



**MULTI-FACTOR-AUTHENTICATION
DESKTOP-INTEGRATION
TOKEN
SELF SERVICE & SUPPORT**



LinOTP

Product Information

ADAPTIVE MFA / 2FA AUTHENTICATION

LinOTP is an open source, adaptive multi-factor solution for enterprise environments. LinOTP is vendor independent and provides a wide variety of solutions which allow for an easy integration. Due to its highly modular architecture LinOTP works vendor-independent and supports different authentication protocols, token and user repositories. The software supports multi tenancy, it is easily scalable, user friendly and can quickly and simply be implemented. With the help of LinOTP the highest security standards can effortlessly be achieved by our customers.

BASIC TECHNOLOGY OTP

LinOTP mainly uses one time passwords (OTP) to increase the security of all types of logon processes. One time passwords offer the advantage that they do not require a driver from the client side. The modular concept allows for the support of OTP-Tokens using different algorithms. LinOTP supports the open algorithms HOTP (event based), TOTP (time based), OCRA (challenge response based) and mOTP. Besides these proprietary tokens like e.g. Vasco DIGIPASS, the sending of one time passwords via SMS and daily passwords can be used. It is irrelevant whether a customer wants to use softtokens or hardware-tokens. The optional use of hardware tokens, which calculate the one time password for the user, can also contribute to increasing the security. Innovations of the OATH-certified version LinOTP 2.8 include features such as FIDO U2F support, registration of FIDO U2F, preparing email and SMS tokens in a self-service portal, temporary email and SMS tokens, multiple challenge response tokens per user with identical token PINs and optimized troubleshooting.

OPTIMAL ADAPTATION THROUGH MODULAR ARCHITECTURE

Due to the modular construction of LinOTP you can decide yourself which authentication protocol you want to use and where your user information is stored. LinOTP is quickly and easily adaptable in order to fulfill your special requirements. The overview graphic highlights the high modularity of the solution. Apart from the actual LinOTP core all components can be randomly combined and also extended. For example it does not matter how many user repositories you use: LDAP, Active Directory, Novell eDirectory, diverse SQL server and Flatfile respond in mixed mode operation and can be arranged in realms / groups when and if required. Tokens can also be specifically allocated to one or several realms / groups. Even the authentication modules are interchangeable and further modules can be implemented when required for almost every use case. The administration can be run both under Windows and / or Linux via different Management Clients. In addition LinOTP offers a self-service frontend, through which the end users can themselves assign tokens or for example, can change their PIN number.



**MULTI-FACTOR-AUTHENTICATION
DESKTOP-INTEGRATION
TOKEN
SELF SERVICE & SUPPORT**



ADVANTAGES LINOTP

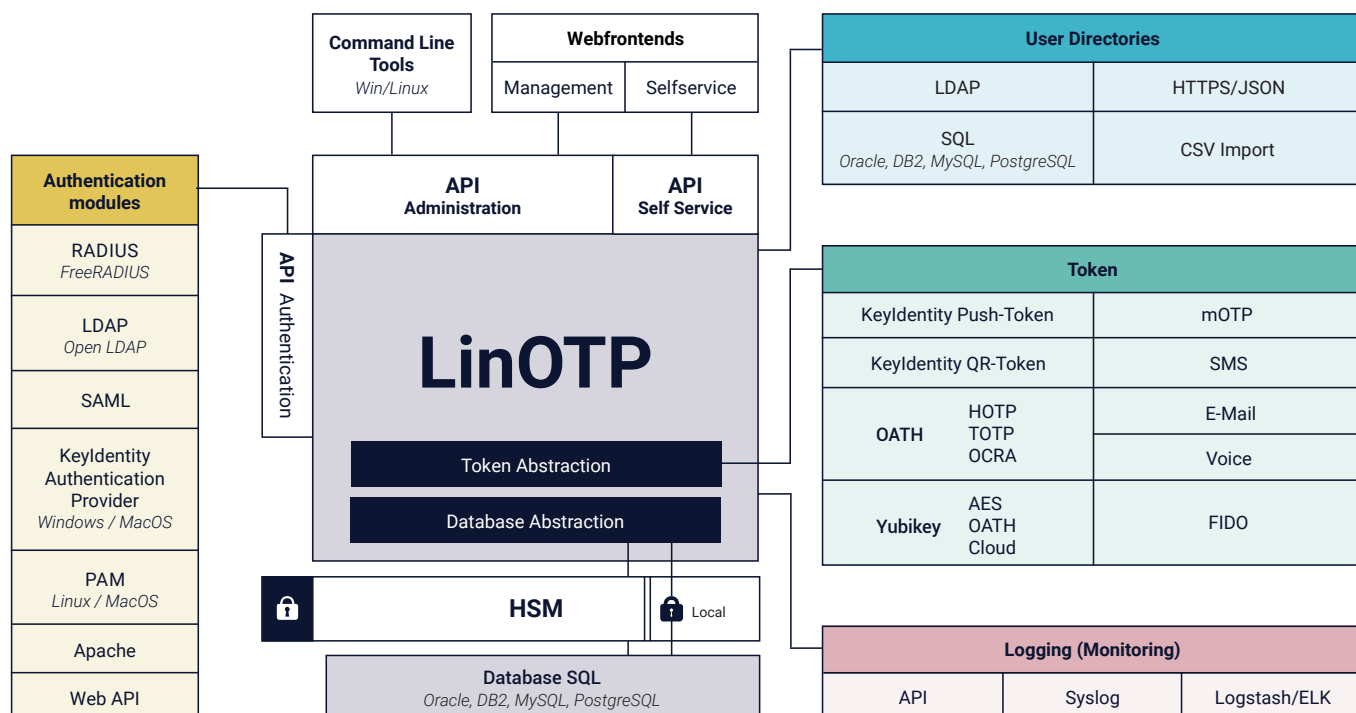
- ✓ Strong Two-Factor Authentication (2FA)
- ✓ Multi Tenant OTP Platform
- ✓ Easily to scale and to enhance
- ✓ Rapid Deployment
- ✓ Vendor-Independent
- ✓ Modulare Architektur
- ✓ Granular Rights and Role Management
- ✓ Open Source

