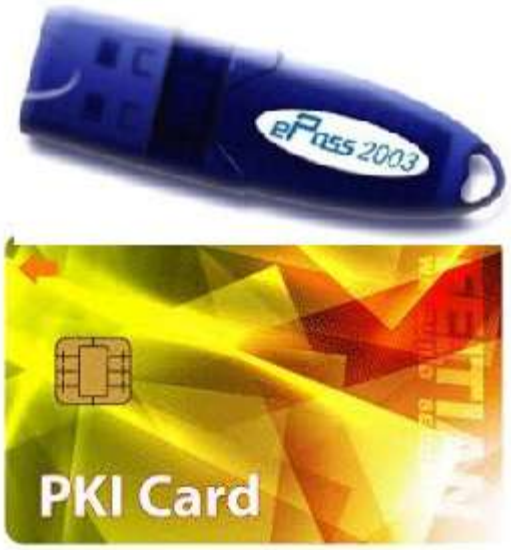
Решения по аутентификации пользователей

DATAWAY SECURITY

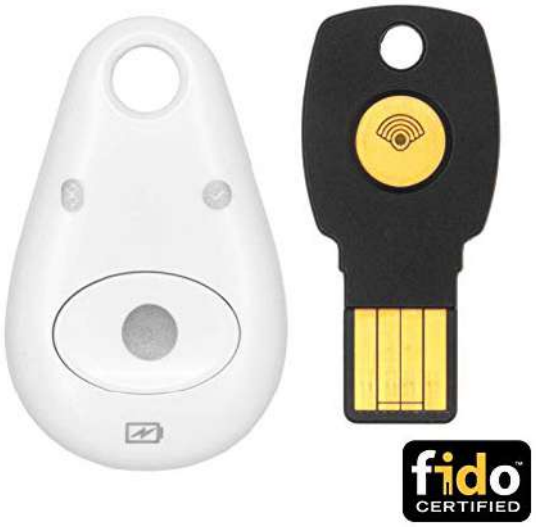
ДОВЕРИЕ | ЗАЩИТА | БЕЗОПАСНОСТЬ

Продуктовая линейка вендора



PKI токены и PKI карты

Display карты, OTP токены и Fingerprint карты

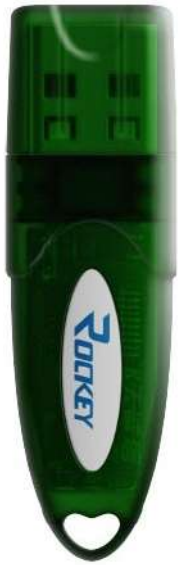


FIDO токены (U2F и FIDO2)

DATAWAY SECURITY

Продуктовая линейка вендора

Smart Card Reader

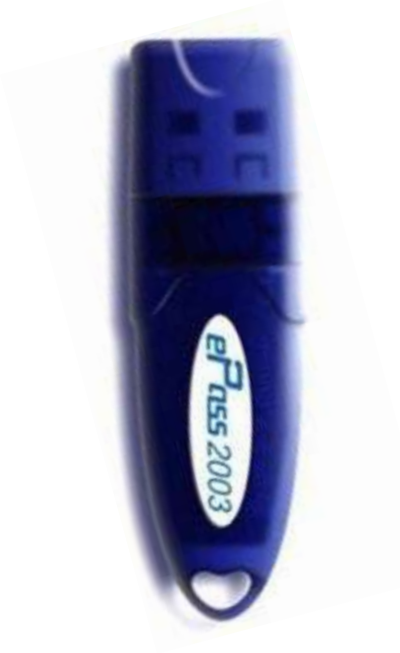


Защита ПО от нелегального использования

Сервера аутентификаций

DATAWAY SECURITY

PKI токен ePass 2003Auto



Технические характеристики:

Объем памяти: 64КБ (EEPROM), опционально возможно установить Flash память: 4ГБ и 8ГБ

Процессор: 16 бит smart card chip (сертифицированный Common Criteria EAL 5+)

Криптографические алгоритмы: RSA 512/1024/RSA 2048 бит, ECDSA 192/256 бит, DES/3DES, AES 128/192/256 бит, SHA-1 / SHA-256

Поддерживаемые стандарты: X.509 v3 Certificate Storage, SSL v3, IPSec, ISO 7816 1-4 8 9 12, CCID

Middleware: Microsoft Windows MiniDriver, Windows middleware for Windows CSP, библиотека PKCS#11 для Windows, Linux и MAC

Крипто интерфейс API: Microsoft Crypto API (CAPI), Cryptography API: Next Generation (CNG), Microsoft Smart Card MiniDriver, PKCS#11, PC/SC

