



EUTRONSEC

INFOSECURITY

OTP: The next generation



WebOTP



NOW A MEMBER OF Aladdin
EUTRONSEC



WebOTP

This solution comes with a particularly aggressive price and it allows secure authentication with a WEB server. The main feature of this token is the possibility to send authentication information via the USB port of the computer without having to install any software and/or driver and without also any need for administrator privileges. The WEB server receives an authentication string that contains the user's ID and an incremental counter; it is absolutely secure thanks to double encrypting carried out with AES 256 bit algorithm by using first the user's private key and then the WEB server's.



WebOTPtime

The product uses the same technology of the base product with the addition of the time factor inside the authentication string though. Indeed the USB token contains a timer that is synchronized with the WEB server's. An even more secure solution then, ideal also for home banking projects.



Practical applications

- Control of access to Website allocated areas for:
- Remote management of sales networks and Competence Centers
 - Selling of by-consumption services on the Internet
 - Online publishing
 - Secure management of ASP services
 - Selling of software and computer services on the Internet
 - Secure access to financial and insurance services
 - Controlled release of information
 - Home Banking

WebOTP product features

The main features of WebOTP that distinguish it from a traditional OTP unit are as follows:

Usability The interaction requested to the user is extremely reduced. The user is only requested to insert the device in a USB port upon authentication.

Identification Besides being authenticated the user is also identified. Therefore it is not necessary to request the user an identifier like a username before authentication.

Secure authentication Authentication is based on 128 information bits and on the AES 256 bits algorithm. It is therefore almost impossible to carry out a brute force attack.

In WebOTP the authentication is based on the use of the AES 256 bit symmetric cryptography algorithm, as opposed to the common hash algorithm used by traditional OTP devices.

Using a symmetric cryptography algorithm is possible for WebOTP thanks to the USB connection which does not prescribe any length limits in the authentication code. Symmetric cryptography requires operating with an authentication code of at least 128 bits, many more bits than a traditional OTP display with few figures can display.

The advantages of using a symmetric cryptography algorithm during OTP authentication are manifold:

Identification Besides authentication the user, it is also possible to identify him/her. It is therefore possible for the user to avoid identification upon authentication. By comparison a traditional OTP unit always demands to know who the user is in advance.

Security The authentication code contains 128 bit of security information. By comparison, the traditional display-equipped OTP's use maximum 40 bits, often fewer.

Speed The authentication check is easy and quick. The authentication server will be submitted to a much reduced workload. By comparison a traditional OTP unit with hash function requires a process by attempts for guessing the time values or the events used by the device.

Resistance to Brute Force Attack Given the high security level of the authentication, it is not necessary to block access to the users after a certain number of unsuccessful attempts. By comparison, a traditional OTP device is obliged to use block techniques for preventing brute force attacks.

Resistance to DoS Attack The authentication server is especially proof against Denial Of Service - type attacks, which are programmed for requiring a high number of fictitious authentications in the attempt of blocking user access. The authentication check is very quick also in case of failure. By comparison, with a traditional OTP unit based on hash function a failed authentication case is always the worst possible event in terms of performance time.

Effective error management In case of authentication failure, it is possible to know the exact reason of the failure. In particular it is possible to distinguish between errors due to faulty devices and errors due to attack attempts. For instance, it is possible to continue to use a time-based device with a flat battery as if it was an event-based device. By comparison, a traditional OTP unit with hash function has always got only one type of authentication failure and no further information is possible to infer from the error.

Requirements

- **Client** Windows 98 or higher, Mac OSX, Linux 2.4 or higher
- **Browser web** Internet Explorer, Netscape, Mozilla, Firefox, Camino
- **Server** The developer's kit allows the integration with every web authentication platform
- **Authentication system** OTP event based, challenge/response optional
- **Encryption** AES 256 bit on board, SHA 256
- **Authentication variables** incremental counter, WebOTPTime has also an internal timer
- **Application PIN** implementable
- **Supply Battery** WebOTPTime has an internal battery with 5 years of use guaranteed.
- **Driverless**

