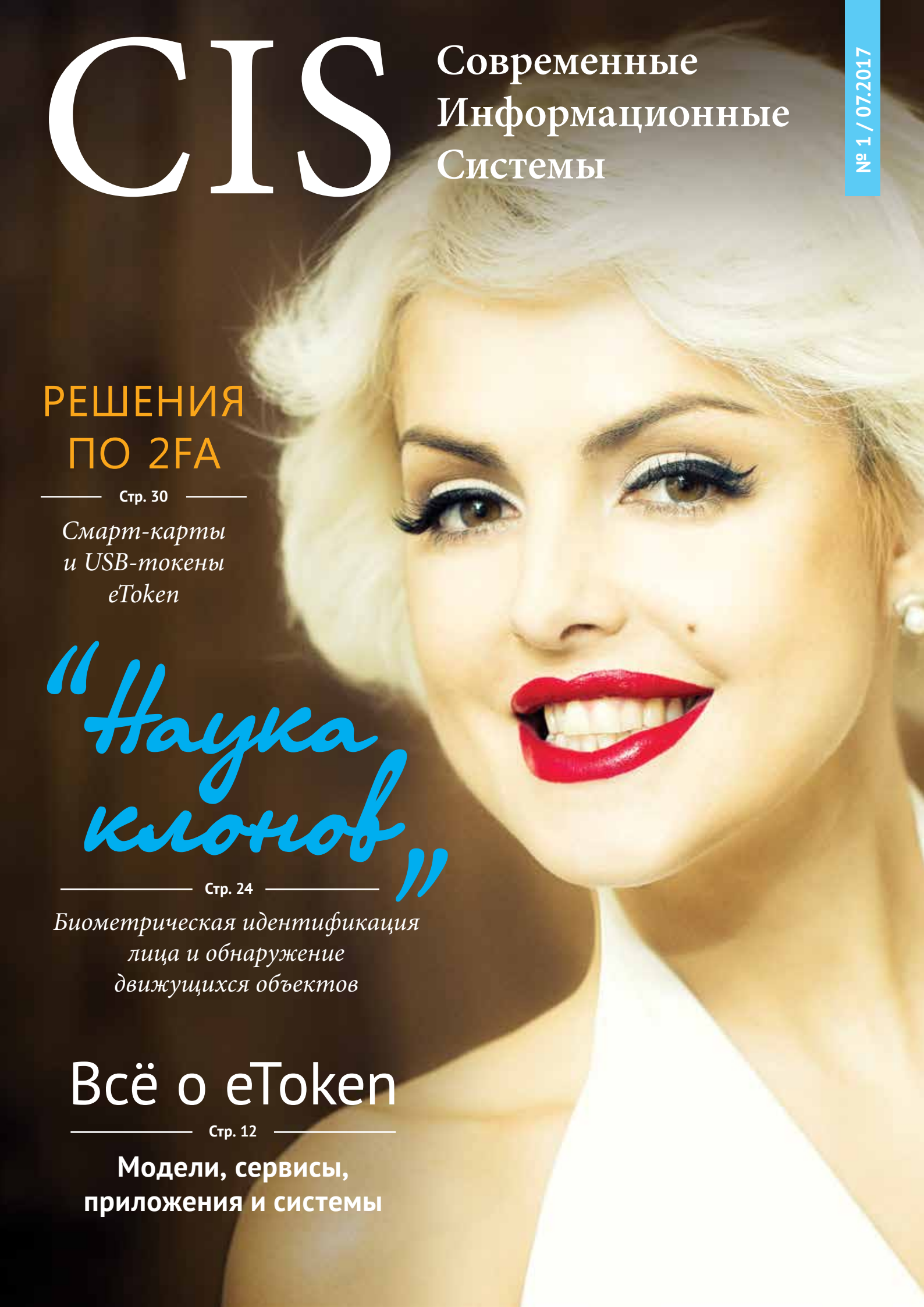
CIS
Современные Информационные Системы
№ 1 / 07.2017



РЕШЕНИЯ ПО 2FA

Стр. 30

Смарт-карты и USB-токены eToken

"Наука клонов"

Стр. 24

Биометрическая идентификация лица и обнаружение движущихся объектов

Всё о eToken

Стр. 12

Модели, сервисы, приложения и системы

ПРЕДИСЛОВИЕ

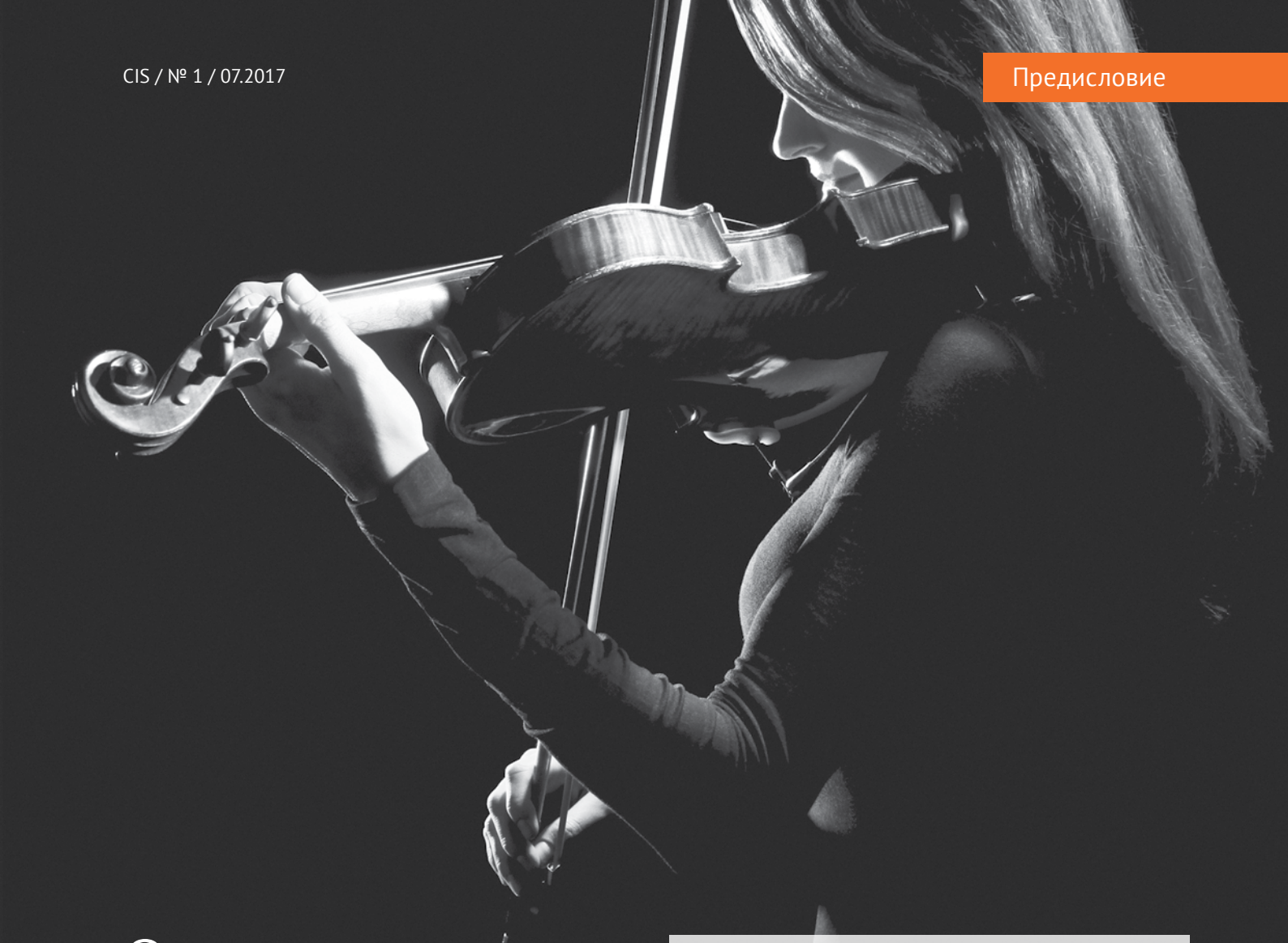
ПРОДУКТЫ

РЕШЕНИЯ

ТЕХНОЛОГИИ

ОПЫТ

КАЛЕНДАРЬ



От редактора

Вы держите в руках (или читаете с экрана) первый номер журнала «Современные информационные системы», посвящённый информационным технологиям.

Задача журнала – показать общий ландшафт рынка ИТ-решений, то разнообразие платформ, идей и инструментов, которые могут быть использованы российскими ИТ-директорами и руководителями. Причём показать их характеристики максимально равномерно, нейтрально и профессионально. И тем самым немного помочь в выборе решений и продуктов, предоставив вам самую актуальную информацию на данный момент.

