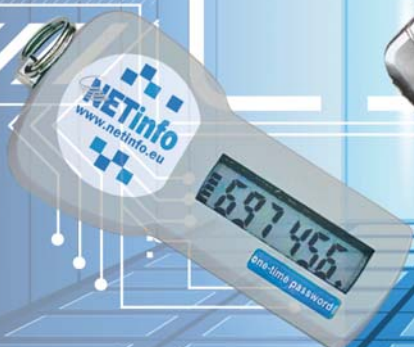


SCANNING ...



# The Smart Move

## ▶ NETteller Authentication Suite 2-Factor User Authentication via Mobile Device and/or OTP Token



### DEFINITION

Two-factor authentication is a security process in which the user provides two means of identification, one of which is typically a physical token, such as a card, and the other of which is typically something memorized, such as a security code. In this context, the two factors involved are sometimes spoken of as *something you have* and *something you know*.

A common example of two-factor authentication is a bank card: the card itself is the physical item and the Personal Identification Number (PIN) is the data that goes with it.

### Why 2-Factor Authentication?

A two-factor authentication could drastically reduce the incidence of online identity theft, phishing expeditions, and other online fraud, because the user's password would no longer be enough to give a thief access to their information.

Using more than one factor of authentication can also be called strong authentication; using just one factor, for example just a password, is considered weak authentication.

### What is NETteller Authentication Suite?

NETteller Authentication Suite is an Authentication Server utilizing both a Mobile Phone and/or an OTP Token, which allow e-Businesses to enhance their user security easily, quickly, affordably and with little implementation risk.

NETteller Authentication Suite does this by providing an innovative authentication solution that protects access to Web-based resources by providing a 2-Factor user authentication through the use of existing mobile phones and/or OTP Token. NETteller Authentication solution serves to overcome the security inadequacy of the Internet/Intranet, by allowing a user to authenticate itself using its personal mobile phone or the NETinfo OTP Token.

### e-Banking and NETinfo Authentication Server

It is a big issue for Banks to properly identify the customer that is using their e-Banking services. Online fraud has been increasing over the years to alarming figures. Although there are lots of ways to improve the security of online transactions, is relatively simple to implement and could reduce the risk of transactions, in a most cost effective and convenient way, either by using SMS TAN (Mobile phone) or OTP Token device.

**SMS TAN and OTP Token; Two Authentication options in one package.**

### SMS Authentication

SMS authentication is not more than sending an SMS message to the mobile phone of the customer that is in the process of performing an online transaction. In this message we send a code (TAN) that must be entered by the online Banking user as part of the transaction process.



37 Stasicratous Street, 1st Floor  
1065 Nicosia, P.O. Box 22658  
1523 Nicosia, Cyprus  
Tel: +357 22 753636, Fax: +357 22 765680  
URL: [www.netinfo.eu](http://www.netinfo.eu), [www.netteller.eu](http://www.netteller.eu)  
e-mail: [netteller@netinfo.eu](mailto:netteller@netinfo.eu)



As an idea it could not be simpler:

- No Software installation on customer's Mobile Device.
- Online internet banking customers will need to have their mobile phone close to hand if they want to use any functionality that requires TAN (Transaction Authentication Number).
- TAN is automatically generated by NETteller Authentication Server, and is valid only for the specific time, the open session and the specific transaction.
- After logging on to e-banking or when they request for a transaction specific TAN, customer will receive an eight-digit code by a text message to their mobile phone, which they will need to enter online within the specific time limit (ie. 5 minutes) to complete the transaction.

SMS authentication system will ensure fraudsters can't raid people's bank accounts simply by finding out their password and log-in. This is because they would also need the customer's mobile phone to obtain the eight-digit code; they need to have the same session ID and to perform the specific Transaction for which the TAN was generated.

SMS TAN, it's more secure than a simple username and password. It's easy to implement, with no extra hardware and no software installation on mobile devices. It's easy for the customers to understand and use.



### OTP Token Authentication

The NETInfo OTP Token is a high quality One Time Password device designed to provide strong user authentication. It is fully integrated into the NETInfo Authentication Server as an alternative to SMS TAN, giving the user the flexibility to use either SMS TAN or the OTP Token.

When using NETInfo OTP Token for authentication, the user just input the 6 digit dynamic password displayed on the screen to the system to authenticate. The password is change/renew every 60 seconds to ensure greater security. No need to press any button; very easy and simple to use token.

#### NETInfo OTP Token key features

Size:	55 x 25 x 9 mm
Display	8 character LCD display
One Time Password update time:	60 seconds
Operating Temperature	-40 to 100 degrees Celsius
Humidity	Waterproof
Battery life	4,5 Years
Robustness	Can be dropped from a height of 15 m

### How NETteller Authentication Server Works

The Two-factor authentication combines something you have; your mobile device or a Token device. NETteller Authentication Server provides validation for "something you have" to enable strong authentication of end users.

The user has to option to use either its mobile device or the OTP Token.

