

# ActivIdentity Смарт-карты

➤ Многофункциональные персональные идентификаторы

Многофункциональные смарт-карты заменяют традиционные ключи, идентификационные бэджи с фотографией, электронные пропуска, предоставляя ряд дополнительных функций. Смарт-карты являются наиболее защищенной платформой для объединения функций физического и логического доступа.

## Гибкое решение в области идентификации и безопасности

Одна единственная смарт-карта может совмещать:

- Идентификационные бэджи с фотографией для визуальной идентификации;
- Электронные пропуска для физического контроля (СКУД);
- Генераторы одноразовых паролей для удаленного доступа;
- Хранилище цифровых сертификатов и секретных ключей;
- Пароли для доступа к рабочим станциям и приложениям.

В дополнение к этому смарт-карты предоставляют защищенное пространство для хранения и генерации идентификационных данных пользователя, таких как: пароли, сертификаты и ключи PKI, одноразовые пароли и биометрическую информацию. Они позволяют осуществлять множество функций, включая строгую аутентификацию к удаленным системам, доступ к рабочим станциям и сетевым ресурсам, приложениям, а также обеспечивают защиту информации и электронных транзакций (шифрование данных, защищенная загрузка и электронная цифровая подпись). С помощью решения ActivIdentity Smart Employee ID СКУД-карты и карты для контроля доступа к ИТ-ресурсам могут быть выпущены непосредственно в СКУД, что повышает безопасность и снижает операционные риски.

## Применение смарт-карт:

При развертывании инфраструктуры смарт-карт их функционал можно задействовать постепенно. Например, можно начать с двухфакторной аутентификации на рабочих станциях, а позднее добавить другие функции. Смарт-карты ActivIdentity являются основными компонентами таких решений как:

- ActivIdentity Smart Employee ID;
- ActivIdentity Strong Authentication;
- ActivIdentity Enterprise Single Sign-On - SecureLogin;
- ActivIdentity Secure Information and Transactions.

ActivIdentity предлагает полный спектр продуктов для развертывания и использования смарт-карт, включая апплеты, карт-ридеры и ПО для работы смарт-карт: ActivClient, ActivID Card Management System, 4TRESS AAA Server for Remote Access и SecureLogin SSO.

## Широкий перечень платформ и стандартов:

Смарт-карты могут применяться в различных операционных системах, платформах управления идентификацией и приложений, таких компаний как: Sun, Microsoft, Citrix, WatchGuard Technologies, Cisco, Check Point, Lenel и других. Поддерживая открытые стандарты и такие операционные системы как: Windows, Solaris и Linux, MAC, смарт-карты от ActivIdentity работают на различных платформах, позволяя разворачивать решения в смешанных средах.

Так же они могут использоваться совместно с другими средствами аутентификации, такими как: генераторы одноразовых паролей ActivIdentity, USB-ключи ActivKey и программные генераторы на мобильных устройствах, для облегчения перехода или для удовлетворения потребностей определенных групп пользователей.

## Преимущества

### Безопасность

- Многофакторная аутентификация обеспечивает более надежную защиту, чем пароли и другие альтернативные решения;
- Решение ActivIdentity является идеальным для хранения конфиденциальной информации и идентификационных данных;
- Проверка PIN-кода, генерация, хранение ключей и другие операции выполняются на карте;
- Карты соответствуют требованиям по безопасности FIPS 140-2;
- Смарт-карты ActivIdentity Smart Employee ID с радио-меткой используются так же для контроля физического доступа в помещения.

### Удобство использования

- Пользоваться также легко, как обычным банкоматом;
- Удобно хранить цифровые сертификаты и другие данные;
- Программное обеспечение ActivIdentity позволяет впоследствии добавить идентификационные данные и другую информацию.

### Эффективность

- С помощью одной единственной смарт-карты обеспечивается защита идентификационных данных, используемых при строгой аутентификации в ИТ-среде, защита электронных коммуникаций и безопасный физический доступ в помещения;
- Предоставляется возможность аудита и получения отчетности о событиях на физическом и логическом уровнях;
- Общая стоимость владения (TCO) ниже, чем у альтернативных методов и технологий.