Если представить структуру журнала более образно, то его можно сравнить с оркестром, в котором есть дирижёр. В этом номере такое центральное место занимают продукты и решения от компании Gemalto. И есть оркестранты – технологические партнёры, предлагающие свои решения в различных сферах и областях на основе продуктов компании Gemalto. Все они играют одно музыкальное произведение под названием «двухфакторная аутентификация».

Надеюсь, вы сможете найти на страницах нашего журнала те решения и продукты, которые помогут решить актуальные задачи и обеспечат наиболее эффективную защиту вашей компании.

Понарин Станислав
главный редактор

Главный редактор: Понарин Станислав.

Корректор: Степанов Артём.

Отдел рекламы и распространения: info@sovinfosystems.ru.

Регистрация журнала: федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Номер свидетельства: ПИ № ФС 77 – 69584.

Дата регистрации: 02.05.2017.

Наименование СМИ: Современные Информационные Системы.

Форма распространения: печатное СМИ, журнал.

Территория распространения: Российская Федерация.

Адрес редакции: Малый Сухаревский пер., д. 9, стр. 1, офис 36, г. Москва, 127051.

Язык: русский.

Периодичность: 4 раза в год (1 раз в квартал).

Тираж 5 000 экз. (отпечатанный тираж).

Журнал предназначен для лиц старше 16 лет.

Добро пожаловать в SafeNet Authentication Client!

SafeNet Authentication Client (SAC) является связующим универсальным программным обеспечением, которое управляет обширным набором аппаратных и программных решений Gemalto-SafeNet для инфраструктуры открытых ключей (PKI).

С чего всё началось?

Более 20 лет назад израильская компания Aladdin Knowledge Systems представляет новые USB-токены в семействе токенов аутентификации, совместно выпуская ПО eToken Run Time Environment (RTE) с комплектом драйверов к данным устройствам. На рынке появляются, помимо классических смарт-карт eToken PRO, всем запомнившиеся модели eToken PRO R2, впоследствии перешедшие в серии eToken PRO 16K, 32K, NG-OTP и 64K.

Само программное обеспечение стало неотъемлемой частью для персональных средств аутентификации – оно позволяло выполнять различные сценарии «машинных» операций, применяемых к самим токенам:

- просмотр текущего состояния и статуса устройства;
- переименование;
- разблокировка;
- инициализация (форматирование до «заводских» настроек);
- смена ПИН-кода пользователя;
- настройка качества и сложности пароля.

После появления новых аппаратных и программных технологий, стали появляться токены, соответствующие стандарту Java Global Platform: eToken PRO JAVA 72K и хорошо зарекомендовавшие себя обновлённые модели – eToken NG-Flash и eToken NG-OTP. Выпускается eToken PKI Client, функциональность которого значительно расширена и усовершенствована.

Программное обеспечение реализует поддержку как предыдущего поколения смарт-карт eToken PRO CardOS, так и нового семейства eToken PRO Java. Но главное преимущество eToken PKI Client перед предыдущим поколением ПО – это, конечно, появление:

- поддержки полной совместимости с системами управления жизненным циклом смарт-карт;
- поддержки работы с токенами из браузеров (Internet Explorer, Mozilla Firefox, Google Chrome);
- поддержки на уровне вендор-совместимости большого количества решений Microsoft, Cisco, CheckPoint, Juniper, VMWare, Citrix и т. д.;
- поддержки шаблонов групповых политик для централизованного администрирования настроек ПО администраторами служб ИТ и ИБ;

История совместного успеха

За последовательностью слияний ряда компаний на текущий момент SafeNet Authentication Client обеспечивает полную поддержку всех современных устройств eToken, iKey, а также смарт-карт IDPrime MD и .NET. Тем самым Gemalto-SafeNet реализовали «единую точку входа», создавая универсальную среду для ра-

Главное меню программного обеспечения eToken RTE 3.66

Главное меню программного обеспечения eToken PKI Client 5.1 SP1

Главное меню программного обеспечения SafeNet Authentication Client 10.3

боты разных классов устройств в единой среде пользовательского интерфейса. Благодаря чему пользователи развернутых инфраструктур, скажем, eToken или IDPrime PKI, могут и далее применять имеющиеся у них устройства, используя преимущества и возможности единого интерфейса ПО.

Основные характеристики

- Строгая двухфакторная аутентификация для защиты сетей и защиты данных:
  - аутентификация в инфраструктуре Microsoft Active Directory;
  - аутентификация в VDI (Microsoft, Citrix, VMWare);
  - аутентификация в VPN (Cisco, Microsoft, Juniper, CheckPoint и другие);
  - работа с тонкими клиентами;
  - пользователю предоставляется единый вид идентификации/аутентификации на множествах платформ.
- Поддержка общих критериев (Common Criteria) и поддерживаемых FIPS устройств.
- Полная поддержка IDPrime MD, SafeNet eToken и iKey.
- Поддержка PIN PAD считывателей устройств.
- Полная поддержка пользовательской кастомизации с созданием корпоративного дизайна интерфейса, включая настройку политик безопасности.
- Расширенные настройки администрирования SAC посредством административных шаблонов позволяют администраторам управлять опциями SAC. «Включая» или «отключая» те или иные флаги, можно гибко настроить только тот минимум операций, который пользователю достаточен для работы. Например, заблокировать пользователю возможность удаления содержимого с ключевого носителя.
- Не стоит забывать, что с ПО пользователи получают возможность пользоваться собственными CSP и KSP, поставляемыми с SAC:
  - CSP – eToken Base Cryptographic Provider;
  - KSP – SafeNet Smart Card Key storage Provider.
- Простая интеграция с большинством решений с поддержкой приложений на основе стандартов API.
- Поддержка виртуальной клавиатуры, минуя ввод пароля с физической клавиатуры. Тем самым обеспечивая безопасную и надёжную защиту при аутентификации на устройстве от кейлогеров.

При внушительном модельном ряде USB-токенов и смарт-карт Gemalto вслед за SafeNet сохранила в SAC поддержку моделей предыдущих поколений устройств, которые были выпущены довольно давно, но не престают работать и стоят на страже безопасного доступа к различным сервисам и средам у многочисленных заказчиков.

Поддержка устройств

- USB-токены и смарт-карты eToken.
- Смарт-карты iKey.
- Смарт-карты IDPrime.

Сейчас SAC обеспечивает полную поддержку и обратную совместимость устройств линейки eToken и iKey, а также IDPrime MD и .NET – смарт-карт в портфеле производителя Gemalto. Приблизительно с таких слов начинается обзор к описанию ПО в пользовательском руководстве.

Вместо заключения

SafeNet Authentication Client – это продукт с собственным набором сервисных утилит, криптопровайдеров и драйверов к устройствам линейки продуктов Gemalto.

Разбиваем заблуждения тех, кто назовёт решение SafeNet Authentication Client лишь только драйвером. С SafeNet Authentication Client пользователи решают задачи, которые выходят за рамки представления об обслуживании устройств драйвером, открывая возможность локального администрирования и использования устройств, хранящих ключевую информацию. С использованием SafeNet Authentication Client предприятия; финансовые, учебные, медицинские учреждения; правительственные органы и т. д. подходят к решению задач безопасности с использованием современных технологий по защите данных и инновационных средств криптографии.

gemalto
security to be free

Gemalto

www.safenet.gemalto.com
www.gemalto.com

TESSIS

TESSIS –
официальный дистрибьютор в России

www.tessis.ru

SafeNet Authentication Client

Унифицированный клиент-посредник, который позволяет управлять всей линейкой аутентификаторов Gemalto-SafeNet с использованием сертификатов, включая eToken, смарт-карты IDPrime и iKey, USB-устройства и программные решения. Сохраняя полную обратную совместимость и все функции предыдущих версий промежуточного ПО, SafeNet Authentication Client обеспечивает полную поддержку всех актуальных устройств eToken и iKey, а также смарт-карт IDPrime MD и .NET.

Простое управление аутентификацией Gemalto на базе PKI

SafeNet Authentication Client соединяет аутентификаторы PKI Gemalto с приложениями, обеспечивая полный набор инструментов для локального администрирования и поддержку множества продвинутых функций для обеспечения информационной безопасности, включая цифровые подписи, проверку подлинности перед загрузкой компьютера и шифрование диска. SafeNet Authentication Client позволяет генерировать и хранить закрытые ключи в высоконадёжных аутентификаторах на основе смарт-карт и токенов, благодаря чему пользователь может не опасаться за сохранность своих учётных данных.

Средства управления SAC снижают расходы на службу поддержки, позволяя пользователям самим управлять своими картами, токенами и сертификатами.

