Mehr-Faktor-Authentifizierung

Open Source MFA mit privacyIDEA

Cornelius Kölbel
@cornelinux
cornelius.koelbel@netknights.it
https://privacyidea.org

tübix
11. Juni 2016

Identität – Authentifizierung
Alltag

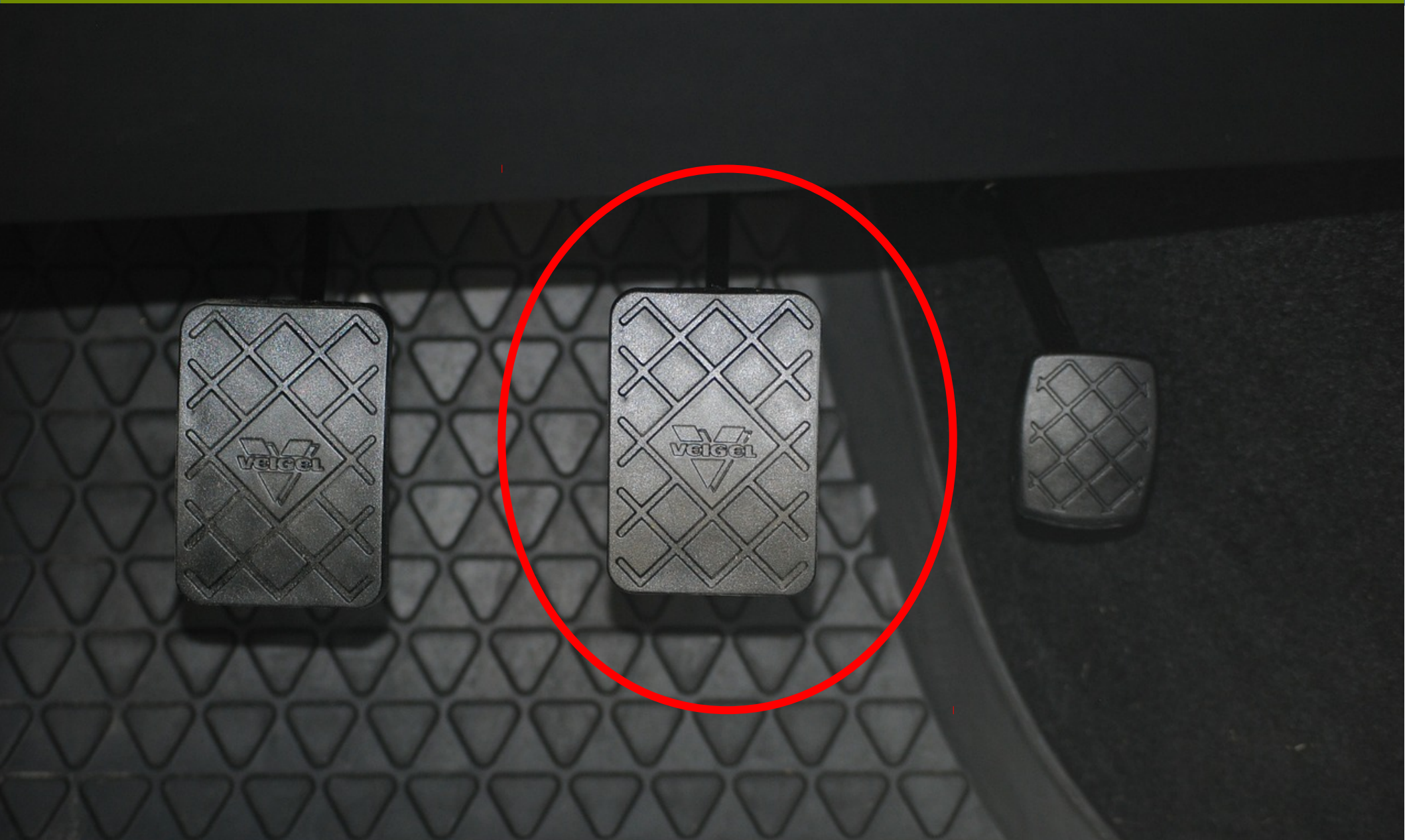
- **Zwischenmenschlich**
  - **Gesicht**
  - **Stimme**
  - **Verhalten**

Identität – Authentifizierung
Auto

- Jedem Deutschen sein Auto
  - Schlüssel

Identität – Authentifizierung

Schöne Neue Welt?