Цикл перезаписей: 500 000 запись/стирание

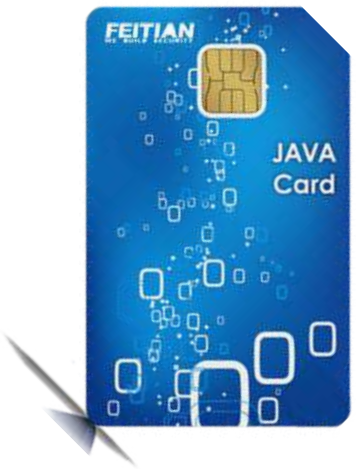
Интерфейс: USB 2.0 совместим с USB 1.1

Поддержка операционных систем: 32 и 64-бит Windows XP SP3 и выше, Windows Server 2003 и выше, 32 и 64-бит Linux, MAC OS X

Токен ePass2003 Auto обеспечивает защиту цифровых коммуникаций и транзакций используя архитектуру открытых ключей PKI. Токен основан на чипе смарт карты и обеспечивает работоспособность практически на всех ПК без докупки card reader. Для Windows токен не требует дополнительных драйверов. Основное применение – цифровые подписи и двухфакторная аутентификация.

DATAWAY SECURITY

PKI Card и JAVA Card



Технические характеристики:

GlobalPlatform & Java Card spec compliant Java Card

Объем памяти: 64КБ (EEPROM)

Процессор: 16 бит smart card chip (сертифицированный Common Criteria EAL 5+)

Криптографические алгоритмы: RSA 512/1024/RSA 2048 бит, ECDSA 192/256 бит, DES/3DES, AES 128/192/256 бит, SHA-1 / SHA-2

Поддерживаемые стандарты: X.509 v3 Certificate Storage, SSL v3, IPSec, ISO 7816 1-4 8 9 12, CCID

Middleware: Microsoft Windows MiniDriver, Windows middleware for Windows CSP, библиотека PKCS#11 для Windows, Linux и MAC, Java Card Developer's Kit

Крипто интерфейс API: Microsoft Crypto API (CAPI), Cryptography API: Next Generation (CNG), Microsoft Smart Card MiniDriver, PKCS#11, PC/SC

Интерфейс: ISO/IEC 7816 (T=0 / T=1) contact interface, ISO/IEC 14443 Type A/B and Mifare contactless interface

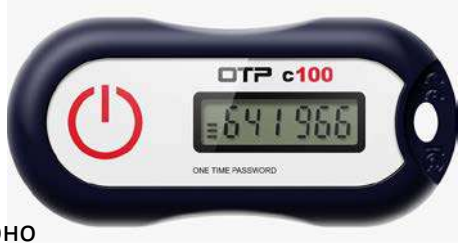
Цикл перезаписей: 500 000 запись/стирание

Поддержка операционных систем: 32 и 64-бит Windows XP SP3 и выше, Windows Server 2003 и выше, 32 и 64-бит Linux, MAC OS X

Карты разработанные в соответствии с отраслевыми стандартами, установленные такими организациями как GlobalPlatform и Smart Card Alliance. Имеются как обычные PKI карты, так и Java карты поддерживающие сторонние апплеты. Такие карты идеально подходят для удостоверений, также можно заказать карты с RFID метками MIFARE.

DATAWAY SECURITY

OTP токен C100 HOTP



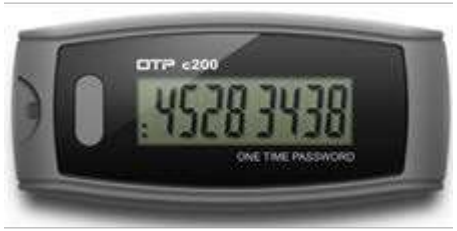
Функционал и описание продукта:

- Уникальный пароль, генерируемый каждый раз, пароль не может быть использован повторно
- Не требуется установка программного обеспечения на стороне клиента
- Соответствие открытому алгоритму OATH с синхронизацией по событию
- Легкая интеграция, с другими серверами аутентификации, подходит для **ESET Secure Authentication**
- Доступны seed'ы в формате PSKC
- Не требуется запоминать какие-либо пароли, либо PIN кода
- Не зависит от операционных систем и среды работы конечного пользователя
- Легкий и удобный брелок генератора паролей.
- ЖК дисплей на 6 символов с таймером обратного отсчета времени (15 секунд)
- Встроенный счетчик событий
- Безопасная память RAM
- Продолжительность жизни батареи 5 лет
- Seed код находится в защищенном от взлома, зашифрованной области памяти.
- Легко интегрируется с широким спектром решений для проверки подлинности и удаленному доступу

Токены C100 HOTP (одноразовый пароль на основе события) используется алгоритм на основе событий, который каждый раз генерируется при нажатии кнопки. Поскольку значения на основании событий могут быть более длительные, чем по времени, токены спроектированы так, что после 15 секунд дисплей отключается.

