Infosheet

NCP Advanced Authentication

SECURE COMMUNICATIONS

Next Generation Network Access Technology

NCP Advanced Authentication

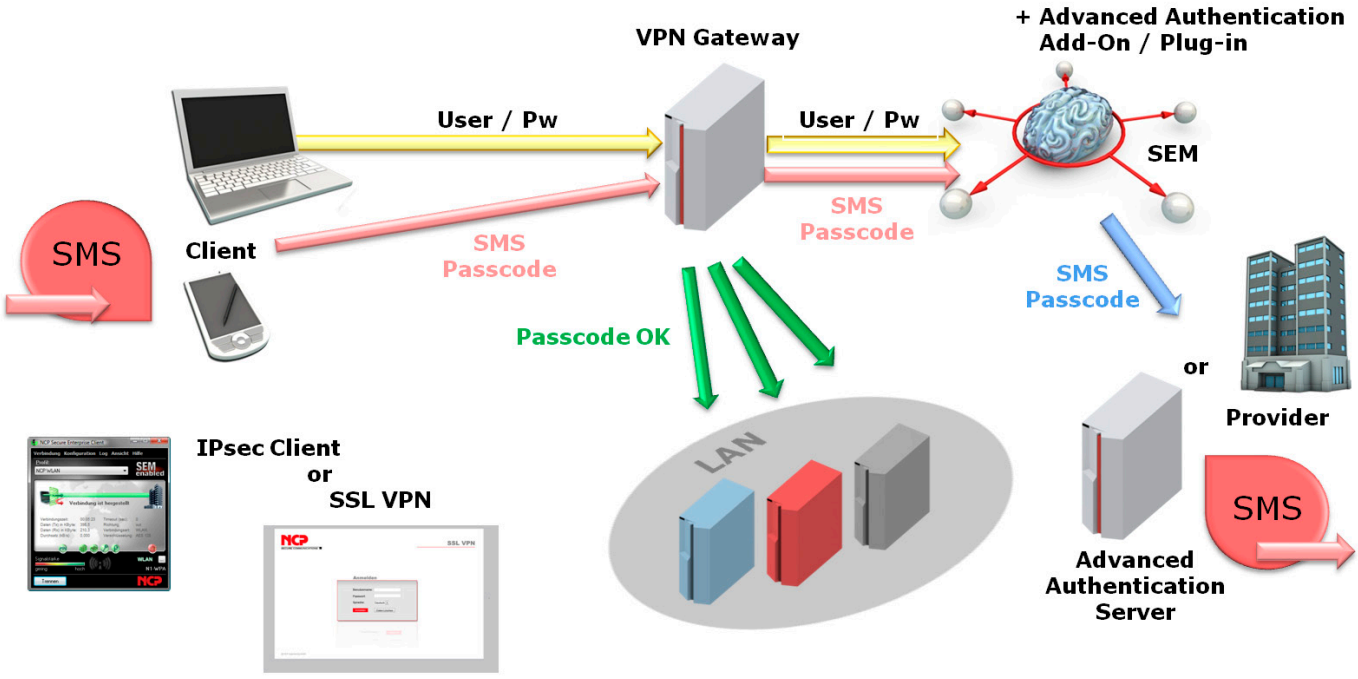
Since the release of version 3.0 of NCP's Secure Enterprise Management, NCP has been offering its customers strong authentication through text messages (SMS). This authentication process is an alternative to fee-based supplementary solutions of third party suppliers and is available for IPsec and SSL VPN solutions.

Strong authentication processes are based on the necessity of ownership and knowledge. First, the user has to know his password for login and second, he has to own a device that provides a one-time password for login as well. This one-time password is only valid for a limited time-span and a single login/session.

In contrast to solutions with hardware tokens, strong authentication through text messages (SMS) has the advantage that the user receives a one-time password which the system generated by chance at login. A token-based solution has to have a spreadsheet readily available at the authentication server and the spreadsheet has to contain a one-time password for each token, depending on the time. This leaves a potential risk if the authentication server is compromised or this spreadsheet falls into the wrong hands. Such authentication solutions further have the drawback that the hardware tokens have to be replaced after some time, a process that naturally results in additional costs. For authentication via text messages (SMS) a simple cell phone is completely sufficient and a modern smartphone is not necessary.

NCP's advanced authentication offers two possibilities to send text messages. The option for small scale environments with a small number of users is NCP's advanced authentication con-nector which comes free of charge, naturally. The advanced authentication connector is a Windows software which has to be installed on a computer with connected 3G / GSM hardware. When NCP's Secure Enterprise Management generates a one-time password for a user who is logging in, it transmits the password to NCP's advanced authentication connector via secure HTTPS and the connector then sends it to the user as text message (SMS). NCP had to separate the two components since NCP's Secure Enterprise Management Server are usually installed on computers in shielded data centers. For large scale environments with a high number of users NCP offers a HTTPS interface to predefined text message (SMS) service providers.

NCP's advanced authentication provides the user with a secure second factor for authentication. Creation and distribution of the one-time password as text message (SMS) is only initiated when the user has authenticated his identity with a first, permanent password.


VPN Gateway
+ Advanced Authentication
Add-On / Plug-in
User / Pw
User / Pw
SEM
SMS
Client
SMS
Passcode
SMS
Passcode
SMS
Passcode
Passcode OK
or
Provider
LAN
IPsec Client
or
SSL VPN
SMS
Advanced
Authentication
Server