OpenOTP
Authentication Server

RCDevs security solutions

Product information

The need to secure access to online applications and resources is increasing every day. This is the result of the business evolution where companies' staff work from remote locations, use mobile devices and develop their corporate or external services on the cloud. In this context, it is important that employees, customers and collaborators get strongly identified and authenticated when accessing sensitive systems and data.

With RCDevs OpenOTP you can:

- Achieve strong security for your critical systems with a convenient and efficient user experience.
- Save costs with lower solution TCO and very minimal maintenance requirements.
- Comply with regulatory requirements in the government, industry, healthcare or financial sectors.

Enterprise-Grade Security Solution

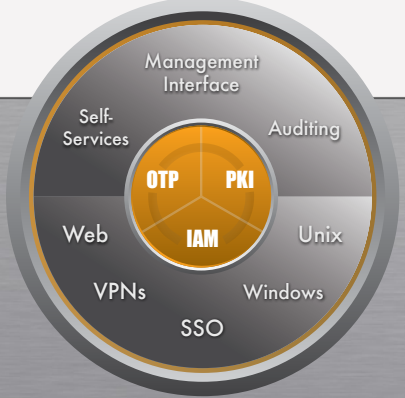
OpenOTP is the most advanced two-factor authentication solution ever. It is versatile, device-independent and based on opened security standards. OpenOTP provides fine-grained user identity and access management (IAM), one-time passwords authentication technologies (OTP), signed authentication with FIDO Universal Second Factor (U2F) and extensive authentication policies for your AD / LDAP users. It is enterprise-ready with strong support for high-availability, load-balancing, multi-tenancy, cloud-readiness, geolocalization, delegated administration and much more.

OpenOTP includes WebADM Server: the RCDevs' centralized interface used for managing your authentication policies, LDAP users, groups and domains while abstracting the complexity of high-level security. It includes user self-services with Token self-enrollment. It natively supports ActiveDirectory, Novell eDirectory, OpenLDAP, Oracle Directory, RCDevs Directory...

OpenOTP provides two-factor authentication with a maximum of flexibility, ease of installation and use. Even though it offers the highest level of functionality available in the market, it is designed for higher performances and simpler integrations. As a result OpenOTP is the only solution with such a set of features, which is being successfully deployed by thousands of companies without requiring any additional assistance.

Hardware Security Module

OpenOTP supports Hardware Security Modules (HSM) from Yubico. HSMs provide hardened storage of critical data with stronger cryptography where the encryption keys are hardware-protected. HSMs provide true random numbers generation (RNG) too. Quality random is required for Token seed generation and out-of-band OTPs.
Using HSMs in OpenOTP is 100% transparent and the move to hardware cryptography can be done at any time without impacting your business. RCDevs WebADM server supports up to 8 HSM modules in hot-plug mode for fault-tolerance and increased performances.



Flexible Licensing and Competitive Pricing

With its flexible licensing options and very competitive pricing, OpenOTP brings an unbeatable combination of cost-efficiency and security to corporate access, Web applications and cloud services. OpenOTP Enterprise Edition is available via permanent licenses or subscription-based models. The whole solution is completely free of charge for trials and for organizations with up to 40 users. In most scenarios OpenOTP has no integration cost. You do not need technology experts and expensive consultancy to start with the OpenOTP two-factor experience!

Resilient Solution for Cloud and Corporate Access

OpenOTP Server can be installed on any Linux box (hosted, virtual or dedicated) and is able to operate in both corporate or cloud service mode. The Linux platform has been chosen for its robustness, security and maintainability. Pre-configured virtual appliances are available for free on RCDevs' Website for a quick and simple testing.

RCDevs provides its customers with remote installation and configuration services for both standalone and cluster setups.

Go to http://www.rcdevs.com/downloads/ to start OpenOTP now!

Authentication Methods
- Event-based Tokens
- Time-based Tokens
- Challenge-based Tokens
- U2F Devices
- SMS OTP
- Mail & Secure Mail OTP
- YubiKey
- Printed OTP Lists
- Emergency OTP
- Simple LDAP

LDAP Compliant
- MS Active Directory
- Novell eDirectory
- Linux OpenLDAP
- Apple Open Directory
- Oracle / Sun Directory
- RCDevs Directory Server
- 389 Directory

Integration APIs
- RADIUS RFC-2865
- SOAP & XML-RPC
- JSON & JSON-RPC
- OpenID 1.1 & 2.0
- C, C++ Libraries
- SAML 2.0
- PAM-UNIX Plugin
- Credential Provider

Supported with
- Web Applications
- VPNs & SSL VPNs
- Citrix Access Gateway
- Microsoft (TMG, OWA, ADFS)
- UNIX / Linux
- Windows Login
- Google Apps