DATAWAY SECURITY

OTP токен C200 TOTP



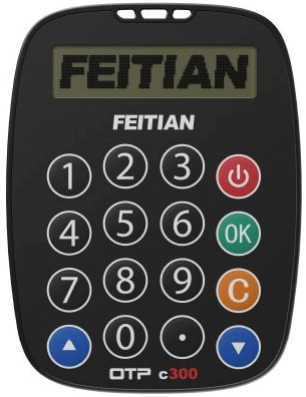
Функционал и описание продукта:

- Уникальный пароль, генерируемый каждый раз, пароль не может быть использован повторно
- Не требуется установка программного обеспечения на стороне клиента
- Соответствие открытому алгоритму OATH с синхронизацией по времени
- Легкая интеграция, с другими серверами аутентификации
- Доступны seed'ы в формате PSKC
- Не требуется запоминать какие-либо пароли, либо PIN кода
- Не зависит от операционных систем и среды работы конечного пользователя
- Легкий и удобный брелок генератора паролей.
- ЖК дисплей на 6/8 символов с таймером обратного отсчета времени (60/30 секунд)
- Встроенный часы RTC
- Безопасная память RAM
- Продолжительность жизни батареи 5 лет
- Seed код находится в защищенном от взлома, зашифрованной области памяти.
- Легко интегрируется с широким спектром решений для проверки подлинности и удаленному доступу

Токены C200 TOTP (одноразовый пароль на основе времени) используется алгоритм основанный на временном интервале, позволяет пользователям безопасно проходить аутентификацию в сети с помощью динамически меняющегося цифрового пароля управляемого RTC (часами реального времени).

DATAWAY SECURITY

OTP токен C300 OCRA



Функционал и описание продукта:

- Уникальный пароль, генерируемый каждый раз, пароль не может быть использован повторно
- Защищено PIN кодом для доступа к генерации одноразового пароля
- Не требуется установка программного обеспечения на стороне клиента
- Соответствие открытому алгоритму OATH с синхронизацией по времени и OCRA
- Легкая интеграция и полная совместимость с стандартом OCRA
- Доступны seed'ы в формате PSKC
- Подпись транзакций, для защиты целостности передаваемых данных
- Не зависит от операционных систем и среды работы конечного пользователя
- Безопасная память RAM
- Уникальный порядковый номер токена
- Продолжительность жизни батареи 5 лет
- Seed код находится в защищенном от взлома, зашифрованной области памяти.
- Поддерживает Radius сервер
- Легко интегрируется с широким спектром решений для проверки подлинности и удаленному доступу

Токены C300 OCRA, позволяют генерировать одноразовый пароль на основании случайного значения, полученного с сервера аутентификации или временного фактора. В дополнение к аутентификации клиента здесь добавлены такие возможности как взаимная аутентификация и подпись транзакций.

DATAWAY SECURITY

Mobile OTP

- **Широкий выбор метода аутентификации:**
  - **По событию HOTP**
  - **По времени TOTP**
  - **Вопрос / Ответ OCRA**
- **Доступ к приложению по PIN паролю**
- **Длина OTP – 6 или 8 знаков**
- **Интервал OTP – 30 или 60 секунд**
- **Поддержка операционных систем**
  - **Android**
  - **iPhone OS**
  - **BlackBerry**

FEITIAN Mobile OTP – это токен на мобильном телефоне для двухфакторной аутентификации пользователя. Данное решение является альтернативной заменой аппаратных устройств, что существенно снижает затраты и предлагает беспрецедентный уровень удобства. Данное приложение поддерживает мобильные ОС iOS, Android и BlackBerry. Кроме того, в FEITIAN Mobile OTP реализованы такие функции как: синхронизация по событию и по времени, запрос-ответ и вычисление электронной подписи онлайн-транзакции. Доступ к генерации одноразового пароля осуществляется посредством PIN-код защиты.

DATAWAY SECURITY

OTP Card

Функционал и описание продукта:

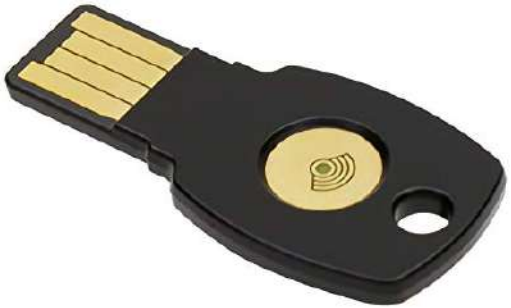
- Прошивка секретного ключа с помощью смартфонов на ОС Android с поддержкой NFC
- Поддержка генерации одноразового пароля по событию, по времени или запрос-ответ
- Время действия одноразового пароля: 30 или 60 секунд
- Длина одноразового пароля: 6 или 8 символов
- Экран: LCD / E-ink
- Срок службы батареи: от 3 до 5 лет
- Физическая защита
  - Защита от вскрытия
  - Водонепроницаемый
  - Пыленепроницаемый
- Поддержка различных сервисов
  - Google Authenticator
  - Совместим с серверами OATH
  - Поддержка сервисов Cloud
- Встраивание контактного чипа смарт-карты (дополнительный функционал)
- Активизация BLE или NFC интерфейса для прошивки секретного ключа на стороне заказчика или пользователя с помощью специального приложения на смартфоне (дополнительный функционал)

OTP Card – это компактное устройство двухфакторной аутентификации (2FA) в форм-факторе пластиковой карты с LCD/E-ink экраном для визуализации одноразового пароля (OTP). Данное устройство поддерживает генерацию одноразового пароля по событию, по времени или запрос-ответ.

