



Starkes Schlüsselbrett

SSH Keys mit
privacyIDEA verwalten

Cornelius Kölbel

cornelius@privacyidea.org

Chemnitzer Linuxtage, 22.03.2015



Warner Bros.



≡ 90 1099³

RSA SecurID®

1 2 3 4 5 6 7 8 9 0

◆

P

Zwei Faktoren

Besitz



Einzigartigkeit des zweiten Faktors

	Software	Hardware
preseeded		 
seedbar		  

Zwei Faktoren

Biometrie



contemporaryarts @ pixaby

privacyIDEA

das OSS OTP System

Applikation
Authentisierung



Web UI (AngularJS, Bootstrap)

WSGI (Apache, NGINX)

REST API (Flask)

Python Bibliotheken
(Tokentype, User)

Datenbank (SQLAlchemy)

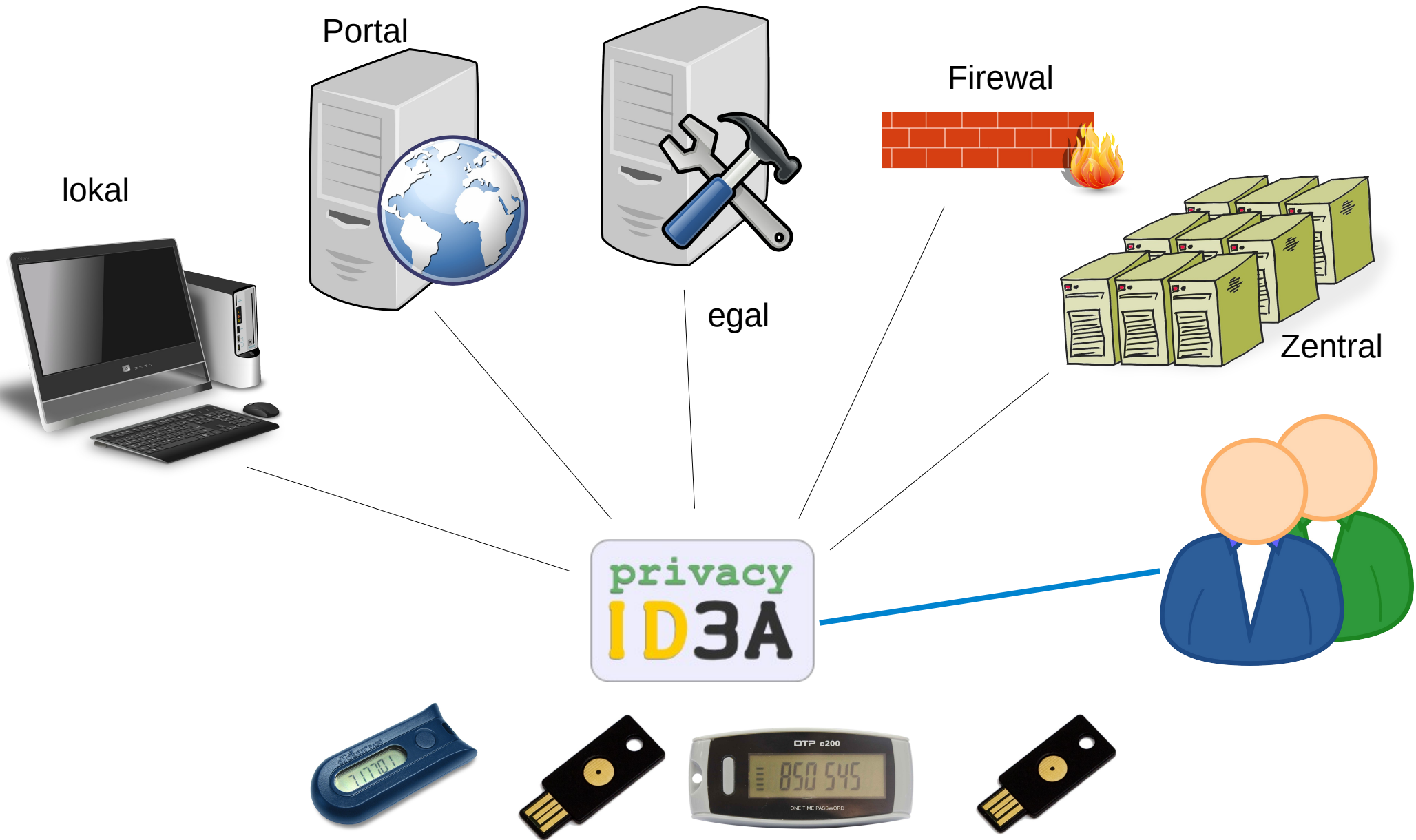
CLI
privacyidea(adm)

