One-Time Password

17.05.2024 11:52:41

FAQ-Artikel-Ausdruck

Kategorie:	RRZE: Glossary	**Bewertungen:**	0
Status:	öffentlich (Alle)	**Ergebnis:**	0.00 %
Sprache:	en	**Letzte Aktualisierung:**	11:29:01 - 30.06.2010

Schlüsselwörter

Identity, Security

Symptom (öffentlich)

Problem (öffentlich)

Lösung (öffentlich)

OTP - A temporary password generated by a time-based algorithm that is then compared to a server-calculated password. It is only valid within a short time "window" (such as one minute) and can (preferably) only be used once within that time window. Also known as Time Synchronisation. The server and the token clocks need to remain synchronised over time and processes are usually implemented to adjust for that. The passwords are usually 6-digit codes and usually generated by a device, either after the entry of a PIN or with a continuous display of the next OTP (ie no PIN required). For example; a hardware token with a display screen, either with or without a keypad. Those with a keypad are two-factor devices ("have" the device and "know" the PIN), whereas those without a keypad are really only a single-factor device. For the latter to become a two-factor solution a PIN/Password can be keyed into the PC along with the OTP during the logon process. Some would argue that constant-display tokens are still only a "single-factor" solution because two passwords are needed (both "know") for authentication (and only one password is needed in the case of a stolen or found OTP constant-display token).

Other methods of generating the OTP are possible, such as where the PIN entered into the token is combined with the token's code to create a single pass-code (this method is prone to user error, as the PIN is not checked by the token, only by the OTP server). Another method consists of the OTP being distributed by the server (eg to a mobile phone or PDA) and then returned to the server in an authentication session within the allowed timeframe - this method should use digital signing of the distribution of the message, for enhanced security.

'One-time Pads' require that both parties have an identical list of pairs of numbers, words, or symbols, preferrably randomly generated. Once a choice has been used, it is crossed off the list and never used again. This method can also be used for "shared secrets" - see Secret Q&A ["https://www.rrze.wiki.uni-erlangen.de/index.php/Glossar#Secret_Q.26A"].

Source: "http://identityaccessman.blogspot.com/2006/08/identity-dictionary.html"