Реализация NFC (коммуникация ближнего поля) предоставляет заказчику возможность прошивать в устройство собственный секретный ключ. Тем самым исключая возможность перехвата секретных ключей во время их передачи или транспортировки с завода изготовителя

DATAWAY SECURITY

ePass FIDO –NFC Secure Key



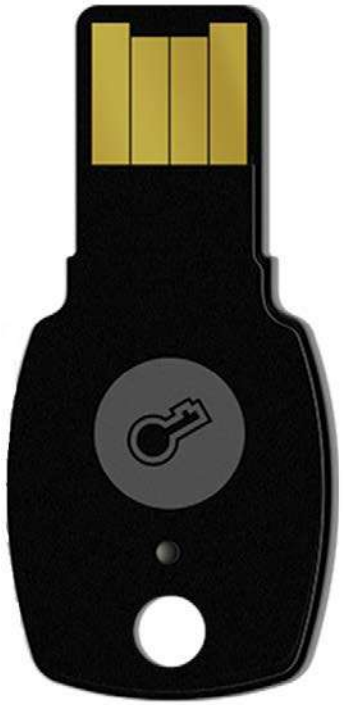
Функционал и описание продукта:

- Полная поддержка стандарта FIDO U2F
- Один токен поддерживает неограниченное количество приложений
- Позволяет пользователям безопасно входить в свои учетные записи
- Все ключи хранятся в специальном защищенном чипе от NXP
- Не требует драйверов, определяется HID, CTAP2
- Поддерживает Windows, macOS, Linux через USB
- Поддерживает Android через NFC
- Поддерживает все современные браузеры (Chrome, Edge, Firefox, Safari, Opera)
- Поддержка расширенной безопасности для Google аккаунта (требуется 2 токена) https://landing.google.com/advancedprotection/
- Поддержка алгоритма HOTP (одноразовый пароль на основе события)
- Поддержка Java Smart Card

Токен ePass FIDO-NFC – это компактный токен двухфакторной аутентификации (2FA) с поддержкой NFC технологии. Один токен способен защитить неограниченное количество приложений, каждому приложению будет присвоена индивидуальная пара ключей, где сервис хранит открытый ключ, а токен хранит закрытый ключ. Данный токен поддерживается приложениями: Google, GMail, Google Drive, Facebook, Twitter, Dropbox, Github, GitLab, Salesforce, Bitbucket, Dashlane, Duo, Digientity, BITFINEX, FastMail, Gandi.net, Keeper, Sentry, а также работу рядом серверов аутентификации поддерживающих HOTP.

DATAWAY SECURITY

ePass FIDO U2F FIDO2 USB Security Key



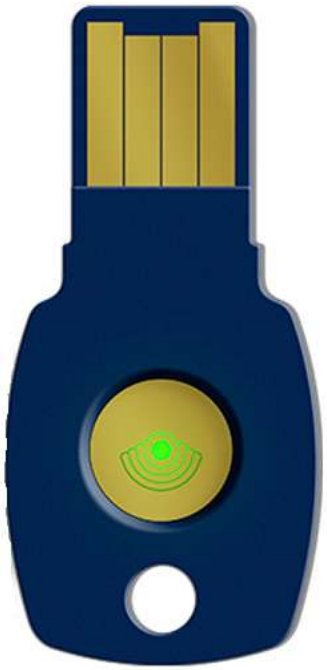
Функционал и описание продукта:

- Полная поддержка стандарта FIDO U2F и FIDO 2
- Один токен поддерживает неограниченное количество приложений
- Позволяет пользователям безопасно входить в свои учетные записи
- Все ключи хранятся в специальном защищенном чипе от NXP
- Не требует драйверов, определяется HID, CTAP2
- Поддерживает Windows, macOS, Linux через USB
- Поддерживает все современные браузеры (Chrome, Edge, Firefox, Safari, Opera)
- Поддержка облачных решений от Microsoft
- Поддержка расширенной безопасности для Google аккаунта (требуется 2 токена) https://landing.google.com/advancedprotection/
- Поддержка алгоритма HOTP (одноразовый пароль на основе события)

Токен ePass FIDO U2F FIDO2 USB Security Key – это компактный токен двухфакторной аутентификации (2FA) и FIDO2. Один токен способен защитить неограниченное количество приложений, каждому приложению будет присвоена индивидуальная пара ключей, где сервис хранит открытый ключ, а токен хранит закрытый ключ. Данный токен поддерживается приложениями: **Microsoft, Microsoft Azure, Microsoft Azure AD**, Google, GMail, Google Drive, Facebook, Twitter, Dropbox, Github, GitLab, Salesforce, Bitbucket, Dashlane, Duo, Digientity, BITFINEX, FastMail, Gandi.net, Keeper, Sentry, а также работу рядом серверов аутентификации поддерживающих HOTP.