Identität – Authentifizierung
Computer

- Benutzer**passwort (123456)**

Begriffsklärung

- Authentisierung vs. Authentifizierung
- Verschiedene Authentisierungsarten

Wissen

Besitz

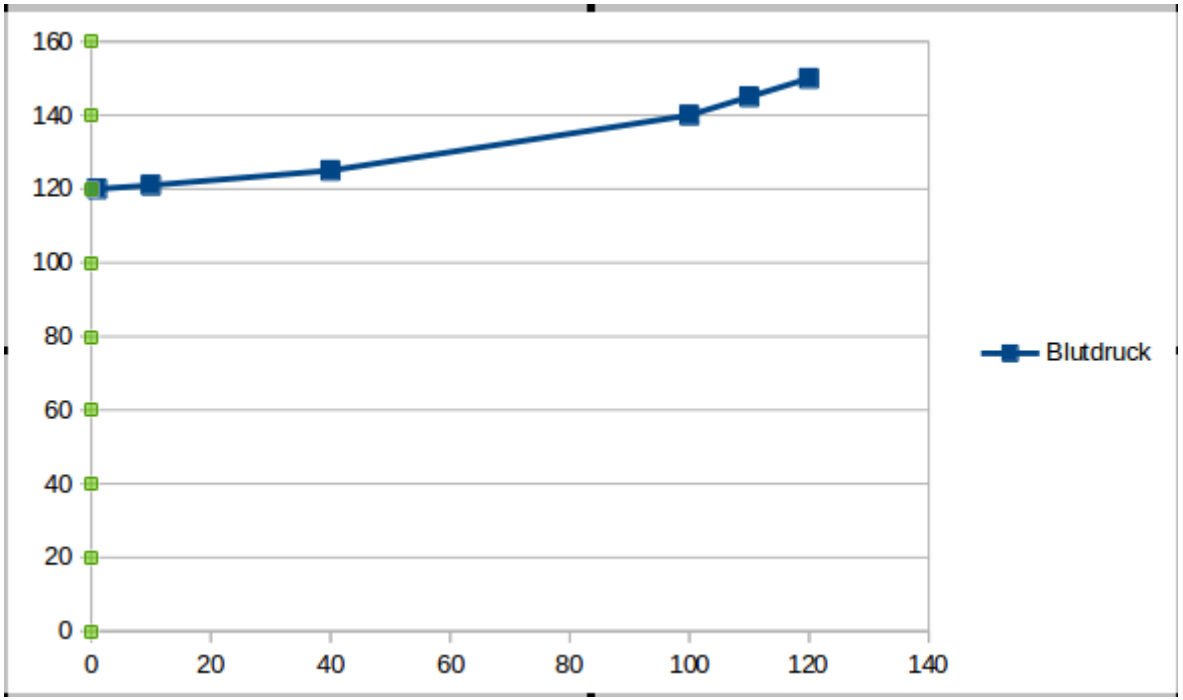
Eigenschaft

Cornelius Kölbel
https://privacyidea.org

privacy IDEA

Passwörter: Komplex und viel

- Tein:ohwenoong7Ao|Sho



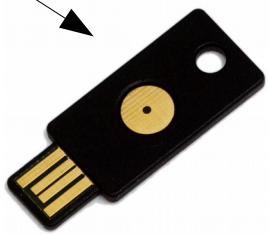
- Nur das Passwort reicht nicht aus.

