



privacy**ID3A**  
AUTHENTICATION SYSTEM

- Manage your second factor in the cloud?
- By Microsoft? By DUO aka Cisco?
- Sync your secret keys (aka passkeys) via Apple?
- Let's keep the secrets where they belong!



privacy**ID3A**  
AUTHENTICATION SYSTEM

# Centrally/On-Prem managed Mutli Factor Authentication with privacyIDEA

FOSS North, Gothenburg, Sweden, 2025-04-15

Cornelius Kölbel



privacyIDEA  
AUTHENTICATION SYSTEM

## privacyIDEA - history

- Based on a system back in **2010** and thanks to RFC4226
- Established in **2014** as an **alternative** to big commercial solutions under AGPLv3.
- Enterprise ready **most flexible** MFA system.



privacy**ID3A**

AUTHENTICATION / SYSTEM

## Lets talk DESIGN

- Developed at Github
- The software stack
  - SPA, Webserver, REST, Python, SQL
- Install: single node, redundancy, container

# Most flexible

Abstraction of...

- users
- auth types
- applications

No one knows what the future will bring --- or which old applications you will find in a dusty corner



privacyID3A  
AUTHENTICATION SYSTEM

**Verify TLS**

Verify the TLS certificate of the server.

**Base DN****Scope****Bind Type****Bind DN****Bind Password**

# Abstraction of users

- **Resolvers** and **Realms**
- flatfile, LDAP/AD, SQL (ownCloud, Nextcloud, Keycloak), HTTP, EntralD

**Per-process server pool**

This setting activates a LDAP server pool that is persisted between requests.

**Edit user store**

The user data in this database can be modified from within privacyIDEA.

**Preset OpenLDAP****Preset Active Directory****Loginname Attribute****Search Filter**

# Abstraction of Authentication Types (aka Token)

- Base **Class**
- Authentication **modes** - Challenge Response, Multichallenge, Enroll-via-Challenge
- Paper, Text message, xOTP, x509, sshkeys, YK, FIDO2, Passkeys



# Abstraction of Applications

cornelius

- REST API
- Plugins: RADIUS, SSO/IdPs, Webapplications, PAM, Windows/CP, EntralD
- Enroll auth device **once** centrally, use **multiple** times at different logins

## Alternate Login Options

WebAuthn

# My definition of application

- Everything, that is not privacyIDEA...
- ...but that is connected to privacyIDEA.
- ...where a user logs in: Keycloak, VPN, Web Application, PAM, Windows...



privacy**IDEA**  
AUTHENTICATION SYSTEM

## All Policies

Create new Policy

# Policies

- Behaviour of privacyIDEA
- Scopes
- Conditions: Different Authentication behaviour in different situations

It is about flexibility

**Description**

Write Authentication

**Events**

validate\_check

**Handlermodule**

Token

**Position**

post

**Order**

2

# Event Handlers

- Link additional actions to API call
- Handlers: UserNotification, Token, Script, Counter, Logging, WebHook, CustomUserAttributes, RequestMangler, ResponseMangler
- Conditions

 **count\_auth**

This can be '>100', '<99', or '=100', to trigger the action, if the tokeninfo field 'count\_auth' is bigger than 100, less than 99 or exactly 100.

 **count\_auth\_fail**

This can be '>100', '<99', or '=100', to trigger the action, if the difference between the tokeninfo field 'count\_auth' and 'count\_auth\_success' is bigger than 100, less than 99 or exactly 100.



Web-Application, Firewall,  
SSH, PAM,  
...  
Windows Login

## Recurring Tasks

- Event Counter and simple stats
- Currently used to create statistics
- Can run on distinct node

Station

REST, WebUI

LDAP, SQL,  
Flatfile, SCIM



privacyID  
AUTHENTICATION  
Userstore

# Token details for WAN0001AF3A

[View token in Audit log](#)

Type	Value	Action
Maxfail	10	<a href="#">Edit</a>
Fail counter	0	<a href="#">Delete</a>
OTP Length	6	<a href="#">Edit</a>
Count Window	10	<a href="#">Reset fail counter</a>
Sync Window	1000	<a href="#">Edit</a>
Description	authenton#1 - FIDO2.1 Authenticator <b>(now)</b>	<a href="#">Edit</a>
Info	<ul style="list-style-type: none"><li>aaguid: b267239b954f4041a01bee4f33c145...</li><li>attestation_issuer: 1.2.840.113549.1.9.1=AXEL.VOND...</li><li>attestation_level: untrusted</li><li>attestation_serial: 4170000090359</li><li>attestation_subject: CN=authenton#1 - FIDO2.1 Authe...</li><li>count_auth: 4</li><li>count_auth_success: 4</li><li>last_auth: 2024-10-17 06:11:25.263418+02:...</li><li>origin: https://privacyidea.office.net...</li><li>pubKey: a50102032620012158206cd282ae4f...</li><li>relying_party_id: office.netknights.it</li><li>relying_party_name: NetKnights</li><li>tokenkind: software</li></ul>	<a href="#">Edit</a>

# Webauthn, FIDO2 and Passkeys

- FIDO2 - whole spec --- device and application
- Webauthn - application part
- Passkey --- special config of FIDO2

privacyIDEA: U2F (2015), Webauthn (2020), Passkeys  
**(now)**

# Plugin privacyIDEA Credential Provider

- **Offline - OTP** symmetric key
- one client
- no online



privacy**ID3A**  
AUTHENTICATION SYSTEM

# Plugin privacyIDEA Credential Provider

- **Offline - Webauthn** - assymmetic!
- several clients
- online at the same time



privacy**IDEA**  
AUTHENTICATION SYSTEM

- Demo privacyIDEA
- Windows client in virtual box

Do you want to try it?

Install: [Read the docs](#)



privacy**IDEA**  
AUTHENTICATION SYSTEM

# Your next steps

- Stay in control!
- Use privacyIDEA!

<https://privacyidea.readthedocs.io>

- Talk about it!

<https://community.privacyidea.org>

- Contribute!

<https://github.com/privacyidea>



privacy**ID3A**  
AUTHENTICATION SYSTEM