multiOTP®

OATH initiative for open authentication CERTIFIED

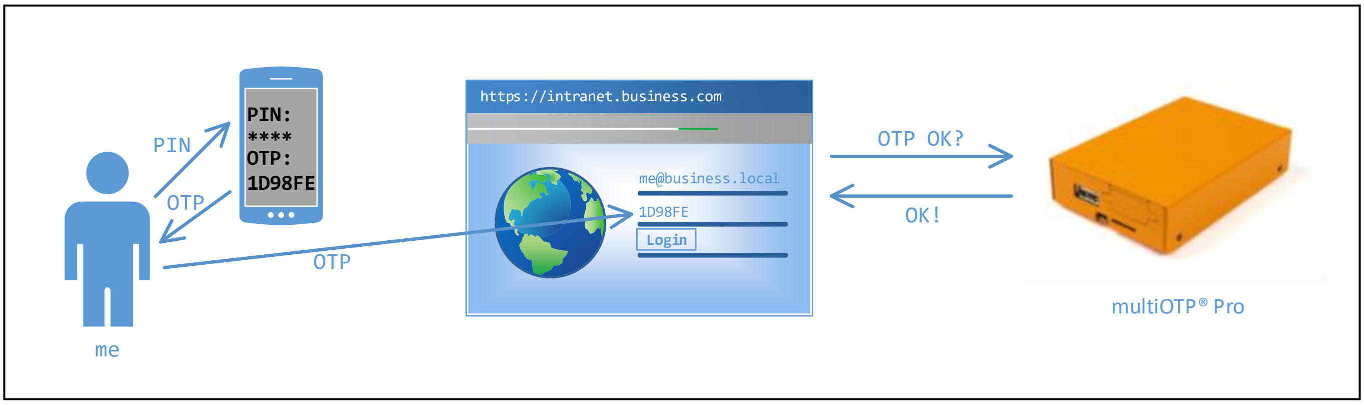
Because a single password doesn't protect you anymore!

The One Time Password (OTP) system is the best protection against password stealing. The password generated is valid only during a short period of time and cannot be used more than once.

The multi*OTP*® solution helps you to quickly and effectively setup a standalone RADIUS strong authentication system that covers your needs for a reasonable price.

Easy, quick, inexpensive.

2023-09-22



multi*OTP*® lets you use your smartphone as a password generator. The new generated password, combined with your own PIN code or your AD/LDAP password, allows you to login on your extranet portal or access your company network through VPN.

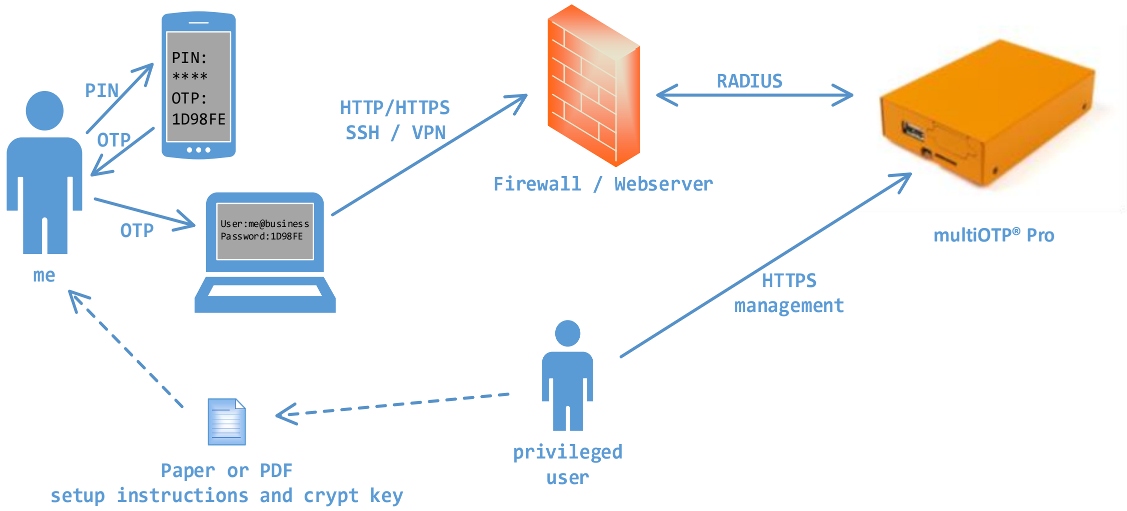
Thanks to a free mobile app available for your iPhone or your Android, deployment is much easier and faster than any *key-tokens* or *one-time-pads*!

Password generator can be set up quickly on a smartphone by catching a QRcode printed on each private information page generated by **multi*OTP*®**.

This system combines pragmatism and security. Very easy to setup and available at an affordable price, it's an ideal solution for companies of any size!

Any OATH hardware tokens are also supported and easy to deploy thanks to a self-registration process. For the first login, just type the username and the serial number of the token followed by the generated password, and the token is accepted and directly attributed to the user!

Based on the RADIUS protocol, **multi*OTP*** ® can be used for multiple purposes: VPN authentication, SSL-VPN connections, extranet portals, etc. This protocol is implemented in many common appliances and software (firewall, Apache HTTP server, OpenSSH, etc.).



multi*OTP* ® is available as a low power hardware device or as a virtual appliance.

More information, list prices, online demo, free virtual appliance and other resources are available on our website: **https://www.multiotp.com**

Key features

multi*OTP*®	Device	Pro (virtual)	Enterprise (virtual or RPI)
Setup in 10 minutes	yes (plug'n'play)	yes (VMware, Hyper-V, OVA standard)	
Initial user licenses	20 integrated	1 free	
Maximum number of users	500		100'000
Raspberry Pi binary image (1B, 1B+, 2B, 3B, 3B+, 4B)	no		yes (limited to 500 users)
Second instance synchronization for high availability	no		yes (master-slave(s) HA)
API REST availability for automation and authentication	no		yes
Other enterprise functionalities	no		yes
Size (in mm) / Disk space	62 mm x 21 mm x 90 mm	16GB virtual disk	
Consumption / resources	< 5 W, USB powered	4 vCPU, 4GB RAM	
Console availability for network parameters configuration	no	yes	
Maintenance / update	Free minor version update 20% installed licences prices for major version		Included the first year 20% installed licences prices / year
Easy to use web management interface	yes		
Active Directory / LDAP automatic users synchronization	yes, based on group(s) membership, with automatic tokens creation and distribution		
Active Directory / LDAP passwords instead of PIN codes	yes (PAP)		
Supported hardware/software/paper tokens	OATH TOTP, OATH HOTP, mOTP, YubiKey, SMS, TAN (scratch password list)		
PSKC token file support	yes, including AES-128-CBC and PBE		
Free Windows multiOTP Credential Provider (open source)	yes		
Free software tokens creation	yes		
FreeOTP or Google Authenticator compatible QRcode	yes, PDF generation with customizable templates		
Supports challenge/response mode	yes, including specific challenge message when waiting for SMS code		
SMS one time code support	yes (Clickatell, IntelliSMS, ASPSMS, Swisscom, eCall, Nexmo, Afilnet)		
Unlock token process for the end user	yes, transparent process (prefix + OTP[n] + space + OTP[n+1])		
Street price (VAT included)	CHF 499.-	free, with 1 free user	
Street price for 10 additional users (VAT included)	CHF 200.-		CHF 350.-