Преимущества

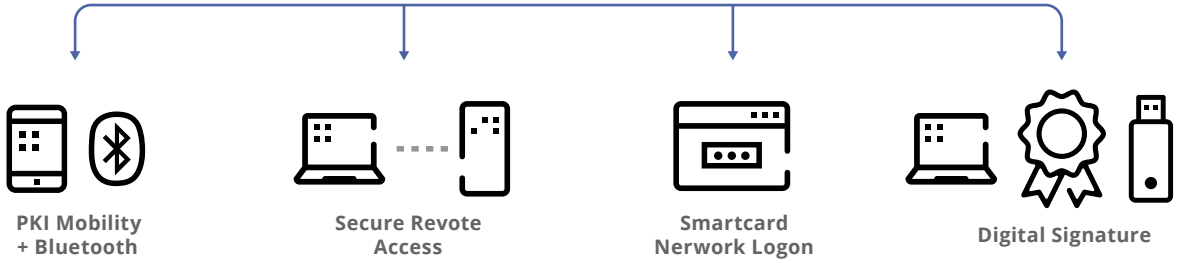
- Прозрачное взаимодействие со всеми стандартными приложениями безопасности на основе сертификатов.
- Упрощённые консолидированные инструменты, позволяющие пользователям управлять своими собственными картами, токенами и сертификатами.
- Поддержка безопасного доступа, шифрования данных и цифровых подписей в одном аутентификаторе.
- Упрощённое управление безопасностью за счёт развёртывания множества приложений безопасности на единой платформе.
- Использование защиты на базе сертификатов от любых клиентов и серверов благодаря поддержке целого ряда платформ.

Особенности

- Полная поддержка смарт-карт IDPrime MD, включая поддержку нескольких слотов и изменения качества ПИН-кода.
- Поддержка считывателей ПИН-клавиатур.
- Строгая двухфакторная аутентификация для защиты сети и данных.
- Поддержка устройств, сертифицированных в соответствии с требованиями ФСТЭК.
- Локальное администрирование и использование устройств.
- Легко настраиваемый клиент: начиная с конфигурации безопасности и политик и заканчивая пользовательским интерфейсом.
- Полная интеграция с любыми приложениями, основанными на сертификатах, за счёт использования стандартных API-интерфейсов.
- Поддержка расширенных приложений управления паролями для защиты компьютеров и обеспечения доступа к локальной сети с использованием входа в систему eToken Network Logon или Gemalto IDGo Credential Provider. Поддержка виртуальной клавиатуры, исключающая необходимость вводить пароли с помощью физической клавиатуры для обеспечения защиты от кейлогеров на уровне ядра.
- Общий внешний вид на всех платформах.

Общее решение для всех пользователей и платформ

SafeNet Authentication Client доступен на Windows, Mac и Linux, поэтому ваша организация может в полной мере использовать решения для обеспечения информационной безопасности на базе сертификатов, включая устойчивую проверку подлинности, шифрование и цифровые подписи, практически для любых устройств, включая мобильные. Решения MobilePKI от Gemalto полностью совместимы с SafeNet Authentication Client (SAC) и позволяют легко расширить сферу использования PKI на мобильные устройства.



Защита информации и персональных данных

Комплекс решений SafeNet по защите информации и персональных данных от Gemalto позволяет организовать всестороннюю защиту информации, цифровой идентичности, платежей и транзакций на любых предприятиях, в финансовых учреждениях и государственных органах. При создании решений главным приоритетом была безопасность данных, которую обеспечивают инновационные методы шифрования, лучшие в своём классе криптографические инструменты и средства устойчивой аутентификации и идентификации. Решения SafeNet от Gemalto помогают защитить именно то, что имеет значение для клиента.

Операционные системы

- Windows Server 2008 R2 SP1;
  Windows Server 2008 SP2;
  Windows Server 2012 и 2012 R2;
  Windows Server 2016;
  Windows 7 SP1;
  Windows 8;
  Windows 8.1;
  Windows 10.
- MAC OS X 10.11.6, 10.12.3.
- Дистрибутивы Linux: Ubuntu 13.10, 14.04, CentOS 6.6, 7.0, Red Hat 6.6, 7.0, SUSE Linux enterprise desktop 11.3, 12.0, Fedora 20, Debian 7.7.

API

- PKCS#11 V2.20, MS CryptoAPI и CNG (CSP, KSP), Mac Keychain (TokenD), PC/SC.

Криптографические алгоритмы

- 3DES, SHA-256, RSA вплоть до 2048 бит, криптография на основе эллиптических кривых (ECC).

Удостоверяющие центры

- Microsoft, Entrust, VeriSign.

Браузеры

- Mozilla Firefox.
- Internet Explorer, Microsoft Edge (без выпуска сертификатов).
- Google Chrome (без выпуска сертификатов)

Аутентификаторы SafeNet

- IDPrime MD 830;
  IDPrime MD 3810;
  IDPrime MD 3811;
  IDPrime .NET (только интерфейсы SAC PKCS#11 и IDGo 800 Minidriver).
- SafeNet eToken Pro;
  SafeNet eToken Pro Smartcard;
  SafeNet eToken 4100;
  SafeNet eToken 5100/5105;
  SafeNet eToken 5200/5205;
  SafeNet eToken NG-OTP;
  SafeNet eToken 5110, 5110 HID;
  SafeNet eToken 7300, 7300-HID;
  eToken Virtual.

Кто мы

Gemalto – мировой лидер в области цифровой безопасности, который делает современный связанный сетями данных мир более защищённым.

Наши ноу-хау помогут подтвердить вашу личность и защитить данные, сохранив их в безопасности, а также позволят вам работать с различными сервисами на ваших мобильных устройствах, любом подключённом к сети оборудовании, в «облаке» и других аналогичных сценариях.

Наши решения лежат в основе современного образа жизни, начиная от мобильных платежей, через решения корпоративной безопасности и заканчивая интернетом вещей, и позволяют нашим клиентам предоставлять безопасные услуги в цифровом мире для миллиардов людей и устройств.

---

gemalto
security to be free

Gemalto

www.safenet.gemalto.com
www.gemalto.com

TESSIS

TESSIS –
официальный дистрибьютор в России

www.tessis.ru

SafeNet Authentication Service

Видение SafeNet Authentication Service заключается в том, чтобы сделать двухфакторную аутентификацию общедоступной. Для достижения этой цели платформа SafeNet Authentication Service предоставляет решение, которое проще и дешевле в использовании, чем традиционные системы с использованием аппаратных токенов и ручным назначением.

Доступная, гибкая и «облачная» аутентификация

Для снижения рисков, с которыми сталкивается бизнес, огромное значение играет выбор правильного решения для аутентификации. Очевидно, лучшие решения поддерживают самую широкую линейку аутентификаторов и могут обеспечить защитой как «облачные», так и локальные приложения, а так же любую сеть, доступ к которой осуществляется с любого устройства.

При выборе решения для аутентификации, помимо основных параметров безопасности, так же необходимо учитывать возможности быстрого развёртывания, внедрения и управления. Администраторы обслуживающие системы аутентификации, знают, что основная часть затрат заключается в постоянном обслуживании пользователей и токенов. SafeNet Authentication Service значительно снижает все вышеперечисленные затраты.

SafeNet Authentication Service идеально подойдёт для вашего бизнеса, если вы подбираете решение для аутентификации, которое предлагает:

- простое и быстрое развёртывание с использованием автоматизированных рабочих процессов, для минимизации администрирования и настройки конфигурации;
- свобода от построения сложных ИТ-инфраструктур, соотношение цены и качества, соответствие вашего бюджета и совокупной стоимости владения (TCO);
- техническое совершенство и инновации.

SafeNet Authentication Service доказывает, что высокая (надёжная) безопасность не должна означать высокие затраты на обслуживание.

Gemalto более двух десятилетий предоставляет выгодные инновационные решения для широкого круга клиентов по всему миру.

Непревзойдённая гибкость

Вы хотите сохранить свою текущую систему аутентификации? Нет проблем. Вы в полной мере можете воспользоваться преимуществом решения SafeNet Authentication Service, не теряя уже существующие вложения в аутентификацию. В отличие от любого другого решения на рынке SafeNet Authentication Service позволяет продолжать использовать вашу систему аутентификации с вашими токенами. Решение SAS может сосуществовать с существующими системами аутентификации, при этом обеспечивая единое представление об активности аутентификации пользователей во всех имеющихся системах.

Возможности SafeNet Authentication Service

- Быстрая миграция. Переход от вашей существующей технологии – просто и быстро с использованием бесплатных агентов миграции.
- Быстрое внедрение. Назначение токенов для 20 000 пользователей всего за 20 минут.
- Легкая автоматизация. Добавление пользователей из любых хранилищ, таких как LDAP, Oracle, SQL и других.
- Выбор из широкой линейки аутентификаторов. Используйте аппаратные, программные, мобильные и Push-аутентификаторы, SMS, графические аутентификаторы для формирования пароля в дополнение к контекстной аутентификации под управлением единой платформы.
- Лёгкая масштабируемость. Увеличивайте количество пользователей без ограничений.
- Управление рисками. Для эффективного управления рисками контекстная аутентификация от Gemalto требует дополнительного фактора аутентификации только в ситуации высокого риска. Неограниченное количество гранулированных политик, позволяющих организовать различные уровни аутентификации для различных рабочих процессов, местоположений и мобильных устройств.
- Полный аудит. Для соблюдения стандартов безопасности, таких как SOX, PCI, HIPAA, возможность автоматизации построения подробных отчётов о соответствии системы и её аудита.
- Организация повсеместной защиты. Решение SafeNet Authentication Service достаточно гибкое для того, чтобы работать со всеми технологиями: как локальными, так и «облачными». «Облачные» и веб-приложения работают на основе (с использованием) защищённого протокола SAML.