## Модель использования смарт-карт

### Отходя от традиционных решений.

#### Почему необходимо заменять пароли?

Пароли небезопасны: Пароль может быть использован любым, кому он известен и невозможно удостовериться, что пользователи, прошедшие процедуру аутентификации с помощью паролей, являются теми самими, за которых они себя выдают.

Пароли неудобны: Пользователи обычно выбирают слабые пароли, которые легче запомнить. Политики надежных паролей могут уменьшить данный риск, но, вместе с тем, пароли становятся слишком сложными для запоминания, поэтому пользователи записывают их на бумажных или иных легкодоступных носителях. В обоих случаях итог один: недостаточная защита идентификационных данных и слабые места в политике безопасности.

\* только для ActivIdentity Smart Employee ID.



Фото и физический доступ \*



Доступ к приложениям с помощью SSO



Доступ к рабочим станциям и сетевым ресурсам



Защита информации и транзакций



Защита информации и транзакций

**Характеристики**

- 64 кб или более памяти доступно приложениям и данным;
- Поддерживают многие высокоскоростные интерфейсы: контактный (ISO 7816) и бесконтактный (ISO144243);
- Высокопроизводительные 8/16 битные микроконтроллеры смарт-карт;
- Симметричные алгоритмы шифрования: Triple DES, AES;
- Поддержка ключей PKI до 2048 бит;
- Низкий уровень потребления энергии подходит для использования с портативными устройствами;
- Внутренние датчики безопасности;
- Удовлетворяют требованиям ROHS (бесвинцовая технология);
- Удовлетворяют многим стандартам безопасности таким как: FIPS140 и FIPS201.

**Расширяемость**

Открытые API и SDK позволяют легко интегрировать данное решение с другими продуктами, такими как: дополнительные системы управления идентификационными данными пользователей, удостоверяющими центрами.

**Поддерживаемые стандарты**

- Управление смарт-картами: GlobalPlatform;
- Java Card ;
- ActivIdentity CMS и ActivClient;
- PIV / FIPS 201;
- PIV / FIPS 201;
- FIPS 140-2;
- FIPS 140-2 Hardware Security Modules;
- Directory interface: LDAP v3.0;
- Web: SSL 3.0;
- Accessibility: Section 508 ;
- PKI: PKCS#7, PKCS#10, PKCS#11, X509, CRMF/CMMF/CRM;
- U.S. DoD GSC-IS and CAC.

**Продукты**

- ActivID Card Management System (CMS);
- ActivClient;
- Считыватели ActivIdentity;
- SecureLogin SSO;
- Сервер 4TRESS AAA;

**Технологические решения**

- Строгая аутентификация;
- SSO уровня предприятия;
- Защита информации и транзакций;
- Управление устройствами и данными пользователя.

**Отраслевые решения**

- Smart Employee ID;
- Smart Employee ID for PIV;
- Strong Authentication for Banking;
- Single Sign On for Healthcare.

**Решения партнеров**

- Novell Identity Assurance solution;
- Smart Employee ID for Sun Java System Identity Manager;
- Smart Employee ID with Lenel OnGuard;
- Smart Employee ID for PIV with Lenel IdentityDefender.

**Мнения партнеров**

«С помощью ActivIdentity Smart Employee ID персонал Sun Microsystems имеет возможность использовать единую смарт-карту как для доступа к ИТ-ресурсам так и для физического доступа в помещения. Мы объединяем процессы по выпуску и управления этими картами вместе с собственными продуктами по управлению идентификационными данными пользователя для упрощения и достижения максимальной эффективности работы во всей нашей инфраструктуре. Smart Employee ID позволяет усилить безопасность, при этом увеличивая производительность труда пользователей, повышая контроль и мобильность».

Боб Уоррал, CIO, Sun Microsystems



**Rainbow Technologies – дистрибьютор компании ActivIdentity на территории России и стран СНГ.**

- Лицензия Гостехкомиссии (ФСТЭК) РФ на деятельность в области защиты информации.
- Лицензии ФСБ России на распространение, техническое обслуживание шифровальных (криптографических) средств.
- Лицензия ФСБ России на разработку, производство, шифровальных (криптографических) средств с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем.

Ваш партнер: