eToken™

## Задачи обеспечения безопасности

### Двухфакторная аутентификация

- Строгая аутентификация с использованием PKI-технологий
- Аутентификация с использованием одноразовых паролей (One-Time Password – OTP)

### Управление паролями

- eToken Network Logon
- eToken Web Sign-On

### Безопасность данных

- Защита компьютера на этапе загрузки , шифрование данных
- Электронная цифровая подпись
- Безопасная электронная почта

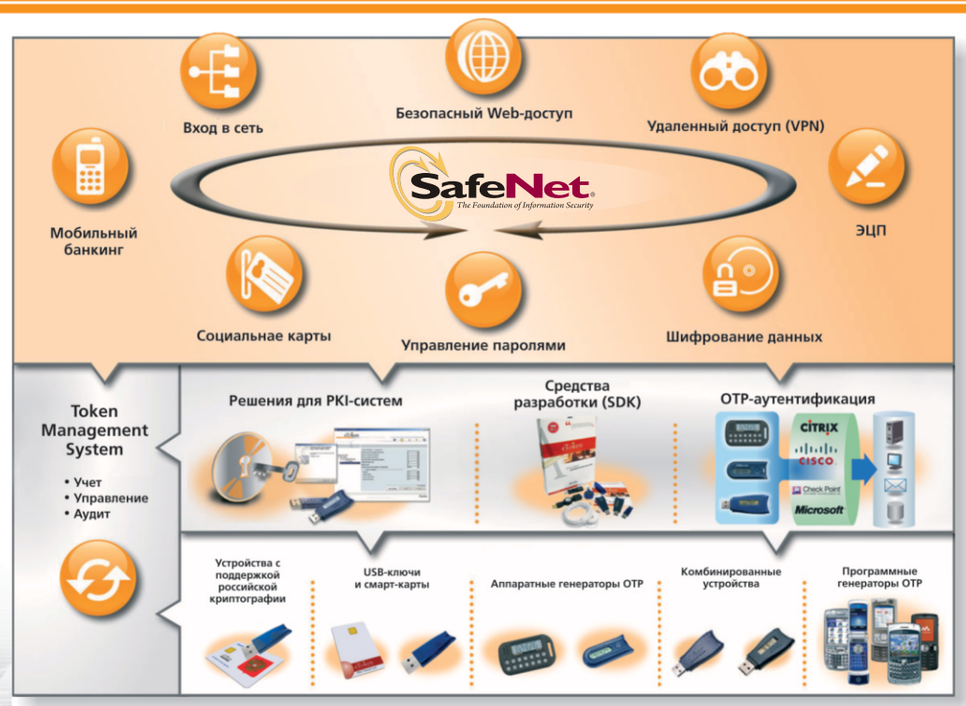
> *Рост интереса к средствам аутентификации и увеличившееся их разнообразие является следствием общего перехода от паролей к более надежным технологиям.*
>
> *Gartner, 2009*

## Линейка продуктов eToken

Компания « SNG Security » предлагает широкий спектр продуктов и решений для комплексного решения задач обеспечения информационной безопасности и защиты конфиденциальных данных.

Линейка продуктов eToken включает в себя аппаратные и программные средства аутентификации пользователей, программное обеспечение для их использования в PKI-системах, средства для создания инфраструктуры аутентификации любого масштаба, систему управления USB-ключами и смарт-картами, а также средства разработки для интеграции eToken со многими современными решениями в области информационной безопасности.

SafeNet® The Foundation of Information Security eToken™





*РЕШЕНИЯ НА ОСНОВЕ USB-КЛЮЧЕЙ И СМАРТ-КАРТ ДЛЯ*

***аутентификации и хранения ключевой информации***

SafeNet® The Foundation of Information Security


SafeNet® The Foundation of Information Security

"SNG Security"
Тел.: +7(727) 321-85-11
Факс: +7(727) 321-85=12
e-mail: info@sng-security.kz
www.sng-security.kz

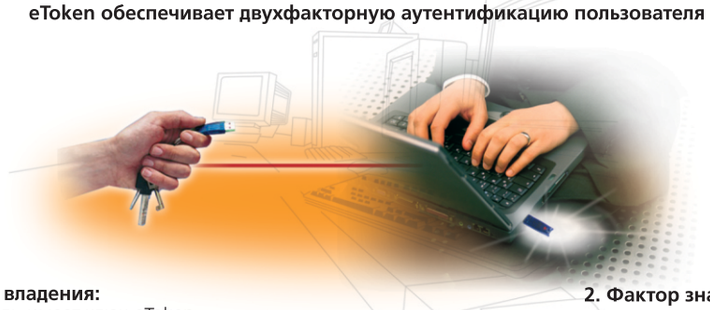
# eToken – персональное средство аутентификации и хранения ключевой информации

eToken компании «**SNG Security**» позволяет пользователям, IT-администраторам и администраторам безопасности более эффективно управлять процессом аутентификации, безопасно сохраняя в памяти eToken пароли, закрытые ключи, сертификаты открытого ключа, профили пользователя и другую информацию, нуждающуюся в безопасном хранении.

Использование eToken позволяет:

- повысить защищенность и обеспечить безопасный доступ к информации;
- эффективно управлять паролями;
- всегда иметь при себе персональные цифровые данные (сертификаты, ключи ЭЦП и шифрования, коды доступа), хранящиеся в защищенной памяти.

**eToken обеспечивает двухфакторную аутентификацию пользователя**



**1. Фактор владения:**
пользователь *имеет* ключ eToken

**2. Фактор знания:**
пользователь *знает* пароль ключа

# Для чего нужен eToken?

## Безопасный доступ

**Вход в сеть и на рабочие станции**

eToken позволяет осуществлять двухфакторную аутентификацию пользователей на локальной рабочей станции и при обращении к защищенным сетевым ресурсам. При этом могут использоваться как технология регистрации с использованием сертификатов инфраструктуры открытых ключей (PKI), так и стандартная аутентификация Microsoft (GINA API) с обычными паролями пользователей.