Cornelius Kölbel
https://privacyidea.org

Mehr-Faktor-Authentifizierung: Kombination

+

Smartcard



Passwort

PIN

OTP

Cornelius Kölbel
https://privacyidea.org

privacy IDEA

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

Cornelius Kölbel
https://privacyidea.org

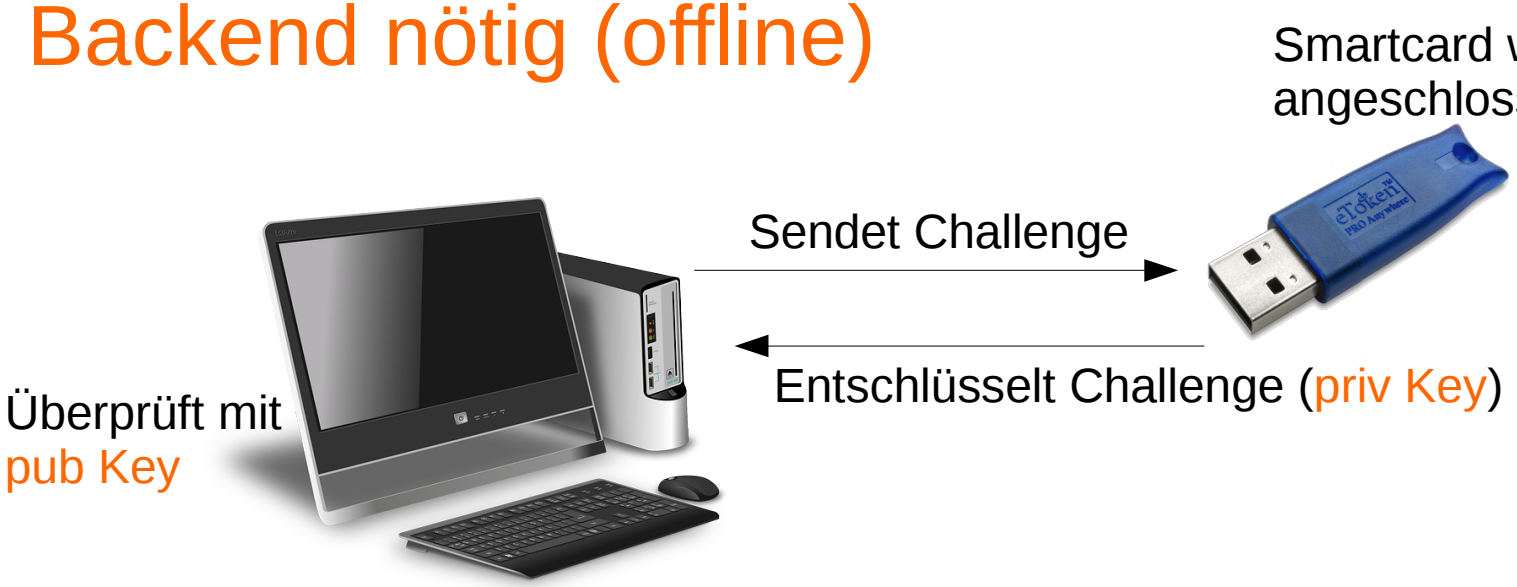
Anforderungen an 2. Faktor

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

Cornelius Kölbel
https://privacyidea.org

Smartcard

