




privacyID3A
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!



privacyID3A
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.



privacyID3A
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

Noone knows what the future will bring --- or which old applications you will find in a dusty corner



Verify TLS

☐

Verify the TLS certificate of the server.

Base DN

dc=netknights-lab,dc=intranet

Scope

SUBTREE

Bind Type

Simple

Bind DN

netknights-lab\administrator

Bind Password

Abstraction of users

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

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

sAMAccountName

Search Filter

(sAMAccountName=*)(objectCategory=person)



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

- REST API
- Plugins: RADIUS, SSO/IdPs, Webapplications, PAM, Windows/CP, EntraID
- 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...



All Policies

Create new Policy

Policies

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

It is about flexibility

1	✓	2stepenrollment	admin	{ "hotp_2step": "allow", "totp_2step": "allow" }	[]
1	✓	pi-update-policy-3d7f8b29cbb1	admin	{ "caconnectorread": true, "configread": true, "eventhandling_read": true, "mresolverread": true, "periodictas...	[]

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

Stration

REST, WebUI



LDAP, SQL,
Flatfile, SCIM



privacyID3A
AUTHENTICATION Userstore

Token details for WAN0001AF3A

[View token in Audit log](#)

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)

Info

- aaguid: b267239b954f4041a01bee4f33c145...
- attestation_issuer: 1.2.840.113549.1.9.1=AXEL.VOND...
- attestation_level: untrusted
- attestation_serial: 4170000090359
- attestation_subject: CN=authenton#1 - FIDO2.1 Authe...
- count_auth: 4
- count_auth_success: 4
- last_auth: 2024-10-17 06:11:25.263418+02:...
- origin: https://privacyidea.office.net...
- pubKey: a50102032620012158206cd282ae4f...
- relying_party_id: office.netknights.it
- relying_party_name: NetKnights
- tokenkind: software

[Edit](#)

Plugin privacyIDEA Credential Provider

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



Plugin privacyIDEA Credential Provider

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



- Demo privacyIDEA
- Windows client in virtual box

Do you want to try it?

Install: Read the docs



privacy**ID3A**
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>



privacyID3A
AUTHENTICATION SYSTEM