Комплексная система защиты

Решение SafeNet Authentication Service использует стандартные протоколы RADIUS и SAML – это означает, что вы можете интегрировать его в любую сеть или приложение, которое вы используете, включая решения всех ведущих поставщиков. Для приложений и устройств, не поддерживающие стандартные протоколы, можно использовать агенты SafeNet Authentication Service.

Агент можно использовать для защиты систем, доменов, служб удалённых рабочих столов и терминальных пользователей Microsoft Windows. Все агенты можно скачать БЕСПЛАТНО.

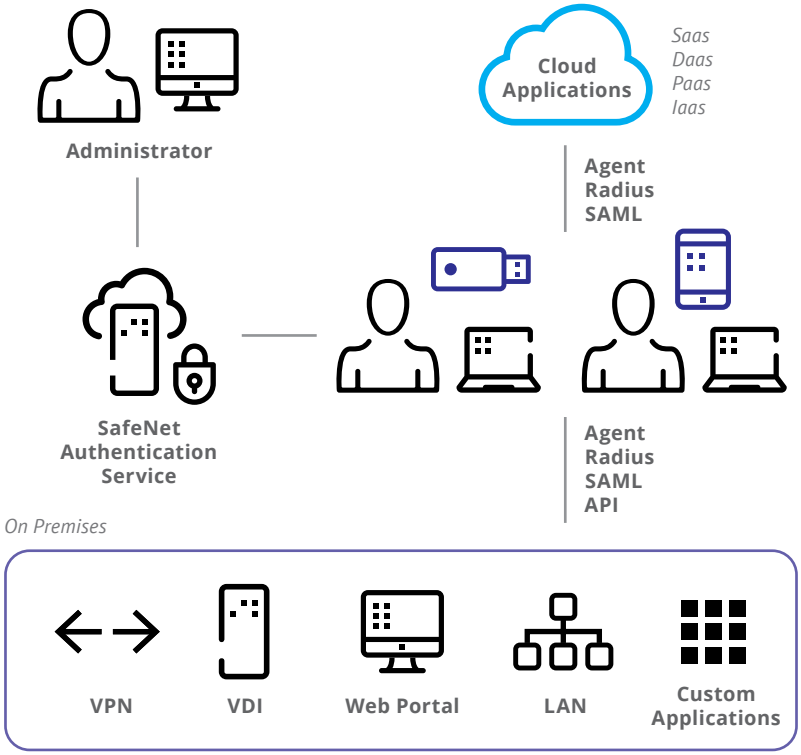
Интеграционные возможности

Безопасный доступ к любому приложению с любого устройства.

Простота использования

SafeNet Authentication Service предоставляет вам возможность:

- автоматического назначения и управления пользователями и токенами, что позволяет экономить время и средства за счёт массового предварительного распределения токенов любого типа по груп-



пам пользователей и их отзыва на основе заданных администратором политик, а так же выполнять самостоятельную регистрацию (каждый пользователь может получить любой токен и зарегистрироваться без участия администратора);

- обеспечивать гибкий подход к управлению политиками, позволяющий не только определять общие правила, но и детализировать политики;
- предварительно определять политики безопасности на основе ролей и прав делегирования, соответствующие наилучшим отраслевым практикам;
- поддерживать множество бизнес-подразделений (и связанных с ними сетевых доменов), обеспечив централизованное управление системой, контроль над её состоянием, и, кроме того, делегировать администрирование локальных пользователей конкретному бизнес-подразделению;
- импортировать или вручную загружать данные пользователей системы аутентификации в службу SafeNet Authentication Service с возможностью их автоматической синхронизации;
- автоматически создавать отчёты по расписанию с помощью предварительно заданных или настраиваемых шаблонов, которые можно экспортировать в сторонние приложения;
- настраивать все параметры с сохранением полного контроля над процессом аутентификации пользователей;
- получать доступ к веб-порталу самообслуживания, с помощью которого пользователи могут самостоятельно выполнять типовые задачи и решать простые вопросы без привлечения администратора.

Экономия по доступной цене

При использовании SafeNet Authentication Service оплата всех необходимых элементов аутентификации рассчитывается по количеству пользователей. Круглосуточная доступность, программные и SMS-токены, консоль управления, агенты миграции и доступа – всё это уже включено в стоимость, так что вы получаете гарантию безопасности бизнеса и предсказуемости расходов. Постоянное предоставление новых токенов, регистрация и отмена регистрации пользователей, создание отчётов, мониторинг использования и прочие рутинные задачи администрирования, выполняемые вручную, значительно увеличивают трудозатраты. SafeNet Authentication Service решает эту проблему благодаря автоматической инициализации ресурсов в режиме самообслуживания, способной существенно снизить расходы на администрирование и обслуживание. Если пользователь теряет токен, система автоматически создает новый токен за считаные секунды.

В стоимость решения входит программное обеспечение и все агенты, обеспечивающие интеграцию с внешними системами. Таким образом, мы гарантируем экономию до 60% по сравнению с традиционными решениями.

Аутентификация на ваш выбор

SafeNet Authentication Service позволяет реализовать аутентификацию таким образом, чтобы она соответствовала нуждам ИТ-структуры.

Доставка по мере необходимости. SafeNet Authentication Service упрощает сложную инфраструктуру и снижает затраты на закупку аппаратного обеспечения.

Собственная реализация. SafeNet Authentication Service Private Cloud Edition (PCE) предлагает полную автоматизированную систему и простое использование решения SafeNet Authentication Service, которое реализуется в инфраструктуре вашей организации. Попробуйте решение SafeNet Authentication Service сейчас: бесплатно в течение 30 дней.

Внесение изменений в организацию должно быть целесообразным. Использование решения SafeNet Authentication Service сократит ваши расходы и время. Внедрение решения настолько простое, что процесс активации может занять всего несколько минут, не причиняя существенных изменений инфраструктуре и бизнес-деятельности.

---

gemalto
security to be free

Gemalto

www.safenet.gemalto.com
www.gemalto.com

TESSIS

TESSIS –
официальный дистрибьютор в России

www.tessis.ru

SafeNet Authentication Manager

Гибкая, расширяемая и масштабируемая платформа управления аутентификацией.

Поддержка растущих потребностей

SafeNet Authentication Manager – это комплексная платформа аутентификации, которая позволяет организациям реализовывать прогрессивную стратегию строгой аутентификации для обеспечения локального и удалённого доступа к различным корпоративным ресурсам с использованием единого сервера аутентификации. Благодаря поддержке решений на основе OTP, сертификатов и программных аутентификаторов, а также контекстной аутентификации, SafeNet Authentication Manager позволяет решать потребности в безопасном доступе – как сегодня, так и в будущем.

Аутентификация на основе контекста

Возможности аутентификации на основе контекста позволяют обеспечить удобный, экономически эффективный и безопасный удалённый доступ с ненавязчивой, но надёжной проверкой подлинности, сохраняя при этом необходимую гибкость для добавления в случае необходимости защиты с помощью более надёжных методов.

Возможности контекстной аутентификации в SafeNet Authentication Manager упрощают работу, требуя от пользователей использовать дополнительные факторы аутентификации только в случаях несоответствия их действий заранее определённым политикам.

Строгая аутентификация: теперь и в «облаке»

SafeNet Authentication Manager позволяет организовать строгую двухфакторную аутентификацию с использованием инфраструктуры открытых ключей (PKI). Также по мере переноса ИТ-ресурсов в «облачные» среды и приложения SaaS-предприятия сталкиваются с задачей обеспечения удобного и безопасного доступа к основным приложениям и высококонфиденциальным ресурсам, которые выводятся за пределы корпоративной сети.

SafeNet Authentication Manager предоставляет бесшовную, последовательную надёжную аутентификацию и возможность федеративного входа в систему для корпоративных пользователей, которым необходим безопасный доступ к приложениям Office 365 и SaaS-приложениям, таким как GoogleApps и SalesForce.com (SFDC).