Awards Winner

CARTES 2012

SC MAGAZINE

http://www.rcdevs.com • Info@rcdevs.com

OpenOTP
Authentication Server

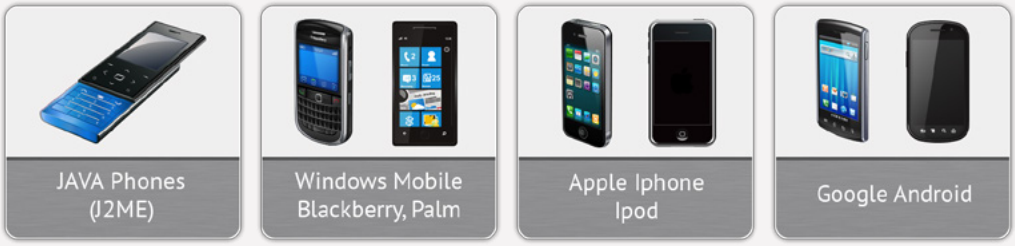
RCDevs security solutions

Product information

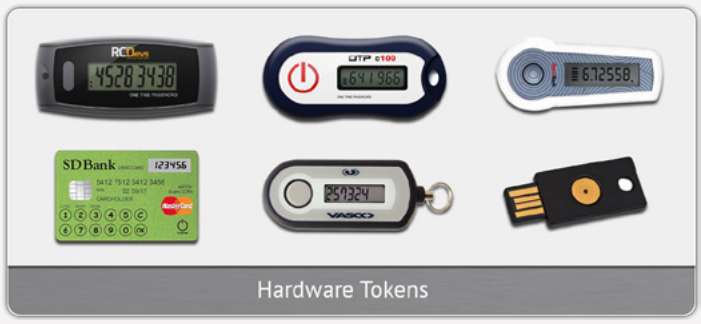
Client Support and Interfaces

OpenOTP provides two-factor authentication with OATH Software and Hardware Tokens, mobileOTP, Google Authenticator, Yubikey, out-of-band authentication with SMS, mail and secure-mail, printed OTP lists. It supports multiple Tokens per-user, fallback OTP, combined LDAP+OTP, PIN code, concatenated passwords, Token inventories, etc...

OpenOTP supports OATH Event-based, Time-based and Challenge-based standards for both Software and Hardware Tokens. Software Tokens are available free-of-charge for J2ME mobile phones, Windows Mobile, Palm, Blackberry, iPhone and Android platforms.



OATH-compliant Hardware Tokens with any form-factor are supported. This includes keychain-like or keypad-based OTP calculators, banking cards, Yubikeys, etc... RCDevs provides its own time-based OTP Token for OpenOTP. Yet customers are free to choose and re-use Hardware Tokens from any third-party provider: RCDevs solutions are 100% vendor-independent and also support OATH devices from well-known vendors like Feitian, Vasco, Secutech, SmartDisplayer, SafeNet...



You can use OpenOTP with:

- Web Applications (Java, PHP, ASP, .Net...)
- VPNs, SSL-VPNs (Checkpoint, Cisco, Nortel, Juniper, F5, Aventail...)
- Citrix Access Gateway & Web Interface
- Microsoft ISA/TMG (Exchange, Sharepoint...)
- UNIX and Linux (SSH, FTP, OpenVPN, PPTP, POP/IMAP...)
- Windows Login (2008-R2 Server, Vista, 7, 8)
- Web-based Products (Wordpress, SugarCRM, Magento, Drupal, Joomla, RoundCube...)
- Active Directory Federation Services (ADFS)
- OpenID-enabled Web Sites
- SAML-federated Applications and Google Apps
- Amazon Elastic Compute Cloud (EC2)
- Any Other System (with our development SDK)

OpenOTP provides powerful integration APIs and plugins for Web (SOAP/XML/JSON), VPNs (RADIUS), SSO (OpenID/SAML), UNIX (PAM), Windows (Credential Provider). The APIs are designed for simpler integrations and to let programers easily implement two-factor authentication functionalities into existing Web applications and remote access infrastructures.

RCDevs is an award winning security company specialized in next-generation two-factor authentication. RCDevs is building its growing reputation over high-quality security software and its customers' entire satisfaction. RCDevs provides cutting-edge enterprise-grade solutions in world-wide to customers ranging from SMEs to large corporations in the IT, financial, healthcare and government sectors.

RCDevs is the developer of OpenOTP™ Authentication Server (http://www.rcdevs.com/products/openotp/) and TiQR Server (http://www.rcdevs.com/products/tiqr/).

RCDevs' OpenOTP and TiQR Authentication Server received the Highly Commended Award for the Best SME Security Solution at SC Magazine Awards 2012 Europe and the Sesame Awards 2012 for the security innovation.

Technical Specifications

- Hardware / Software OATH Tokens
- FIDO Universal Second Factor (U2F).
- Google Authenticator with QRCodes
- Fallback OTP Methods
- Up to 3 Tokens per User
- Token Inventory Management
- PSKC RFC-6030 Token Import
- Combined LDAP+OTP/U2F Authentication
- Challenged or Concatenated OTP Passwd
- OTP PIN Prefix Protection
- Policies per User, Group, Domain, Client
- Policies per Network & Geolocalization
- Access Time Policies
- User Blocking Policies
- Built-in Replay Attack Protections
- AES-256 Encryption for Sensitive Data
- No Replication nor Import of LDAP Users
- Multiple LDAP Sources (Aggregated)
- User Transaction Duplicates' Protection
- Customizable End-User Messages
- Comprehensive Logging and Accounting
- Multilingual Support for User Messages
- Mail and SQL System Alerts
- Automatic Failover for LDAP, SQL...
- PCI-DSS Compliant

System Requirements

- Compatible LDAP / AD Directory
- Networking with DNS and NTP
- Optional SMSC Service Connection(s)
- Linux 32 / 64Bit (Dedicated or Virtual)

Performances and Scalability

- High Availability with 2-4 Active Servers
- Full Load Balancing and Session Sharing
- 175 Logins per Second and per Server on an Entry-Level Server (Intel-based)
- Multi-Tenancy and Cloud Readyness

http://www.rcdevs.com • Info@rcdevs.com