

Multi-Factor-Authentication

privacyIDEA

privacyIDEA is a multi-client and multi-instance capable system for securing your identities (*ID*) by adding Multi-Factor-Authentication. It runs at a central location in your network and connects to your user management. privacyIDEA manages authentication objects (like different token types, OTP tokens, Smartphone Apps, U2F) and the access rights of the users. It can handle self created cryptographic key material (*privacy*). All actions can be written to a signed audit log (*AAA*).

Multi-Factor-Authentication

In the network at Linux Clients and Windows Clients

Using pam_radius and the privacyIDEA Credential Provider the local login at Linux machines or Windows desktops or terminal servers can be secured with a second factor. The centrally installed privacyIDEA system manages all authentication devices and controls access to the machines on the network.

At the network perimeter (OpenVPN, Citrix, Cisco, Juniper) via RADIUS

privacyIDEA comes with a plugin for the FreeRADIUS server. Thus classical perimeter services like VPNs and firewalls can be connected to privacyIDEA. This adds multi factor authentication to those services easily.

At web applications via REST API

Today communication with customers is done via web services. Web applications and customer portals handle sensitive data. privacyIDEA provides a REST API, that can be used to connect those portals to privacyIDEA and add multi factor authentication to those sensitive applications. There are implementations for TYPO3, OTRS, ownCloud/Nextcloud, Contao, Dokuwiki, Django, Wordpress a.o.

At legacy applications

There are still legacy applications which do not allow for a plugin and have no RADIUS or SAML interface. You still can add two factor authentication to these applications by using the privacyIDEA LDAP proxy. The privacyIDEA LDAP proxy acts as LDAP broker between the original LDAP server, the application and privacyIDEA. Two factor authentication becomes completely transparent to the legacy application.

Outstanding Features

SSH Key Management

Single Sign On with MIT Kerberos, FreeIPA or SAML

Powerful Policy Framework. Policies can depend on client IPs and time

Flexible Event Handler Framework allows simple automation of individual workflows

Development and Support

privacyIDEA is open source and freely available. Github is used for transparent development cycles. Pull Requests are welcome! The core developers are employed at NetKnights GmbH. NetKnights provides consultancy, workshops, support and service level agreements. This way companies can get a liability for the correctness of the software and ensure a safe operation.

Awards

In 2016 privacyIDEA won the Thomas-Krenn-Award and the Open-Source-Business-Award.



privacyID3A
AUTHENTICATION SYSTEM

strong Authentication
secure Identities
open, transparent, extensible

privacyIDEA.org