Преимущества

- Безопасный доступ к ресурсам в облаке. Федеративный вход и автоматическое предоставление ресурсов пользователям SaaS-приложений и Office 365.
- Безопасный доступ к мобильным конечным точкам. Управление учётными данными и проверка подлинности для устройств iOS гарантирует, что только сотрудники с доверенными устройствами смогут получить доступ к корпоративным ресурсам.
- Детализация уровней контроля с помощью контекстной аутентификации. Настраиваемые правила политик с возможностью детального контроля над уровнями аутентификации, действующими при каждом входе пользователя на онлайн-ресурс.
- Обработка различных уровней риска. Поддержка широкого спектра методов аутентификации позволяет гибко работать с различными профилями рисков.
- Гибкость, необходимая для роста. Возможность постепенного развития инфраструктуры аутентификации за счёт добавления решений OTP и CBA, а так же расширенных приложений безопасности.
- Сокращение расходов на поддержку. Автоматизированные процессы, удалённая активация и установка программного обеспечения для токенов программного обеспечения и интуитивные средства самообслуживания обеспечивают всестороннюю поддержку конечных пользователей и снижают затраты на обслуживание.
- Нормативно-правовое соответствие. Комплексные функции аудита и отчётности, обеспечивающие соблюдение требований регуляторов.

Сочетание физического и логического доступа

Многие организации нуждаются в защите физических объектов, таких как двери, парковки и зоны безопасности. Внедрение объединённого решения на основе бейджа несёт очевидные преимущества для пользователей офиса, которым необходимо иметь только одно удостоверение и помнить один ПИН-код или короткий пароль для использования вместе со своими бейджами. SafeNet Authentication Manager – это комплексный сервер для проверки подлинности и управления учётными записями, обеспечивающий защиту физических объектов в дополнение к функциям логического и удалённого доступа.

Функции

- Широкий ряд методов аутентификации и форм-факторов.
- Безопасный доступ к различным ресурсам.
- Защита мобильных устройств.
- Встроенная поддержка федеративных учётных записей.
- Полный набор функций для управления.
- Подготовка отчётности и обеспечение соответствия нормам.
- Полное администрирование всех этапов жизненного цикла.
- Гибкость для роста.

---

gemalto
security to be free

Gemalto

www.safenet.gemalto.com
www.gemalto.com

TESSIS

***TESSIS** –*
официальный дистрибьютор в России

www.tessis.ru

SafeNet Network Logon

Обеспечение полного набора опций для защиты доступа к ПК и локальным сетям.

Безопасный доступ

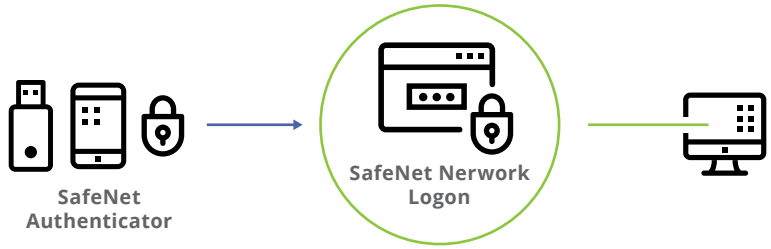
Решение предоставляет методы строгой аутентификации, основанные на цифровых сертификатах и генераторах одноразовых паролей (OTP), которые работают в автономном режиме и в режиме онлайн. SafeNet Network Logon также позволяет создавать уникальные профили входа в домены под управлением ОС Windows, которые могут безопасно храниться на USB-токенах и смарт-картах. Широкий выбор аппаратных и программных аутентификаторов SafeNet позволяет оптимизировать безопасный доступ в зависимости от профилей рисков и требований к удобству использования.

Централизованное управление и широкий выбор аутентификаторов

SafeNet Network Logon поддерживает весь спектр аппаратных и программных аутентификаторов SafeNet, а также проверку подлинности на основе сертификатов. SafeNet Network Logon полностью интегрирован с SafeNet Authentication Manager, который предоставляет ИТ-администраторам полный набор функций для управления проверкой подлинности, включая развёртывание аутентификаторов, аннулирование регистраций, самостоятельное восстановление паролей пользователями, резервное копирование и восстановление учётных данных, а так же решение для тех случаев, когда токен забыт или утерян.

Преимущества

- Выбор из нескольких методов аутентификации, технологий и форм-факторов для обеспечения доступа к локальной сети.
- Централизованное управление локальным и удалённым доступом с помощью одного сервера аутентификации и более надёжная защита для привилегированных пользователей.
- Возможность создания временных токенов для пользователей, которые теряют или оставляют свои токены (при совместном использовании с SafeNet Authentication Manager и SafeNet Authentication Client).
- Функции управления сетевыми паролями и администрирования, позволяющие пользователям управлять своими собственными устройствами.



Использование USB-устройств

- Позволяют хранить несколько сложных паролей и профилей на одном аутентификаторе, благодаря чему пользователи могут получать доступ к нескольким ресурсам с помощью одного токена.
- Поддерживают создание и хранение уникальных профилей пользователей, генерирующих случайные или псевдослучайные пароли для доступа к доменам Windows. С помощью этих средств возможно организовать двухфакторную аутентификацию для доступа к локальной сети без необходимости развёртывания полной инфраструктуры PKI.

Защита информации и персональных данных

Благодаря приобретению SafeNet Gemalto предлагает наиболее полный набор решений для обеспечения безопасности, позволяющих клиентам пользоваться передовыми средствами защиты данных, цифровой идентификации, платежей и транзакций. Теперь ещё более полный, портфель решений SafeNet по защите информации и персональных данных Gemalto позволяет предприятиям любых отраслей, крупным финансовым учреждениям и государственным органам обеспечить действительно надёжную защиту данных, используя инновационные методы шифрования, лучшие в классе методы криптографии и решения строгой аутентификации и управления цифровой идентичностью.

gemalto
security to be free

Gemalto

www.safenet.gemalto.com
www.gemalto.com

TESSIS

TESSIS –
официальный дистрибьютор в России

www.tessis.ru

SafeNet eToken 5110

Если вы раздумываете над выбором, какой ключ лучше и надёжнее, посмотрите на свою банковскую карту, который вы доверяете свои деньги – на 95% чип в вашей банковской карте произведён той же компанией, что и ключи SafeNet eToken 5110.

Сертификат № 2730
В России существует сертифицированная ФСТЭК версия ключей SafeNet eToken 5110. Эти ключи могут быть использованы в системах, подлежащих дальнейшей аттестации.

Microsoft

Позвольте намекнуть, что все сотрудники компании Microsoft для удалённого доступа к своей инфраструктуре уже более 7 лет пользуются картами Gemalto.

Вместо предисловия

А вы знаете, как сейчас выглядит ключ eToken? При упоминании ключа eToken, все вспоминают USB-ключик «рыбку», который изображён на картинке.

И это вполне нормально, так как ключ eToken в форме «рыбки» известен в России с начала 2000-х годов.

Но жизнь движется вперёд, и всем знакомый и полюбившийся USB-ключ «рыбка» морально и технологически устарел. Текущим потомком, единственным и престолонаследным, является ключ SafeNet eToken 5110, который выглядит вот так.

Функциональность ключа для обычного пользователя осталось прежней. Если вы используете родной SafeNet Authentication Client, то никаких изменений при работе с ключом не будет, ну разве что в руке лежит по-другому и белый «хвостик» светится нежно-голубым, что, кстати, очень красиво и романтично, особенно при работе ночью.

Собери свой ключ

Ключи SafeNet eToken 5110 могут быть брендированы под запросы заказчика:

- изменение цвета корпуса;
- нанесение изображения или логотипа;
- нанесение надписей.

FIPS и все-все-все

Борцы за правду и импортозамещение говорят, что новые ключи SafeNet eToken 5110 нельзя использовать в России, так как они поставляются с поддержкой FIPS. Для тех, кого пугает это слово поясняем.

> FIPS (англ. Federal Information Processing Standards, Федеральные Стандарты Обработки Информации) – открыто публикуемые стандарты, разработанные правительством США, используемые всеми гражданскими правительственными учреждениями и контрагентами в США. Многие из стандартов FIPS представляют собой изменённые версии других широко распространённых стандартов (ANSI, IEEE, ISO и т. п.).
>
> Некоторые из стандартов FIPS были разработаны правительством США. Например, коды стран, а также такие криптографические стандарты, как DES (FIPS 46) и AES (FIPS 197).
>
> *(Статья из Википедии)*

Если вы всё же считаете, что FIPS – это неправильно и плохо, то можете просто отформатировать ключ без поддержки этой опции. Сделать это можно с помощью ПО SafeNet Authentication Client или с помощью системы управления жизненным циклом ключей и смарт-карт SafeNet Authentication Manager.

Область применения

Ключи SafeNet eToken 5110 пришли на смену устаревшим ключам eToken 72k Java и полностью совместимы со всеми решениями, в которых поддерживался eToken 72k:

- аутентификация в домене Microsoft Active Directory;
- аутентификация в VDI (Microsoft, Citrix, VMWare);
- аутентификация при удалённом доступе (Cisco, Microsoft, Juniper, CheckPoint и др.);
- работа с ЭЦП, в том числе поддержка ключей SafeNet eToken 5110 в КриптоПро CSP;
- работа с тонкими клиентами (Wyse, TOHK).