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



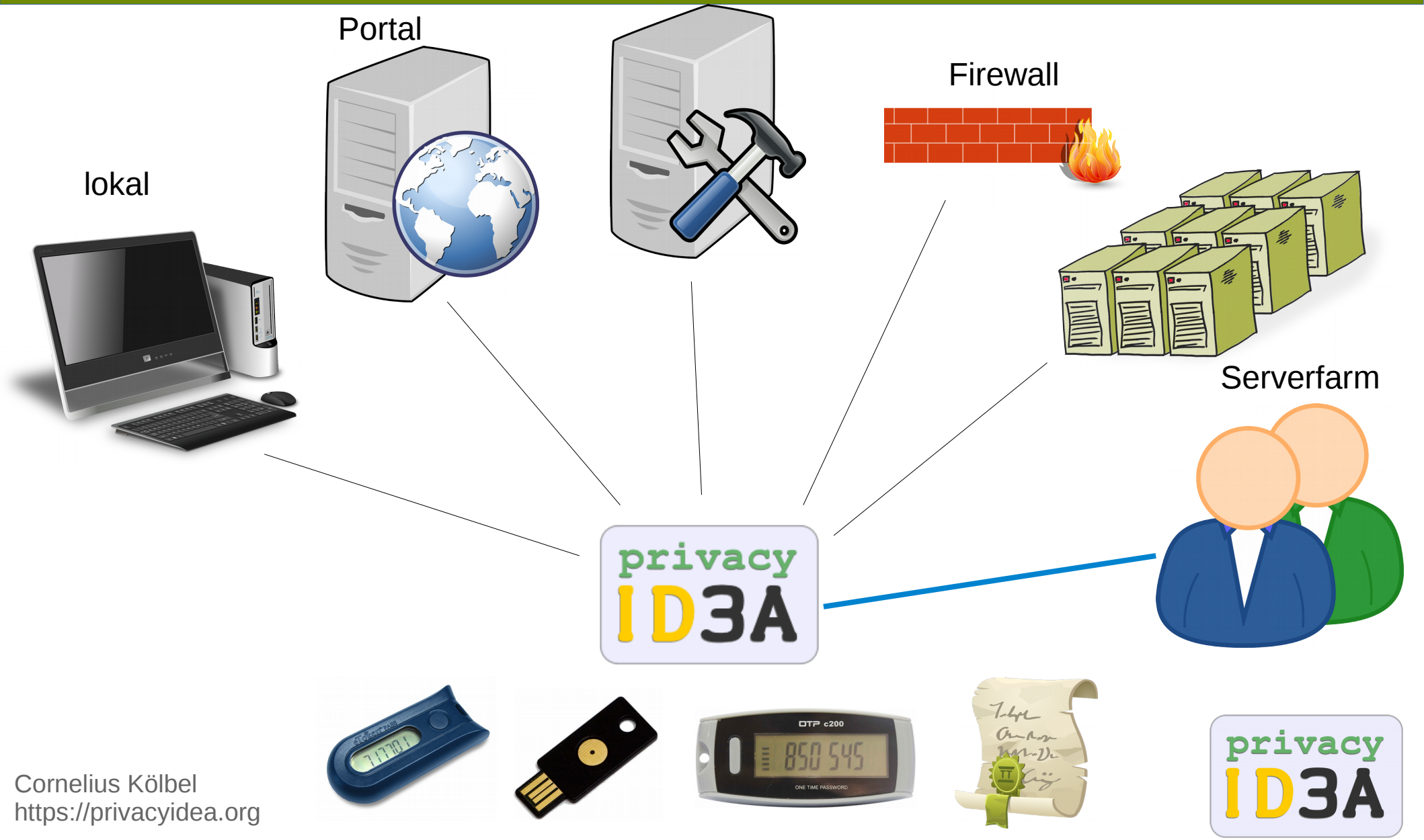
Cornelius Kölbel
https://privacyidea.org

OTP: Einmal-Passwörter

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

Cornelius Kölbel
https://privacyidea.org

privacyIDEA
Überblick



Cornelius Kölbel
https://privacyidea.org

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.

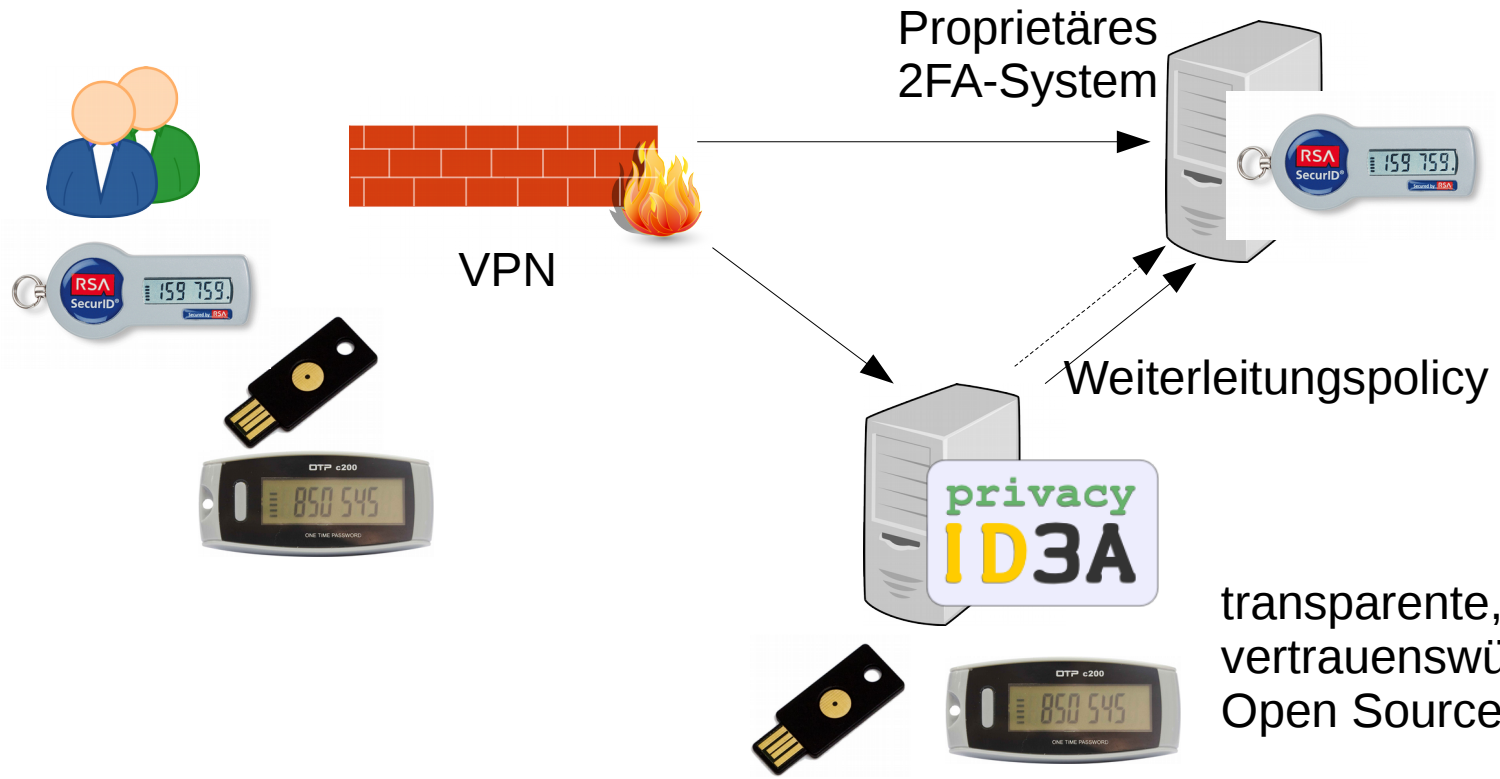
Cornelius Kölbel
https://privacyidea.org

