

# NET-TAN Authentication Server

## User Authentication via SMS Mobile Devices

### Based on 2-Factor Strong Authentication

- Easy to implement
- Easy to understand
- Easy to use
- No extra hardware

### SMS alerts

#### SMS TANs

- User Authentication
- Transaction Authentication
- Session specific
- Transaction specific
- Time duration specific

## 2-Factor User Authentication via Mobile Devices

### 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 NET-TAN Server?

NET-TAN is a Mobile Authentication Server that can allow eBusinesses to enhance their user security easily, quickly, affordably and with little implementation risk.

**NET-TAN Server** 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. NET-TAN serves to overcome the security inadequacy of the Internet/Intranet, by allowing a user to authenticate himself using his personal mobile phone.

### Online Banking and NET-TAN

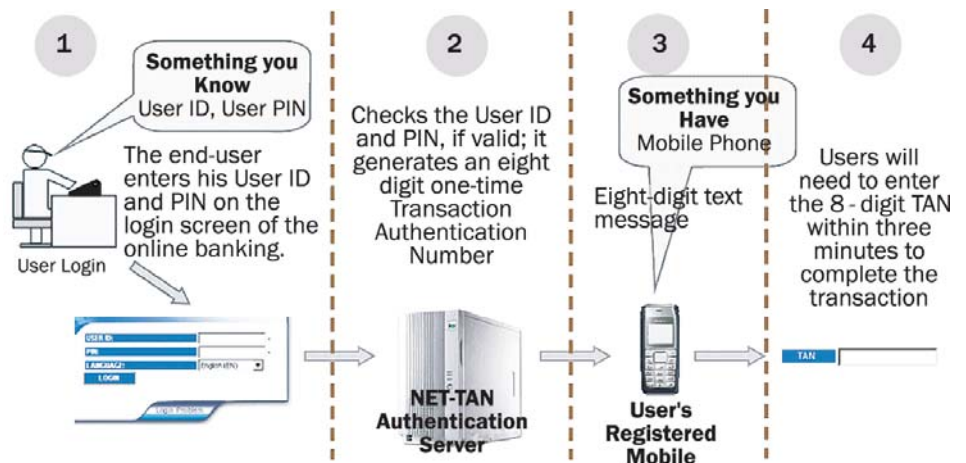
It is a big issue for Banks to properly identify the customer that is using their online Banking services. Online fraud has been increasing over the years to alarming figures. Although there are lots of ways to improve the security of online transactions, NET-TAN, is relatively simple to implement and could reduce the risk of transactions.

SMS authentication is not more than sending a SMS message to the cell phone of the customer that is in the process of performing an online transaction. In this message you will send a code that must be entered by the online Banking user as part of the transaction process. As an idea it could not be simpler:

- Online internet banking customers will need to have their cell phone close to hand if they want to use any functionality that requires TAN authentication.
- After logging on to internet banking or when they request for a transaction specific TAN, customer will receive an eight-digit text message to their cell phone, which they will need to enter online within three minutes to complete the transaction.

NET-TAN 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 cell phone to obtain the eight-digit code.

NET-TAN, it's more secure than a simple username and password. It's easy to implement, with no extra hardware. It's easy for the customers to understand and use.



# NET-TAN Authentication Server (2-Factor Authentication via Mobile Devices)

1



**SUBMIT**



The user submits the transaction

2

The user is displayed with the Pre-Confirmation screen with all Transaction's details.



**Request TAN**

The user requests for a Transaction Authentication Number (TAN).

3

The NET-TAN Authentication Server, identify the user ID and generates a Session specific, Transaction specific, one-time 8-digit TAN.



The NET-TAN Authentication Server

4

Eight-Digit text message



User's Registered SMS mobile device

5



**CONFIRM**

("TAN"):

The user must enter the 8-digit TAN within the specified time limit (2-3 min) and confirm the transaction.

6

The NET-TAN Authentication server checks the TAN against Session, Transaction, Time and User-ID in order to accept the transaction.