DATAWAY SECURITY

ePass FIDO U2F FIDO2 NFC USB Security Key



Функционал и описание продукта:

- Полная поддержка стандарта FIDO U2F и FIDO 2
- Один токен поддерживает неограниченное количество приложений
- Позволяет пользователям безопасно входить в свои учетные записи
- Все ключи хранятся в специальном защищенном чипе от NXP
- Не требует драйверов, определяется HID, CTAP2
- Поддерживает Windows, macOS, Linux через USB
- Поддерживает Android через NFC
- Поддерживает все современные браузеры (Chrome, Edge, Firefox, Safari, Opera)
- Поддержка облачных решений от Microsoft
- Поддержка расширенной безопасности для Google аккаунта (требуется 2 токена) https://landing.google.com/advancedprotection/
- Поддержка алгоритма HOTP (одноразовый пароль на основе события)
- Поддержка Java Smart Card

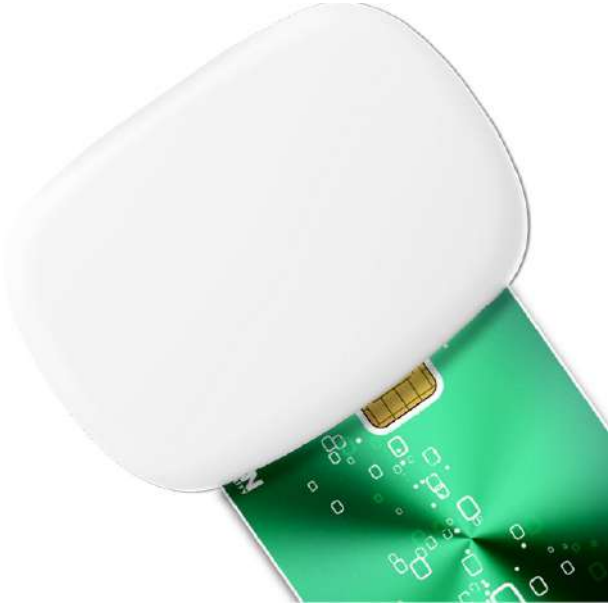
Токен ePass FIDO U2F FIDO2 NFC USB Security Key– это компактный токен двухфакторной аутентификации (2FA) и FIDO2 и поддержкой NFC. Один токен способен защитить неограниченное количество приложений, каждому приложению будет присвоена индивидуальная пара ключей, где сервис хранит открытый ключ, а токен хранит закрытый ключ. Данный токен поддерживается приложениями: **Microsoft, Microsoft Azure, Microsoft Azure AD**, Google, GMail, Google Drive, Facebook, Twitter, Dropbox, Github, GitLab, Salesforce, Bitbucket, Dashlane, Duo, Digientity, BITFINEX, FastMail, Gandi.net, Keeper, Sentry, а также работу рядом серверов аутентификации поддерживающих HOTP.

DATAWAY SECURITY

USB Smart Card Reader R301 - C25

Функционал и описание продукта:

- Стандарт поддержки Smart Card: ISO/IEC7816, T=0 and T=1 protocol, Class A, B, C cards
- Размер карты: ISO 7816-3 ID-1 (full-size)
- Поддержка Extended APDU
- Тактовая частота: 4-12 МГц
- USB коннектор: Тип А либо Тип С
- Поддержка ОС: Win2000+/Linux/macOS/UNIX/Android(OTG)
- При установке не требует драйверов, Plug in and Play
- Возможность обновления прошивки с шифрованием
- Прошивка не может быть считана с ридера
- Защита от электростатики
- Материал – пластик



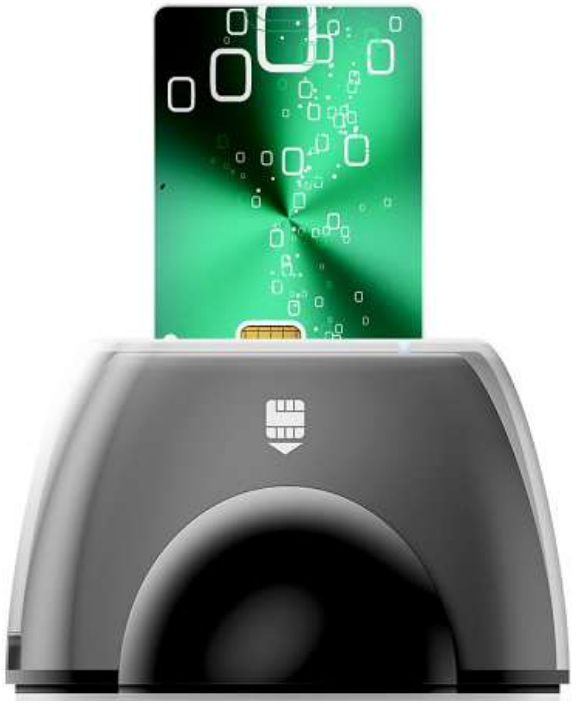
Высокоскоростной контактный считыватель смарт карт, который подключается к ПК через USB порт. Данный Card Reader соответствует стандартной спецификации CCID с интерфейсом USB 2.0 Считыватель может работать со всеми смарт-картами CLASS A, CLASS B и CLASS C, которые соответствуют стандарту ISO 7816-1 / 2/ 3. Также поддерживаются IC карты выполнены в стандарте ISO 7816-3. Данные ридеры широко применяются в банкинге, средства аутентификации, электронное правительство. Данный ридер можно брендировать по требованию клиента.