privacyIDEA
Features

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

Migration bestehender OTP-Lösungen

- Sanfte Migration



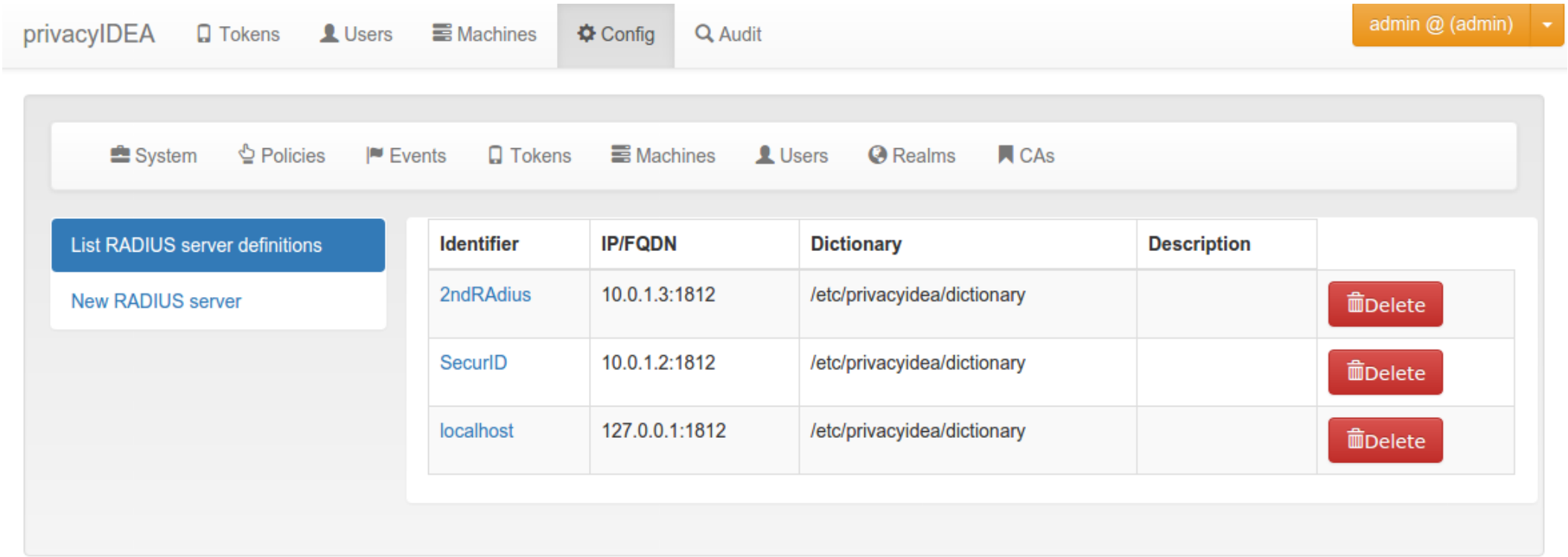
Mischbetrieb aus alten und neuen Geräten