**Безопасность виртуальных частных сетей (VPN) и безопасный удаленный доступ**

eToken позволяет обеспечить двухфакторную аутентификацию пользователей при удаленном доступе к корпоративной сети. Он легко интегрируется с ведущими системами VPN и поддерживает различные методы аутентификации при доступе к VPN, включая одноразовые пароли и цифровые сертификаты.

**Web - доступ**

eToken позволяет обеспечить двухфакторную аутентификацию пользователей при доступе к защищенным Web-ресурсам и подпись конфиденциальных цифровых транзакций. eToken поддерживает несколько методов Web-аутентификации, включая одноразовые пароли и цифровые сертификаты.

# Модели eToken

## eToken PRO (Java)

eToken PRO (Java) – персональное средство аутентификации и защищенного хранения пользовательских данных, аппаратно поддерживающее работу с цифровыми сертификатами и ЭЦП, выпускается в виде USB-ключа и смарт-карты.

Рекомендуется для решения следующих задач корпоративных заказчиков:

- обеспечение строгой двухфакторной аутентификации пользователей в операционных системах и бизнес-приложениях (Microsoft, Citrix, Cisco Systems, IBM, SAP, Check Point), защищенное хранение ключевой информации казахстанского СКЗИ
- защита закрытых ключей ЭЦП пользователей в системах электронного документооборота, формирование ЭЦП документов и транзакций, обеспечение безопасной работы с электронной почтой;
- защита закрытых ключей ЭЦП пользователей систем дистанционного банковского обслуживания.

Смарт-карты eToken PRO (Java) со встроенными радио-метками RFID.

## eToken ГОСТ

eToken ГОСТ – персональное средство криптографической защиты информации для формирования Электронной подписи по ГОСТ 34.310-2004 с неизвлекаемым закрытым ключом, выполненное в виде USB-ключа или смарт-карты. Использование eToken ГОСТ в составе существующих и разрабатываемых информационных систем повышает их защищенность и обеспечивает соответствие требованиям законодательства Республики Казахстан в части защиты информации.

Рекомендуется:

- разработчикам систем ДБО, электронных торговых площадок, систем сдачи налоговой отчетности – для обеспечения безопасности закрытых ключей электронной подписи пользователей этих систем;
- разработчикам СКЗИ - для использования в своих СКЗИ аппаратно реализованных казахстанских криптографических алгоритмов, генератора ПСЧ, а также обеспечения неизвлекаемого хранения закрытых ключей;
- разработчикам СЗИ – для встраивания СКЗИ eToken ГОСТ в создаваемые ими продукты.

## eToken NG-FLASH (Java)

eToken NG-FLASH (Java) – комбинированный USB-ключ, обладающий функциональными возможностями eToken PRO (Java), и оснащенный дополнительным модулем Flash-памяти объемом до 16 ГБ.

Дополнительная Flash-память устройства позволяет хранить данные в зашифрованном виде и может быть использована для:

- доверенной загрузки операционных систем Microsoft Windows или Linux (образ операционной системы записывается в память устройства);
- хранения и запуска предварительно сконфигурированной виртуальной машины (VMWare, Virtual PC) с предустановленным набором ПО и настроенными параметрами безопасности;
- автоматического запуска приложений из памяти устройства;
- безопасного хранения, транспортировки и резервного копирования данных;
- запуска безопасного предварительно настроенного браузера.

Рекомендуется:

- администраторам безопасности, аудиторам ИБ – для создания временных центров по оценке защищенности информационных систем, оценке их соответствия требованиям нормативных документов;
- компаниям, работающим через агентскую сеть (страхование, кредитование) – для создания агентских рабочих мест по обслуживанию клиентов;
- разработчикам ПО – для распространения / тиражирования программного обеспечения;
- всем пользователям – для безопасного хранения, транспортировки и резервного копирования данных.

## eToken NG-OTP (Java)

eToken NG-OTP (Java) – комбинированный USB-ключ с генератором одноразовых паролей (One-Time Password – OTP). Обладает всем функционалом eToken PRO (Java) для использования в PKI-системах, а также может работать без подключения к компьютеру как автономный генератор одноразовых паролей.

Одноразовый пароль может быть использован для:

- аутентификации пользователей при удаленном VPN-доступе, доступе к Web-серверам, опубликованным Web-приложениям;
- подтверждения платежных операций.

Рекомендуется:

- сотрудникам организаций, которым требуется постоянный удаленный доступ к информационным ресурсам вне зависимости от типа используемого для выхода в Интернет устройства;
- банкам, кредитно-финансовым организациям – для повышения уровня доступности предоставляемых ими сервисов, повышения удовлетворенности клиентов качеством обслуживания;
- разработчикам систем ДБО – для создания конкурентоспособных систем ДБО, позволяющих банкам, использующим эти системы, повышать уровень доступности предоставляемых услуг.

## eToken PASS

eToken PASS – автономный генератор одноразовых паролей, не требующий подключения к компьютеру. Является более дешевой альтернативой eToken NG-OTP (Java), без возможности использования в PKI-системах.

Рекомендуется:

- банкам, кредитно-финансовым организациям – для повышения уровня доступности предоставляемых ими сервисов, повышения удовлетворенности клиентов качеством обслуживания;
- поставщикам on-line услуг – для аутентификации доступа подписчиков и максимального расширения аудитории;
- пользователям мобильных устройств (телефонов, смартфонов, коммуникаторов).