DATAWAY SECURITY

USB Smart Card Reader R301 – C41

Функционал и описание продукта:

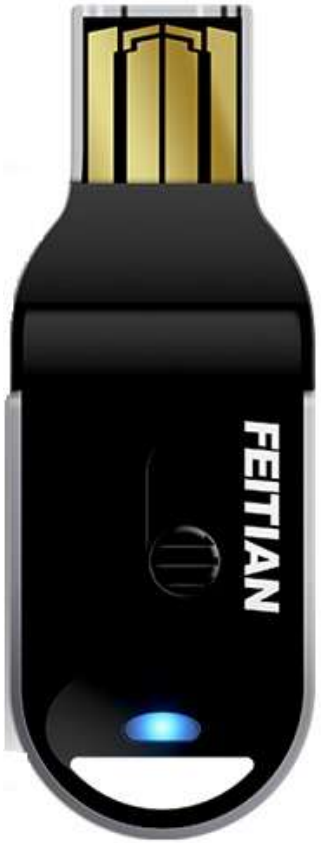
- Стандарт поддержки Smart Card: ISO/IEC7816, T=0 and T=1 protocol, Class A, B, C cards
- Размер карты: ISO 7816-3 ID-1 (full-size)
- Поддержка Extended APDU
- Тактовая частота: 4-12 МГц
- USB коннектор: Тип А либо Тип С
- Поддержка ОС: Win2000+/Linux/macOS/UNIX/Android(OTG)
- При установке не требует драйверов, Plug in and Play
- Возможность обновления прошивки с шифрованием
- Прошивка не может быть считана с ридера
- Защита от электростатики
- Материал – металл и пластик



Высокоскоростной контактный считыватель смарт карт, который подключается к ПК через USB порт. Данный Card Reader соответствует стандартной спецификации CCID с интерфейсом USB 2.0 Считыватель может работать со всеми смарт-картами CLASS A, CLASS B и CLASS C, которые соответствуют стандарту ISO 7816-1 / 2/ 3. Также поддерживаются IC карты выполнены в стандарте ISO 7816-3. Данные ридеры широко применяются в банкинге, средства аутентификации, электронное правительство. Данный ридер можно брендировать по требованию клиента.

DATAWAY SECURITY

USB Smart Card Reader R301 – B6



Функционал и описание продукта:

- Стандарт поддержки Smart Card: ISO/IEC7816, T=0 and T=1 protocol, Class A, B, C cards
- Размер карты: GSM 11.11
- Поддержка Extended APDU
- Тактовая частота: 4-12 МГц
- USB коннектор: Тип А/ Тип С
- Поддержка ОС: Win2000+/Linux/macOS/UNIX/Android(OTG)
- При установке не требует драйверов, Plug in and Play
- Возможность обновления прошивки с шифрованием
- Прошивка не может быть считана с ридера
- Защита от электростатики
- Материал – металл и пластик

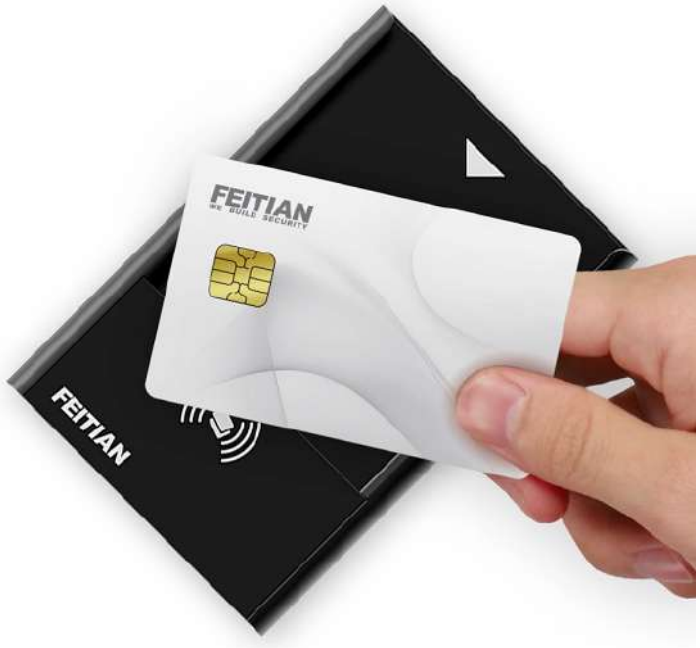
Высокоскоростной контактный считыватель смарт карт, который подключается к ПК через USB порт. Данный Card Reader соответствует стандартной спецификации CCID с интерфейсом USB 2.0 Считыватель может работать со всеми смарт-картами CLASS A, CLASS B и CLASS C, которые соответствуют стандарту ISO 7816-1 / 2/ 3. Также поддерживаются IC карты выполнены в стандарте ISO 7816-3. Данные ридеры широко применяются в банкинге, средства аутентификации, электронное правительство. Данный ридер можно брендировать по требованию клиента.