transparente, vertrauenswürdige, Open Source-Lösung

Cornelius Kölbel
https://privacyidea.org

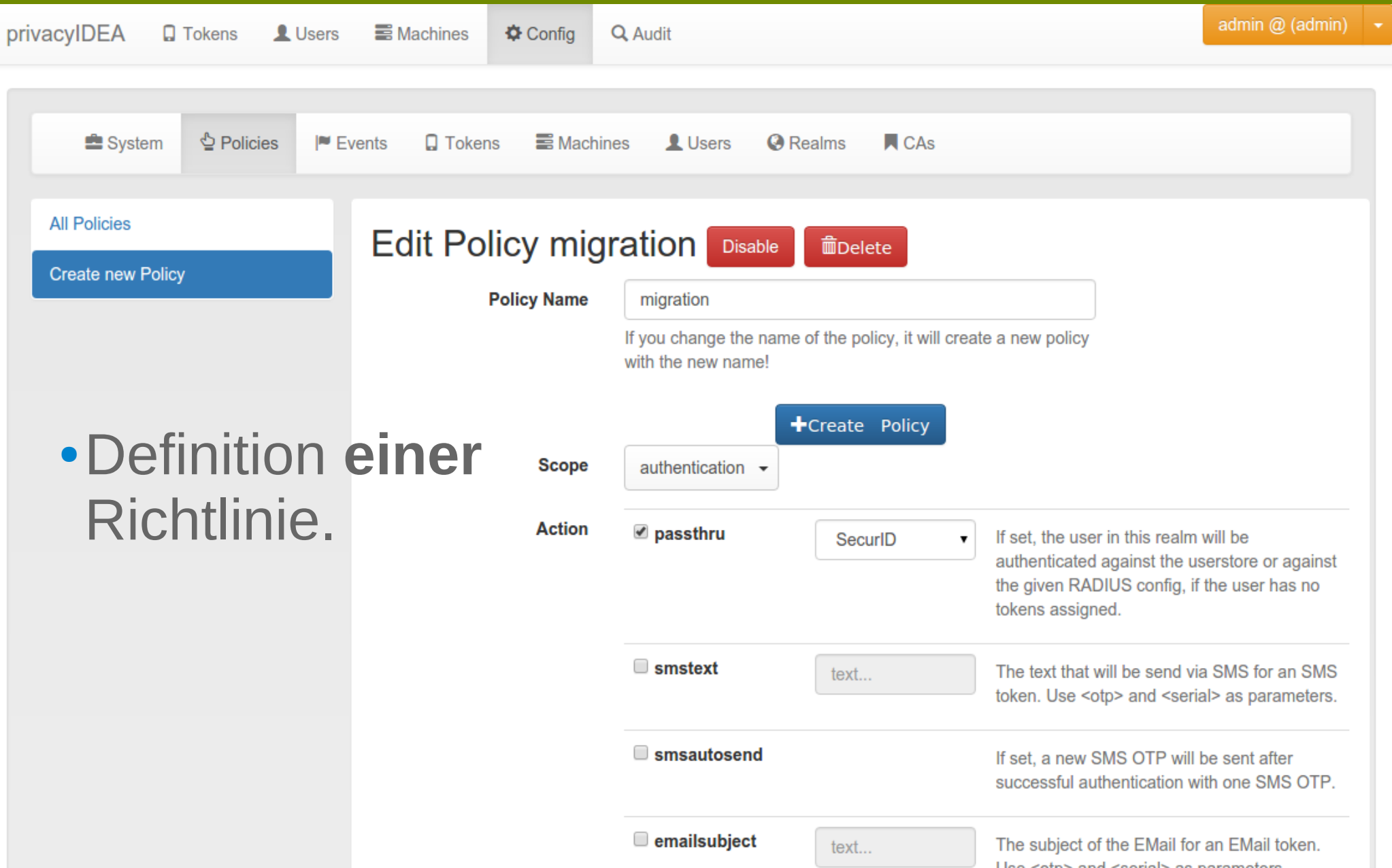
Migration im UI