LINOTP OFFERS MORE

- ✓ Support for diverseAuthentication Protocols
- ✓ Granulare Rechte- und Rollenverwaltung
- ✓ Multiple User Databases
(Microsoft Active Directory, LDAP, SQL Databases, Flat File)
- ✓ Powerful WebAPI (RESTful)
- ✓ Services and Support are operated from Germany
- ✓ High-Availability
- ✓ Large Scale Capabilities
- ✓ Graphical User Interface and Web API for ManagementWeb API
- ✓ User Self Service

INSTALLATION OPTIONS

- ✓ LinOTP Smart Virtual Appliance (SVA)
- ✓ Software packages for Linux



Supported Tokens (Extract)

- | | | |
|--|---------------------------------|--|
| ✓ FIDO / U2F Token | NET, Ezio Token | ✓ Remote Token |
| ✓ SafeNet eToken NG-OTP, eToken PASS | ✓ HID ActiveID OTP Token | ✓ Radius Token |
| ✓ SafeNet Safeword Alpine | ✓ SmartDisplayer Karten | ✓ Tagespasswort Token |
| ✓ Feitian C-100 / C-200 / C-300 | ✓ NagraID 106 / 103 | ✓ QR-TAN Banking Token |
| ✓ Feitian C-601 (Optical OCRA) | ✓ SMS OTP Token / Mobile TAN | ✓ Free Softtoken mOTP |
| ✓ Vasco DIGIPASS-Token (OATH and VACMAN) | ✓ Authenex A-Key V 3.6 | ✓ Each HOTP / TOTP and OCRA Token |
| ✓ Yubico Yubikey, Nano, NEO | ✓ BR Token SafeSIGNATURE | ✓ Mobile Apps for iPhone and Android like FreeOTP, Google Authenticator, OATH Token, Droid OTP |
| ✓ Gemalto IDProve Serie, IDPrime. | ✓ Validustech BC-30, CR-1, PB-1 | |
| | ✓ Simple Pass Token | |

MULTI TENANCY & CLOUD READINESS

The realm based concept, the flexible assignment of tokens, as well as the highly differentiated granular rules for different administrator and user roles makes LinOTP an ideal tool for service providers (XSP's), that with one single LinOTP setup would like to serve several customers / tenants, who have their own user databases. Even in the strongly growing Cloud Provider market the simple connection possibility via Web API meets with approval. Streamlined HTTPS-Requests enable the quick integration of an OTP authentication in any existing Web-Applications.

MANAGEMENT CLIENTS

LinOTP Management Clients also use streamlined connections via a Web API to communicate with the LinOTP Server. Thus selected management functions can be effortlessly integrated in existing Identity Management Frontends or Helpdesk-Portals. Based on the appropriate policies administrators can also adjust which feature set shall be made available to users.



OATH CERTIFIED

LinOTP (version 2.4 and up) is OATH Certified.

KeyIdentity GmbH
Robert-Koch-Straße 9
64331 Weiterstadt

Tel +49 6151 86086-277
Fax +49 6151 86086-299

www.keyidentity.com
info@keyidentity.com