DATAWAY SECURITY

Mobile Smart Card Reader Bluetooth 4.2 NFC – C45F

Функционал и описание продукта:

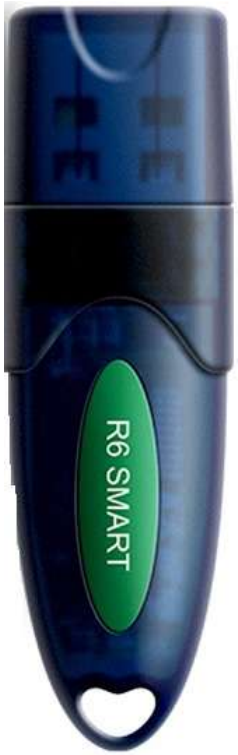
- Стандарт поддержки ISO 7816 standard, T0, T1, CLASS B, CLASS C, CLASS BC
- Стандарт для бесконтактной карты: ISO14443 Type A and Type B, Mifare и Felica стандарты, 13.56МГц
- Тактовая частота: 4-12 МГц
- Интерфейс: USB1.1/2.0/3.0; Bluetooth 4.0/4.1 LE и NFC
- Питание от USB либо внешнего аккумулятора
- Поддержка ОС: Win2000+/Linux/macOS/iOS/UNIX/Android(OTG)
- При установке не требует драйверов для USB, для подключения через Bluetooth требуется драйвер
- Возможность обновления прошивки с шифрованием
- Прошивка не может быть считана с ридера
- Защита от электростатики
- Материал –пластик



Высокоскоростной контактный считыватель смарт карт, который подключается к ПК либо мобильному телефону через USB порт, Bluetooth, NFC. Данный Card Reader соответствует стандартной спецификации CCID с интерфейсом USB 2.0 Считыватель может работать со всеми смарт-картами, которые соответствуют стандарту ISO 7816, T0, T1, CLASS B, CLASS C, CLASS BC. Также поддерживаются ISO14443 Type A и Type B, Mifare стандарт . Данные ридеры широко применяются в банкинге, средства аутентификации, электронное правительство. Данный ридер можно брендировать по требованию клиента.

DATAWAY SECURITY

Модуль защиты ПО Dongle Rockey6 - A1+



Технические характеристики:

Объем памяти: 64КБ (EEPROM)

Процессор: 32 бит smart card chip

Поддерживаемые стандарты: Global Unique Hardware ID and Site-Specific Management Code

Виртуальная машина: Встроенная C51 виртуальная машина

Встроенный алгоритм шифрования: RSA, DES

Встроенные: математические операции с плавающей точкой

Встроенный: счетчик и таймер времени

Уникальный код и глобальный уникальный идентификатор оборудования

Безопасное удаленное обновление ПО на основе одноразовых паролей

Схема управления несколькими модулями

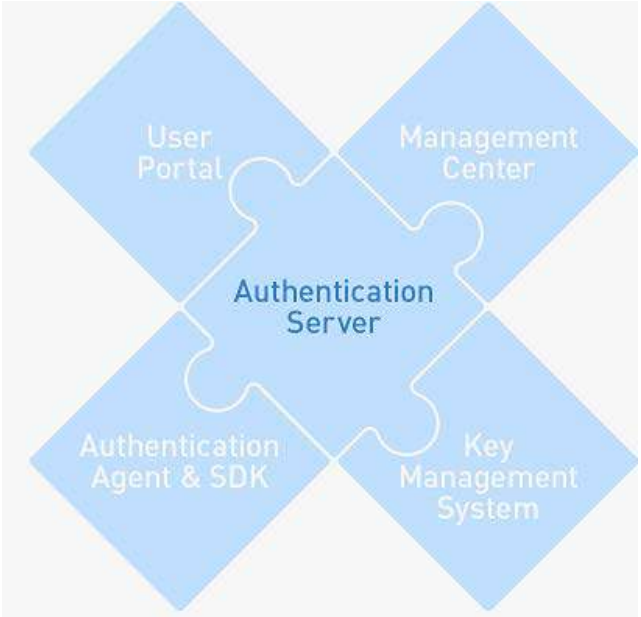
Поддержка приложений: ASM, ASP/PHP, Delphi, Power Builder, Python, Java, Oracle, SQL2000, FoxPro, VB, VBA, VC, C#, VB.Net и т.д.

