedocs.io](https://readthedocs.io))
- Authentisierung an API  
auch gegen privacyIDEA  
selber
- JSON Web Tokens

## POST /token/set

This API is only to be used by the admin! This can be used to set token specific attributes like

- description
- count\_window
- sync\_window
- count\_auth\_max
- count\_auth\_success\_max
- hashlib,
- max\_failcount

The token is identified by the unique serial number or by the token owner. In the later case all tokens of the owner will be modified.

## JSON Parameters:

- **serial** (*basestring*) – the serial number of the single token to reset
- **user** (*basestring*) – The username of the token owner
- **realm** (*basestring*) – The realm name of the token owner

**Return:** returns the number of attributes set in “value”

**Rtype:** json object

## GET /token/

Display the list of tokens. Using different parameters you can choose, which tokens you want to get and also in which format you want to get the information (*outform*).

## Query Parameters:

- **serial** – Display the token data of this single token. You can do a not strict matching by specifying a serial like “OATH”.
- **type** – Display only token of type. You can do a non strict matching by specifying a tokentype like “otp”, to file hotp and totp tokens.
- **user** – display tokens of this user
- **viewrealm** – takes a realm, only the tokens in this realm will be displayed
- **description** (*basestring*) – Display token with this kind of description
- **sortby** – sort the output by column

# API – Token Enrollment

- JWT holen:

POST /auth

username=admin

password=topsecret290374

- Response: "token": "eyJhbGciOiJIUzI1NiJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.sVZDwvXWzHcOOGC9LqkxPQ"

- Token ausrollen:

POST /token/init

Authorization: eyGciOiJIUzI1NiJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.sVZDwvXWzHcOOGC9LqkxPQ (Header)

<diverse Parameter>

# Token Enrollment – python module

- Token in python code ausrollen:

```
client = privacyideaclient(admin, password, URL)  
client.inittoken(parameter)
```

- Token löschen

```
client.removetoken( { „serial“: <seriennummer>} )
```

# Ausblick - Roadmap

- Siehe Github / milestones / issues:
  - PIN-Handling → Eventhandling
  - SMS und Email-Token vereinen
    - Apps wie pushover
  - ownCloud 9.1/Nextcloud
  - Weitere plugins für Webapplikationen

# Schau mal rein

- <http://github.com/privacyidea/>
  - Travis CI, codecov.io
- <http://privacyidea.org>
- <http://privacyidea.readthedocs.io>
- <https://launchpad.net/~privacyidea>
- <https://groups.google.com/forum/#!forum/privacyidea>

# Ihre nächsten Schritte

- Noobs:
  - An welchen Stellen brauchen Sie 2FA?
- Experts:
  - Richtige Technologie?  
Sowohl bei der Management-Software als auch bei den Token?  
→ Migration.
- Workshop ***HEUTE, 16:00 Uhr W3***

§