pi-manage.py

Redundanz

privacyIDEA

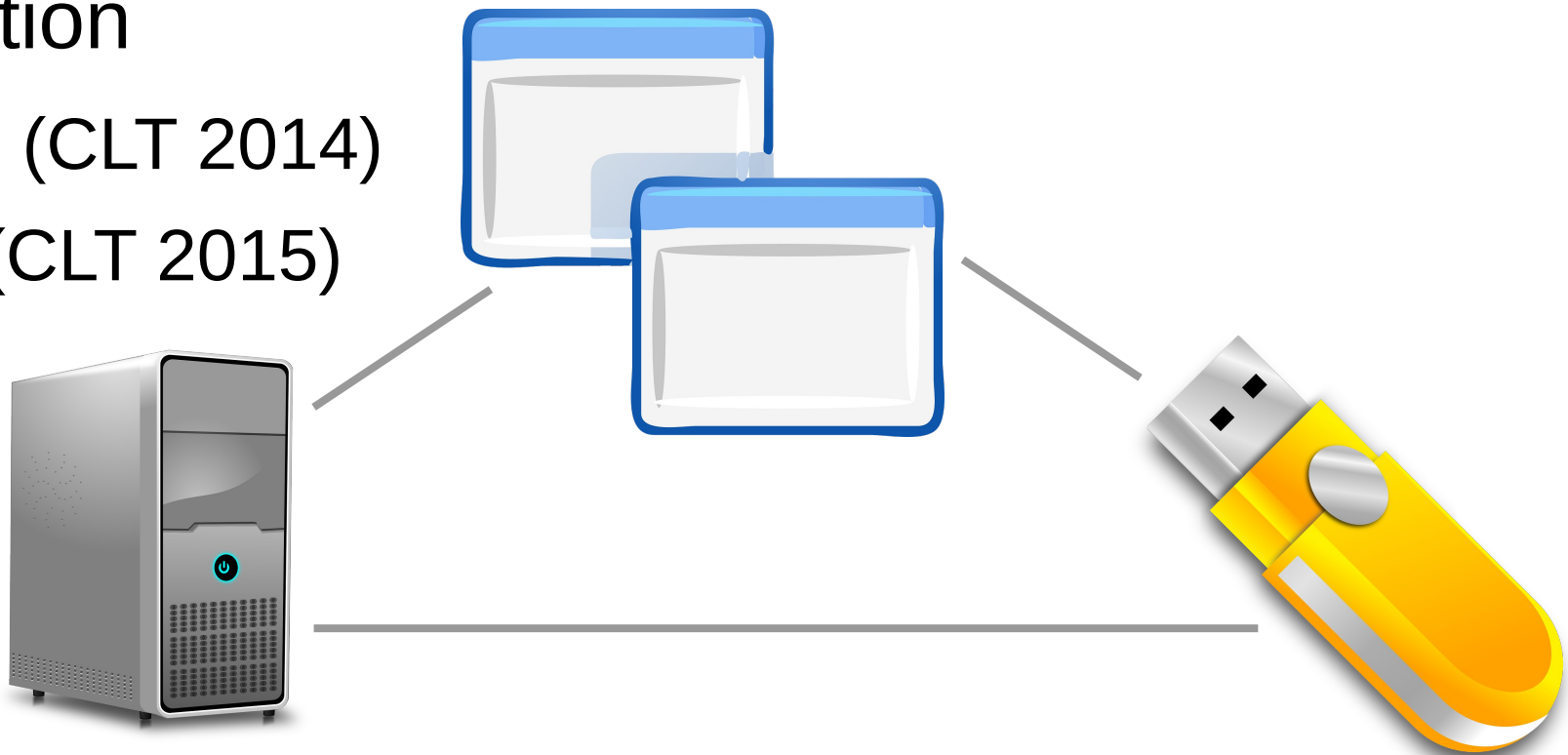
OTP



privacyIDEA

mehr als OTP

- Machine
 - Definition von Maschinen-Quellen
 - Zuordnen von Applikationen
- Application
 - LUKS (CLT 2014)
 - SSH (CLT 2015)