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



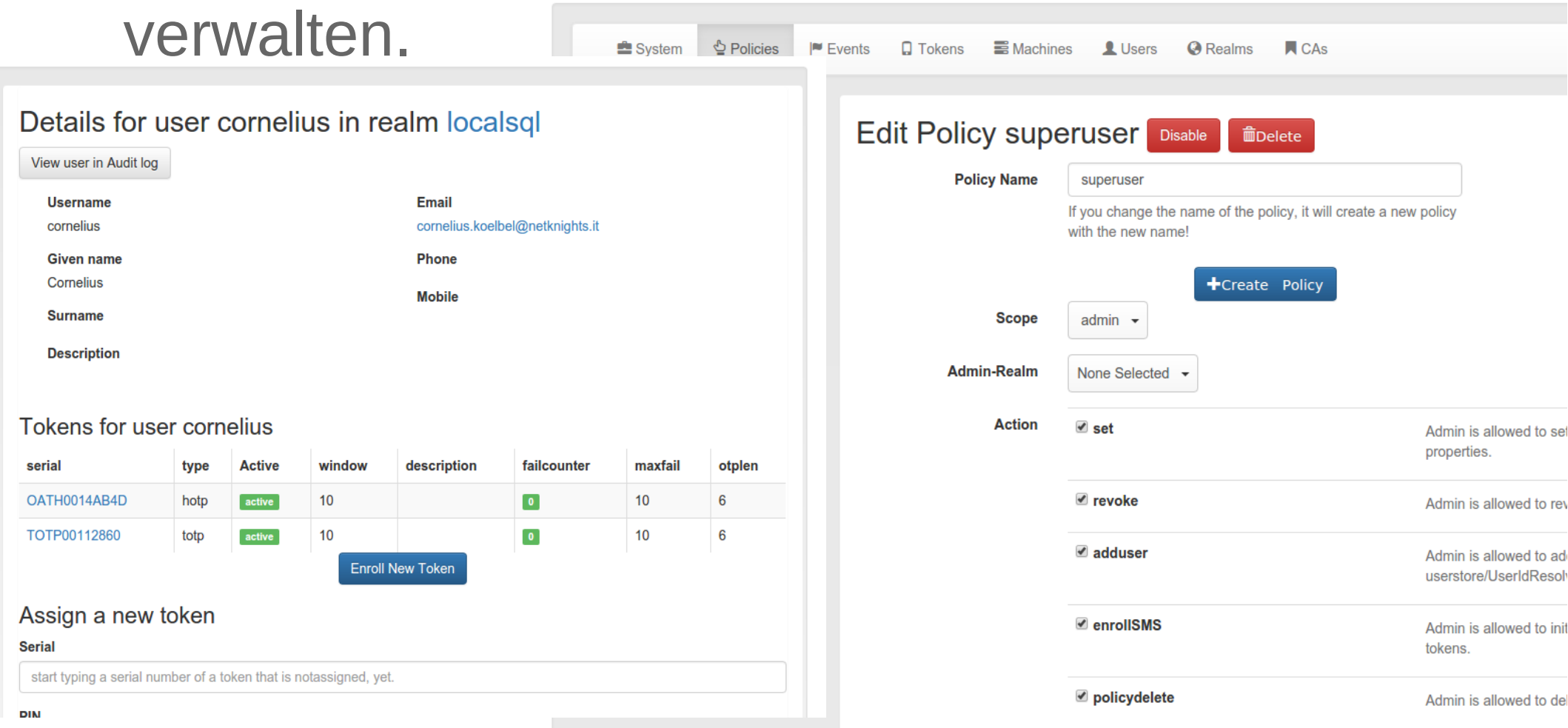
Migration im UI

- Definition **einer** Richtlinie.