Стоит обратить особое внимание на поддержку ключей в КриптоПро CSP.

Таким образом, компания Gemalto совместно с компанией дистрибутором TESSIS полностью подготовили ключ SafeNet eToken 5110 к российским реалиям и обеспечили полную наследуемость eToken 72k Java.

Компания производитель, Gemalto, постоянно расширяет спектр решений, в которых поддерживаются ключи SafeNet eToken 5110, взаимодействуя с мировыми производителями программного обеспечения и оборудования и обеспечивая бесшовную поддержку своего флагманского «из коробки».

Если вы уже используете ключи eToken 72k Java, то переход на SafeNet eToken 5110 не доставит вам никаких хлопот.

Хочешь быть лидером, работай с лидерами

Наверное, стоит рассказать, почему ключи, которые ранее были известны как eToken производства израильской компании Aladdin Knowledge System, теперь стали называться SafeNet eToken, и при чём тут вообще Gemalto.

Давным-давно, уже, наверное, более 7 лет назад, израильская компания Aladdin Knowledge System была куплена американской компанией SafeNet. Спустя какое-то время начался ребрендиг продуктов, и многие продукты приобретённой компании получили приставку SafeNet. Уже тогда ключи стали именоваться SafeNet eToken 72k Java, но до российского рынка данное изменение пришло совсем недавно.

Года 3 назад компания SafeNet была куплена мировым лидером по продуктам информационной безопасности в целом и системам аутентификации в частности: компанией Gemalto.

В портфеле компании Gemalto есть такие продукты, как:

- Hardware Security Module (HSM);
- канальные шифраторы;
- решения для защиты виртуальных сред Protect -V;
- решения для банкинга;
- смарт-карты, USB-ключи и системы управления смарт-картами и USB-ключами;
- генераторы одноразовых паролей и системы управления и проверки одноразовых паролей;
- и другие – более полную информацию можно получить на сайте www.gemalto.com.

В итоге все наработки компании Aladdin Knowledge System перешли в компанию Gemalto, которая обогатила их своим опытом и знаниями и выпустила ключ нового поколения SafeNet eToken 5110.

Поддержка операционных систем	Windows Server 2008 R2, Windows Server 2012 и 2012 R2, Windows 7, Windows 8, Windows 10, macOS, Linux.
Поддерживаемые API и стандарты	PKCS#11, Microsoft CAPI, PS/SC, X.509 v3 certificate storage, SSL v3, IPSec/IKE, MS minidriver (CCID), CNG.
Объём памяти	80kb (81 920b).
Размеры	16,4 x 8,5 x 40,2 мм.
Соответствие ISO	Поддержка стандарта ISO 7816 с 1 по 4 спецификацию.
Рабочие температуры	От 0 C^0 до + 70 C^0.
Условия хранения	От – 40 C^0 до + 85 C^0.
Допустимая влажность	0 – 100% без образования конденсата.
Сертификат влагоустойчивсти	IPX7 – IEC 60529.
Хар-ки USB	USB тип A, поддержка USB 1.1 и 2.0.
Корпус	Твёрдый пластик, с защитой незаметного вскрытия.
Срок хранения данных	Не менее 10 лет.
Количество циклов перезаписи	Не менее 500 000 циклов.
Алгоритмы, реализованные аппаратно	Симметричные алгоритмы: 3DES, AES 128/192/256 bit. HASH: SHA 1, SHA 256. RSA: 1024 bit, 2048 bit. Эллиптические кривые: P-256, P-384.
Сертификаты безопасности	FIPS 140-2 level 2 (SC chip и OS).
Платформа	Gemalto IDCore 30 и апплет eToken.

gemalto
security to be free

Gemalto

www.safenet.gemalto.com
www.gemalto.com

TESSIS

***TESSIS** – официальный дистрибьютор в России*

www.tessis.ru

«Привратник»

Аутентификация в VDI с помощью сертификатов ГОСТ.

Проблематика

Соблюдение требований 152-ФЗ при удалённом доступе к персональным данным. Переход на отечественные решения по выпуску и управлению цифровыми сертификатами и разграничению доступа на их основе. Внутриведомственные требования защиты информации и доступа к ней.

Решение почти подходит

Решение подходит с точки зрения техники, но не удовлетворяет «бумажным» требованиям. Необходимо «научить» решение мирового вендора работать в российских реалиях. Нужно всё сертифицированное и по сертификатам ГОСТ. Требуется подогнать существующее решение под требование регулятора.

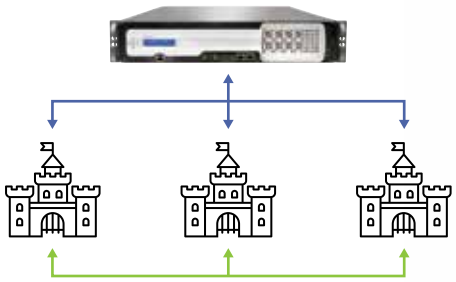
Для кого

- Банковский сектор: кредитные агенты в точках продаж, удалённые микроофисы.
- Страховые компании: страховые агенты «в полях».
- Телеком: агенты по привлечению абонентов, удалённый доступ для внутренних сотрудников.
- И многие другие…

Отказоустойчивость и балансировка нагрузки

Для обеспечения отказоустойчивости и балансировки нагрузки предлагается использовать несколько «Привратников», объединённых в массив.

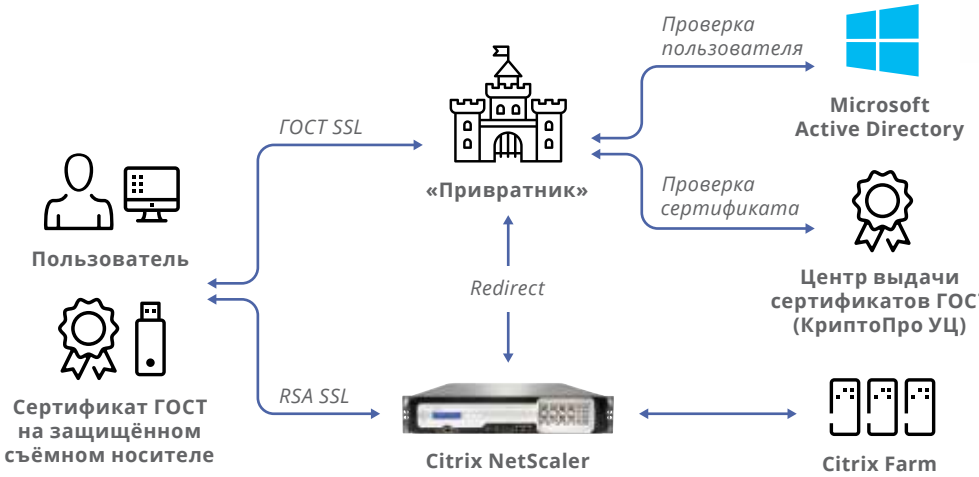
Лицензирование



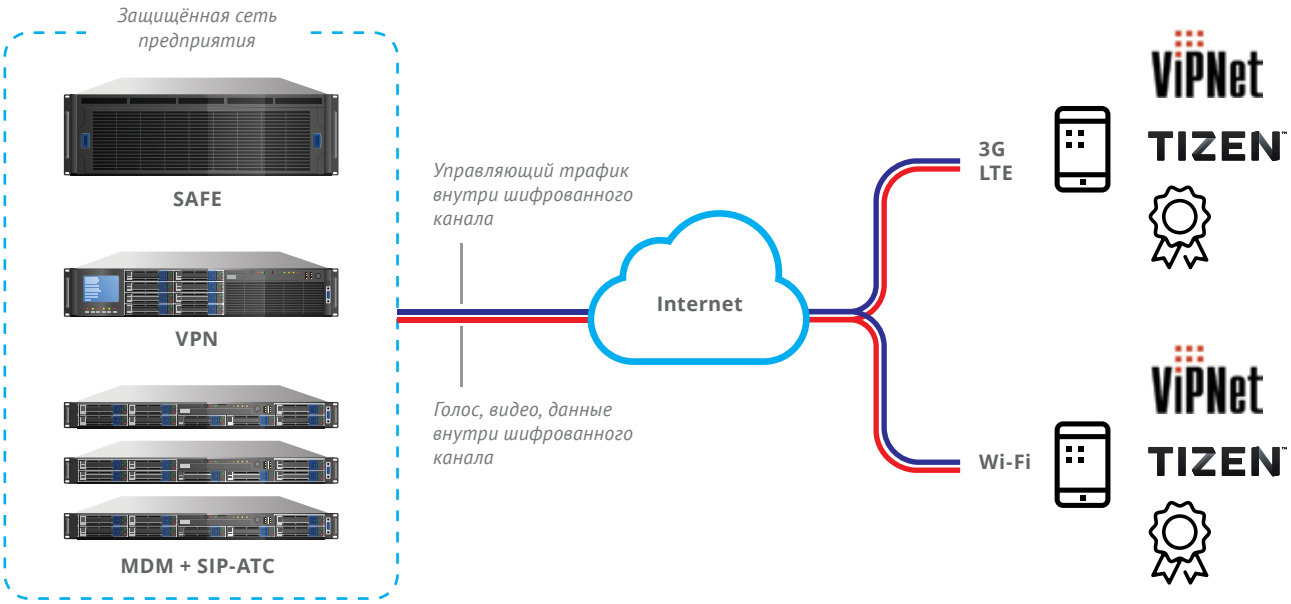
Лицензирование по пользователю, независимо от количества серверов в массиве. «Привратник» доступен в двух конфигурациях: Appliance и Virtual Machine.

