

## 2 Фактора Аутентификации посредством SMS мобильного устройства

### Пользовательская Аутентификация посредством SMS мобильного устройства

#### Основана на сильной двухфакторной Аутентификации

- Легко внедряемая
- Доступная
- Легкая в использовании
- Не требует дополнительных аппаратных средств

### SMS алерты

#### SMS TANs

- Аутентификация пользователя
- Аутентификация транзакций
- Специфика сессий
- Специфика транзакций
  
- Установка лимита времени на проведение транзакции

### Как работает устройство

1. Пользователь вводит ID и PIN код для входа в систему интернет - банкинга.
2. NET-TAN Сервер Аутентификации проверяет ID пользователя и PIN код. При успешной верификации, генерируется одноразовый восьмизначный номер аутентификации определенной транзакции. Уникальный номер

### ОПИСАНИЕ

Двухфакторная аутентификация- процедура обеспечения безопасности, при которой пользователь идентифицируется, предоставляя не менее двух средств аутентификации, одно из которых, как правило, являет собой токен, как, например, карта, а другое обычно необходимо запоминать, например, код безопасности. В этом контексте два используемых фактора часто упоминаются как **нечто, что вы имеете и нечто, что вы знаете.**

Наиболее распространенным примером двухфакторной аутентификации является банковская карта: карта сама по себе является физическим телом, а код PIN представляет собой сопутствующие ей данные.

### Почему 2 Фактора Аутентификации?

2-х факторная аутентификация значительно сокращает уровень сетевого мошенничества и фишинга т.к. конфиденциальной информации о пользователе (ID пользователя и пароль) недостаточно для поддержания высокого уровня безопасности системы.

### Что такое NET-TAN Сервер?

NET-TAN Мобильный Сервер Аутентификации позволяет электронному бизнесу обеспечивать безопасность пользователя легко, быстро, доступно и с наименьшим риском реализации.

NET-TAN Сервер обеспечивает инновационное аутентификационное решение, которое защищает доступ к Web-базе через пользовательскую 2-х факторную аутентификацию при помощи мобильных устройств. NET-TAN служит для преодоления несоответствия безопасности Internet/Intranet, разрешая пользователю подтвердить свою подлинность, используя его личное мобильное устройство.

### Онлайн Банкинг и NET-TAN

Одной из актуальных проблем для Банков является идентифицирование клиентов, которые используют услуги онлайн банкинга. За последние годы число вторжений сетевых мошенников резко увеличилось. Использование NET-TAN значительно сокращает риск при проведении транзакций в системе онлайн.

SMS Аутентификация (Установление подлинности) это не более, как послание SMS сообщения на сотовый телефон клиента, который выполняет транзакцию в системе онлайн. В данном сообщении высылается код, который должен ввести пользователь онлайн банкинга, как часть процесса транзакции. Простой пример:

-Клиент Интернет - банкинга должен иметь при себе сотовый телефон, на случай использования функций, требующих TAN Аутентификацию.

- После входа в систему интернет – банкинга, будет запрошен определенный номер транзакции TAN, который будет выслан SMS сообщением на зарегистрированное мобильное устройство клиента. На проведение сессии система отводит не более 3-х минут.

NET-TAN система аутентификации гарантирует высокую безопасность проведения транзакций, легка и доступна в использовании, не требует дополнительных аппаратных средств.

транзакции TAN (Аутентификационный номер транзакции) посылается SMS сообщением зарегистрированному мобильному устройству.

3. Пользователь получает восьмизначное текстовое сообщение на его мобильное устройство.

4. Пользователь должен ввести восьмизначный номер TAN в течении трех минут, чтобы завершить транзакцию.

### NETinfo Plc

37 Stasicratous street,  
1st Floor

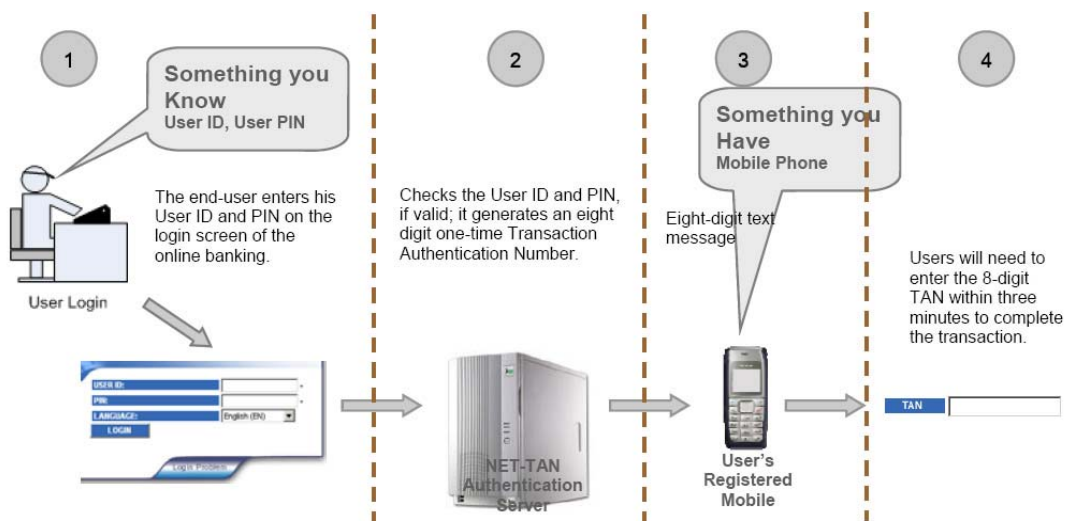
1065 Nicosia

Tel: +357 22 753636

Fax: +357 22 765680

Email: [mail@netinfo.eu](mailto:mail@netinfo.eu)

<http://www.netinfo.eu>



# NET-TAN Сервер Аутентификации (2-Фактора Аутентификации посредством мобильного устройства)