Event Handler - Notification

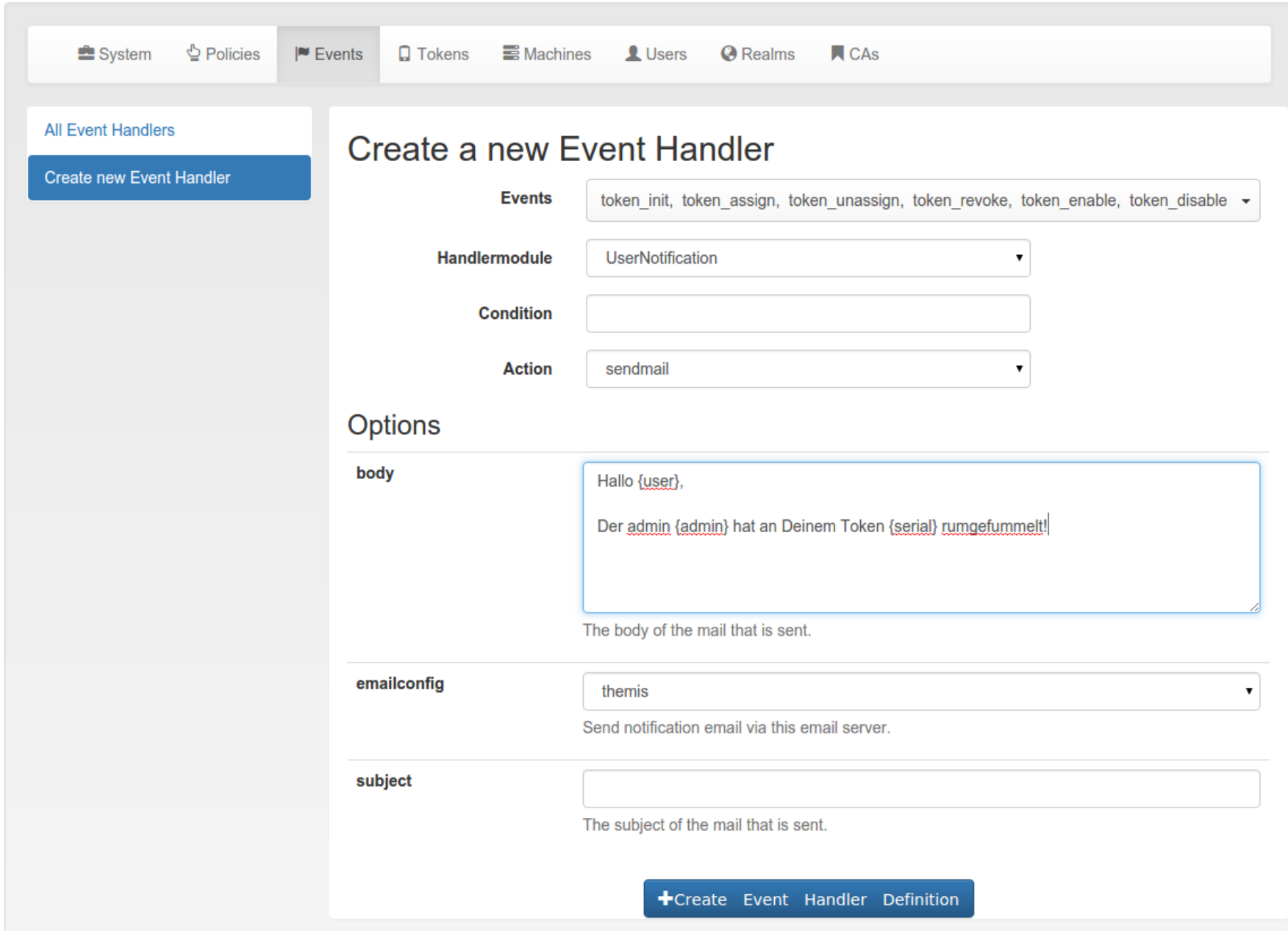
- Jeder Aktion im UI ist ein API-Call
- Admins und Helpdesk-MA können Token verwalten.



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



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)
- 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 ca 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

Cornelius Kölbel
https://privacyidea.org

API – Token Enrollment

- JWT holen:

```
POST /auth
username=admin
password=topsecret290374
```

- Response: "token": "eyGciOiJIUz...GejmbFbM"
- Token ausrollen:

```
POST /token/init
Authorization: eyGciOiJIUz...GejmbFbM (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>})
```

Cornelius Kölbel
https://privacyidea.org

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**

Cornelius Kölbel
https://privacyidea.org

privacy IDEA