Maschinen

privacyIDEA

Tokens

Users

Machines

Config

Audit

Logout admin @
(Role: admin)

All Machines

Quick links

[Edit Machine Resolvers](#)

Number of machines:

hostname ▼	IP Address ▼	Id ▼	Machine Resolver ▼
["localhost"]	127.0.0.1	127.0.0.1	reso3
["puckel"]	127.0.1.1	127.0.1.1	reso3
["themis.az.local","radicale.az.local"]	172.16.200.1	172.16.200.1	reso3
["ip6-localhost","ip6-loopback"]	::1	::1	reso3
["ip6-localnet"]	fe00::	fe00::0	reso3
["ip6-mcastprefix"]	ff00::	ff00::0	reso3
["ip6-allnodes"]	ff02::1	ff02::1	reso3
["ip6-allrouters"]	ff02::2	ff02::2	reso3

Applikation

(Python Klasse)

- `get_options()`
 - Welche Parameter werden erwartet (Username, LUKS-Slot, LUKS-Partition)
- `get_authentication_item(token_type, serial, challenge, options)`
 - Liefert `items`, die für diesen **Applikations-Typen** und **Token-Typen** zur Authentifizierung genutzt werden können.

Applikationen und Token

privacyIDEA

Tokens

Users

Machines

Config

Audit

Logout admin @
(Role: admin)

All Machines

Machine 127.0.1.1

Quick links

[Edit Machine Resolvers](#)

Number of machines:

Details for machine 127.0.1.1 in Machine Resolver reso3

Hostname

["puckel"]

IP Address

127.0.1.1

Machine ID

127.0.1.1

Machine Resolver

[reso3](#)

Tokens and Applications for machine 127.0.1.1

Serial

Application

Options

Attach a new token SSHK0000F61C (sshkey)

Serial

SSHK0000F61C (sshkey)

Application

ssh

User

optional

Attach Token

SSH - Applikation

- `MachineResolver` definieren.
- Token vom Typ `SSHKey` ausrollen.
(Benutzer-Zuweisung ist nicht notwendig)
- `Token` mit `Maschine` verknüpfen und dieser Verknüpfung einen `Applikationstyp` geben.
- `sshd_conf` anpassen.
(`AuthorizedKeysCommand` → `privacyidea-authorizedkeys`)
(hands on)

Ausblick



Wo geht die Reise hin?

Ausblick

An aerial photograph of a tropical island. The island is mostly covered in green vegetation, with a prominent, rocky, and sparsely vegetated headland on the left side. A dark sand beach runs along the coast of the headland and the main body of the island. The surrounding ocean is a deep blue, with lighter turquoise water near the shore. The sky is filled with large, white, fluffy clouds, and the horizon is visible in the distance.

Version 2.2 (21.05.): Offline!

Ausblick

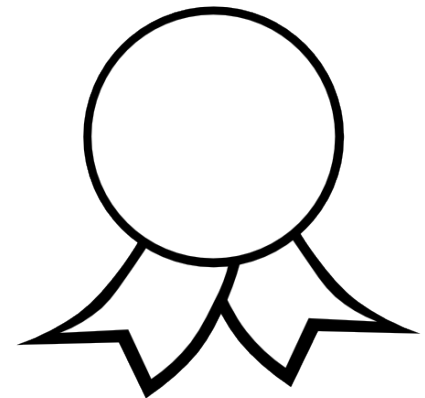
Certificate

Subject: Awesome privacyIDEA 2.3 User

Issuer: You personal privacyIDEA server

X509

Mail:master-of-ca@privacyidea.org



Kommt herzu!

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