Демонстрация решения

Демостенд собран на площадке Citrix. Готовы продемонстрировать решение. Обратитесь к нашему гуру разработки решений по аутентификации.



Tizen – защищённая мобильная связь организации



Возможности

- Защищённая голосовая связь (SIP).
- Защищённый обмен сообщениями (IM).
- Защищённая электронная почта.
- Защищённый выход в интернет.
- Тревожная кнопка.
- Корпоративные приложения.

Платформа на Linux

На основе открытого кода. Gstreamer, X11/Wayland, Webkit/Blink и т. д. Большое количество разработчиков.

Открытый исходный код

Простое добавление новых функций, сервисов и устройств.

Разнообразные категории устройств

Поддержка широкого спектра устройств: от смартфонов и ТВ до бытовой техники (холодильники, фотокамеры и т. д.).

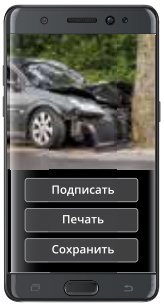
Возможность подключения устройств разных категорий.

Преимущества

- Российское производство – максимальное использование российских решений и разработок.
- Доверенное решение – шифрование по ГОСТ, сертификаты ФСТЭК, ФСБ РФ, в том числе на ОС Tizen (единственная сертифицированная мобильная ОС).
- Белые списки – что не разрешено, то запрещено.
- Установка приложений осуществляется только компанией. Отсутствует магазин приложений.
- Быстрое и безопасное внедрение. Сотрудник сам запускает встроенное приложение для безопасной активации смартфона.
- Безопасность (MDM). Настройка действий при краже или потере, отслеживание местоположения и действий, удалённое управление.

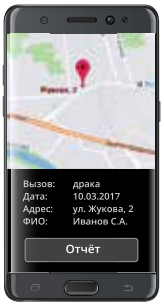
Для кого?

- Руководящий состав.
- Офисные работники.
- Полевые сотрудники.
- Дочерние структуры/партнёры.

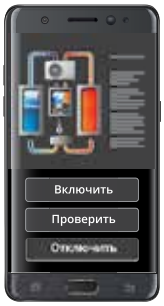


Страхование
Доверенный регистратор ДТП

Полиция
Видео-регистратор



Участковый
Управление происшествиями



Энергетика
Управление подстанциями

SAFE Communications

+7 (916) 531-05-02
i.fedorushkin@safe.com.ru
www.safe.com.ru

«Облачное» резервное копирование с Azure Backup

Основное при работе с резервными копиями – скорость восстановления данных в случае их потери. Azure Backup решает вопросы защиты и быстрого восстановления данных.

Единый интерфейс управления ИТ-инфраструктурой

Компании переходят к использованию смешанной инфраструктуры, объединяющей как локальное, так и «облачное» ИТ-окружения, причём в «облачном» окружении будет реализована модель IaaS (миграция приложений в «облако») с возможностью расширения до PaaS (изначально «облачные» приложения) и SaaS («приложения как услуга»). При этом существенно использовать единый интерфейс для резервного копирования всех ИТ-ресурсов.

Приспосабливаемость

Компании хотят с максимальным эффектом пользоваться возможностями «облака» с общим доступом, где можно, например, развернуть приложения из магазина Marketplace для решения актуальных задач. Также, администратор должен иметь возможность делать резервное копирование и восстановление данных, не обращаясь к центральной ИТ-инфраструктуре для подготовки нужных «облачных» ресурсов.

Снижение стоимости

Модель на базе подписки – очевидное преимущество «облака» с общим доступом, но тут нужно учитывать объём затрат на резервное копирование. К примеру, при развёртывании дополнительной инфраструктуры для резервного копирования в «облаке» затраты возрастают.

Независимость от инфраструктуры

Это одно из основных преимуществ миграции в «облако». Так как резервное копирование нагружает локальную ИТ-среду, компании хотят найти способ резервного копирования, который не зависел бы от инфраструктуры.

Стратегии «облачного» использования

Решение об использовании «облака» для резервного копирования может реализовать одну из трёх стратегий «облачного» использования. Также необходимо произвести оценку, насколько хорошо оно работает в рамках каждой из этих стратегий.

Хранение данных в «облаке». Здесь «облако» с общим доступом используется для хранения вторичной копии данных или как альтернатива хранению на магнитной ленте. Пользователи, как и раньше, управляют «облачным» хранилищем, ответственны за восстановление данных, а также управляют резервной средой, которая остаётся локальной.

«Облако» как среда. Это новый уровень: пользователи запускают приложение резервного копирования на виртуальной машине IaaS, что обеспечивает защиту таких приложений. Здесь всё похоже на предыдущий случай, однако гарантирована защита только виртуальных машин, но не гарантирована защита остальных элементов «облачной» среды (PaaS, SaaS). Также, есть вероятность небольшого

роста совокупной стоимости. К примеру, на одной виртуальной машине IaaS используется не более 32 ТБ — этого недостаточно для приложений резервного копирования. Чтобы делать масштабное резервное копирование, пользователи должны создавать новые виртуальные машины IaaS, настраивать масштабирование, а также подготавливать хранилища для резервных копий. Всё это сказывается на росте затрат на резервное копирование. Как видно по аббревиатуре (IaaS — «инфраструктура как услуга»), эта модель не освобождает от необходимости следить за инфраструктурой, а именно этого ждут компании от перехода в «облако».

«Облачная» платформа. Резервное копирование можно использовать на основе модели PaaS, чтобы иметь резервное копирование в качестве услуги и через единый интерфейс осуществлять управление локальной средой и резервным копированием приложений, исконно ориентированных на «облако» (IaaS, PaaS, SaaS). Так как вся инфраструктура находится в области ответственности поставщика услуг, затраты на резервное копирование не возрастают, и пользователи не должны выполнять действия по управлению инфраструктурой резервного копирования.

Azure Backup была создана как PaaS-служба, в основе которой третья из указанных ранее стратегий. Эта служба полностью оправдывает ожидания компаний от переноса ИТ-инфраструктуры. Также, поскольку Azure Backup является собственной службой Azure, она имеет возможность обращаться к другим службам Azure, что способствует удобству и эффективности резервного копирования. Например, Azure Backup предоставляет доступ к расширенным инструментам мониторинга, задействующим функции Power BI, или углублённой аналитики данных в Azure.

Простое и надёжное резервное копирование в «облаке»

Azure Backup, будучи в первую очередь ориентированным на «облако», предоставляет существенные преимущества, которые едва ли возможно обеспечить при использовании обычных стратегий.

Инструменты резервного копирования при использовании IaaS/PaaS. Azure Backup совместим с виртуальными машинами IaaS – это обеспечивается интерфейсом резервного копирования, который доступен на блейд-сервере виртуальных машин. Выполнение расширения ВМ происходит, если пользователь запрашивает техническую поддержку резервного копирования. Для настройки виртуальной машины IaaS для резервного копирования достаточно несколько щелчков мышью. Чтобы настроить резервное копирование, также можно использовать шаблоны ARM, которые гарантируют поддержку функций ВМ IaaS (например, шифрование диска). Существует план добавить эту возможность в SQL Azure, Azure Files и другие ресурсы и приложения Azure PaaS (к примеру, WebApps и Service Fabric).

Восстановление данных как предоставляемая услуга. Одно из серьёзнейших опасений, относящихся к «облачному» хранению резервных копий – восстановление данных. Это и сопутствующие затраты, и время, которое тратится на локальное восстановление данных, и требования к шифрованию. Обычно восстанавливаются все данные, хранящиеся локально или в «облаке». Необходимо предусмотреть особое хранилище для просмотра элементов в «облаке». Azure Backup использует уникальную технологию: точка восстановления в «облаке» монтируется как том, что позволяет производить её мониторинг, чтобы поэлементно восстановить необходимые данные. Компании могут не затруднять себя подготовкой инфраструктуры – вывод данных с Azure осуществляется без дополнительной стоимости. Эти преимущества задают уникальную ценность Azure Backup. Описанная функция сейчас доступна для виртуальных машин IaaS (операционные системы Microsoft Windows и Linux) и локальных серверов Microsoft Windows. Через несколько месяцев она появится в System Center Data Protection Manager и Microsoft Azure Backup Server.