ROCKEY6SMART - это программный ключ безопасности на основе чипа смарт-карты со встроенным виртуальным устройством C51. Виртуальная машина C51 позволяет выполнять небольшие приложения на устройстве. Следовательно, дизайнер может перенести часть функций на ключ. Dongle будет выполнять как часть приложения. ROCKEY6SMART - это высокоскоростное без интерфейсное устройство Human Interface Gadget (HID), предлагающее приблизительно 64 КБ в памяти и высокопрочные алгоритмы шифрования файлов, такие как RSA и DES.

DATAWAY SECURITY

Сервер аутентификации FOAS

Сервер FOAS – для предоставления сервисов аутентификации для приложений на основе динамической системы паролей. Данный сервер поддерживает токены и карты, которые разработаны по стандарту OATH. Данный сервер поддерживает все передовые технологии и построен на открытой инфраструктуре. Имеются всевозможные SDK для интеграции сервера аутентификации к всевозможным приложениям, но сервер может поддерживать всего лишь одну локацию. Данный сервер поддерживает, как аппаратные, так и программные токены.



Компоненты FOAS:
Authentication Server – сервер на котором происходит аутентификация;
User Portal – функционал для самообслуживания пользователя;
Management center- web консоль централизованного управления;
Key Management System – консоль управления HSM
Authentication Agent & SDK – плагины и SDK для интеграции с существующими системами.

Поддержка ОС: Windows, Linux,Unix, IBM AIX, HP-UX

Поддержка БД: Oracle, SQL Server, My SQL, AD/LDAP

Поддержка протоколов: Radius, LDAP, UDP, SOAPTCP

Поддержка Middleware: Websphere 7.0+, Weblogic 8.0+, JBoss 4.2+, Apache Tomcat 6.0+

Поддержка токенов: Hardware, Mobile, SMS, Software, Card

Поддержка разрядности и времени: 6/8 знаков, 30/60 секунд

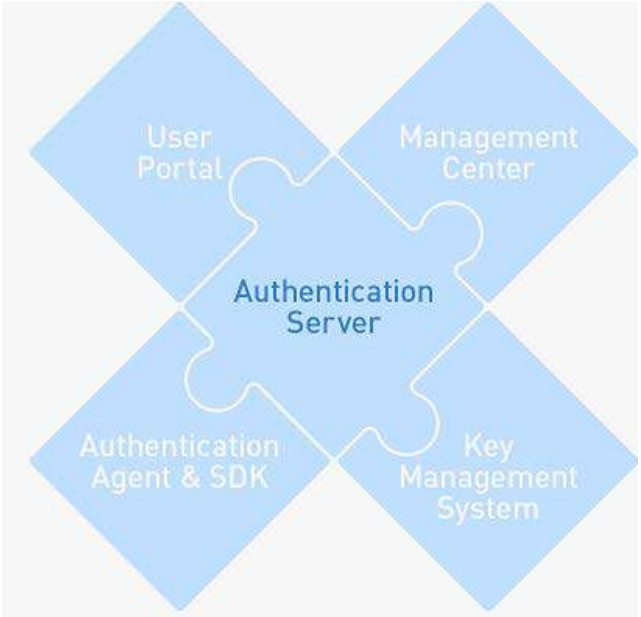
Поддержка алгоритмов: OATH/GM/T 0021-2012

SDK для языков программирования: C/Java/Webservice

DATAWAY SECURITY

Сервер аутентификации FOAS

Сервер FOAS – для предоставления сервисов аутентификации для приложений на основе динамической системы паролей. Данный сервер поддерживает токены и карты, которые разработаны по стандарту OATH. Данный сервер поддерживает все передовые технологии и построен на открытой инфраструктуре. Имеются всевозможные SDK для интеграции сервера аутентификации к всевозможным приложениям, но сервер может поддерживать всего лишь одну локацию. Данный сервер поддерживает, как аппаратные, так и программные токены.



Компоненты FOAS:
Authentication Server – сервер на котором происходит аутентификация;
User Portal – функционал для самообслуживания пользователя;
Management center- web консоль централизованного управления;
Key Management System – консоль управления HSM
Authentication Agent & SDK – плагины и SDK для интеграции с существующими системами.

Поддержка ОС: Windows, Linux,Unix, IBM AIX, HP-UX

Поддержка БД: Oracle, SQL Server, My SQL, AD/LDAP

Поддержка протоколов: Radius, LDAP, UDP, SOAPTCP

Поддержка Middleware: Websphere 7.0+, Weblogic 8.0+, JBoss 4.2+, Apache Tomcat 6.0+

Поддержка токенов: Hardware, Mobile, SMS, Software, Card

Поддержка разрядности и времени: 6/8 знаков, 30/60 секунд

Поддержка алгоритмов: OATH/GM/T 0021-2012

SDK для языков программирования: C/Java/Webservice

DATAWAY SECURITY

Официальный дистрибьютор Датавэй Секьюрити

www. datawaysecurity.ru
info@datawaysecurity.ru
Тел. 8 495 268-0126