Защита от злоумышленников

Резервное копирование является одним из важнейших элементов защиты от вредоносных шифровальщиков. Поэтому современным организациям важно иметь инструмент для резервного копирования, к которому злоумышленники не смогут получить доступ. Информационная безопасность остаётся высочайшим приоритетом, поэтому Azure Backup непрерывно совершенствует пакет Operations Management Suite (OMS), чтобы обеспечить всестороннюю защиту данных. Так, недавно Azure Backup представила целый ряд новых функций для защиты локальной и «облачной» инфраструктуры.

Azure Backup обеспечивает глубокий анализ угроз и своевременное уведомление о проблемах. Резервное копирование могут выполнять только пользователи с действующими учётными данными Azure, получившие ПИН-код с портала Azure. В случае выполнения критически важной операции с резервной копией ответственные лица немедленно получают уведомление, что позволяет уменьшить негативные последствия для компании.

Microsoft

Microsoft
Мировой лидер в области информационных технологий.

www.microsoft.com

Коннектор для взаимодействия SafeNet Authentication с КриптоПро УЦ

Если вы хотите управлять жизненным циклом смарт-карт и сертификатов, выпущенных КриптоПро УЦ, из единого интерфейса, то при использовании SAM и коннектора для КриптоПро УЦ ваши задачи будут решены наиболее удобным образом.

SafeNet Authentication Manager и КриптоПро УЦ

Так сложилось, что за последние годы программный продукт SafeNet Authentication Manager (далее SAM) является, наверное, самой распространённой системой управления жизненным циклом токенов и смарт-карт. У данной системы есть много достоинств и очень широкая функциональность, но есть и недостатки, такие как, например, неадаптированность к российским реалиям. SAM ничего не знает ни про ГОСТ, ни про самое популярное в России решение для построения удостоверяющих центров в соответствии с ГОСТ – КриптоПро УЦ.

Однако SAM имеет открытый API-интерфейс для разработки интеграционных коннекторов с другими решениями, что также, несомненно, является преимуществом SAM.

Решение

Итак, как уже упомянуто выше, SAM «из коробки» не умеет работать с КриптоПро УЦ. Но компания «Современные Информационные Системы» разработала и выпустила на рынок специальный коннектор, позволяющий программному продукту SAM взаимодействовать с КриптоПро УЦ.

Стоит отметить, что коннектор SAM к КриптоПро УЦ использует штатные механизмы SAM и КриптоПро УЦ, объединяя функциональность двух продуктов.

Взаимодействие

Коннектор позволяет реализовать взаимодействие SAM и КриптоПро УЦ в разрезе следующей функциональности:

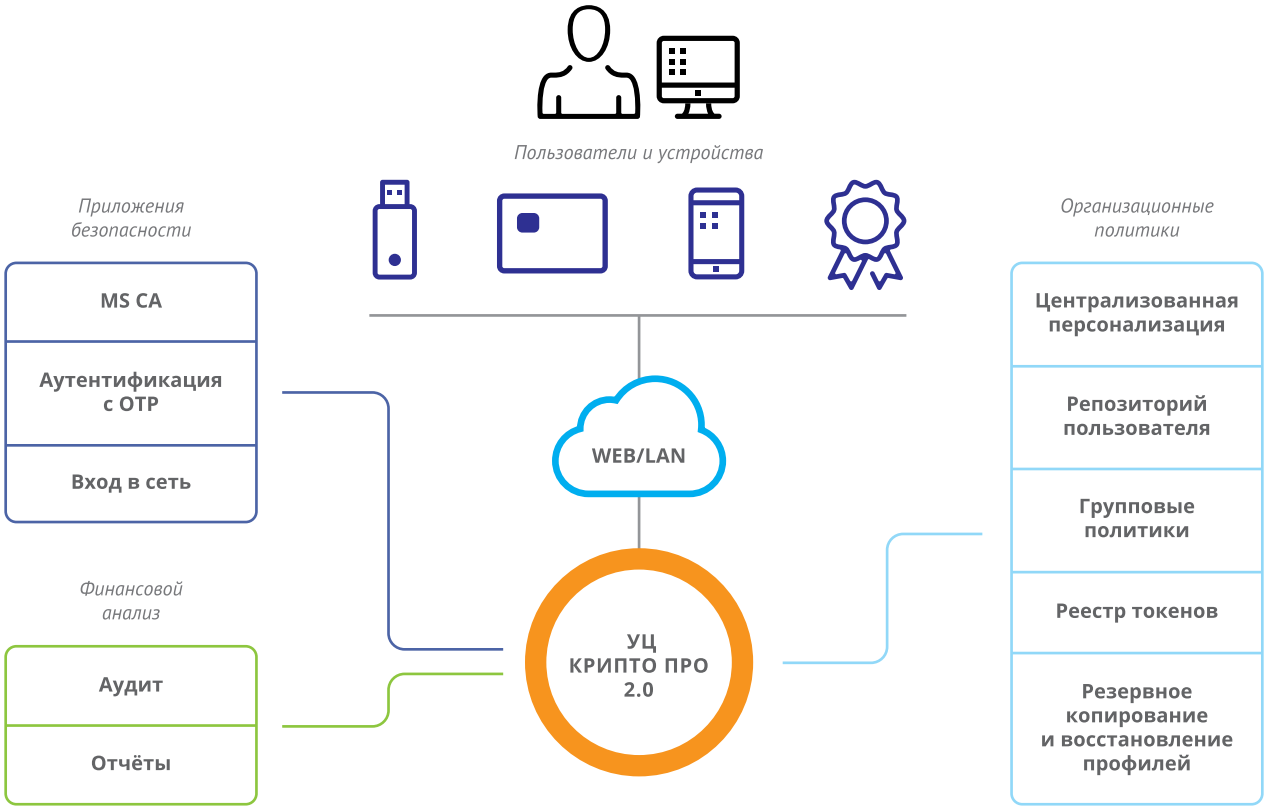
- добавление пользователей в КриптоПро УЦ при назначении пользователю USB-ключа или смарт-карты и выпуска сертификата ГОСТ;
- отправка запроса сертификата в КриптоПро УЦ;
- получение выпущенного сертификата от КриптоПро УЦ и запись его в память USB-ключа или смарт-карты;
- временный отзыв сертификата пользователя с возможностью восстановления в дальнейшем;
- окончательный отзыв сертификата пользователя без возможности восстановления;
- перевыпуск сертификата по истечении его срока действия.

Коннектор позволяет программному продукту SAM взаимодействовать с КриптоПро УЦ версий 1.5 и 2.0.

Архитектура

Коннектор имеет клиент-серверную архитектуру, то есть состоит из двух компонентов:

- клиентской части, которая устанавливается на АРМ офицеров безопасности, занимающихся выпуском и обслуживанием смарт-карт, или на АРМ конечных пользователей – в случае сценариев самообслуживания;
- серверной части, которая устанавливается на сервер SAM.



Настройка

Коннектор имеет набор параметров, настройка которых осуществляется через знакомый администраторам SAM интерфейс, полностью повторяющий интерфейс для настройки политик выпуска смарт-карт в продукте SAM.

Процесс установки и настройки хорошо задокументирован и не вызывает сложностей, даже если вы никогда ранее не работали ни с одним из упомянутых продуктов.

Лицензии

Лицензируется коннектор пакетами по 100, 500 и 1000 пользователей. Также присутствует лицензия на неограниченное количество пользователей.

Лицензия на коннектор является срочной и может поставляться на 1, 2 или 3 года. Данная лицензионная политика позволяет гибко управлять активными лицензиями и не переплачивать за неиспользуемые лицензии.

Сценарий использования

Наиболее распространённым сценарием использования коннектора является следующий.

В компании используются цифровые сертификаты для обеспечения высокой степени защиты при доступе к ИТ-ресурсам и для использования электронно-цифровой подписи в соответствии с ГОСТ (ГОСТ ЭЦП) в корпоративном документообороте.

Выпуск сертификатов

Коннектор может использоваться во всех сценариях выпуска и обслуживания сертификатов, предусмотренных в SAM:

- выпуск пользовательских сертификатов назначенным офицером безопасности;
- выпуск пользовательских сертификатов пользователями через порталы самообслуживания.

При этом пользователь, получающий сертификат, не имеет дополнительных прав доступа к центрам сертификации – процессы выпуска, сопровождения и отзыва сертификата скрыты от пользователя.

Цифровые сертификаты, как и положено, хранятся в памяти смарт-карт (или USB-ключей). Таким образом, у каждого пользователя на смарт-карте есть два сертификата:

- для доступа к ИТ-ресурсам компании, то есть для аутентификации;
- для ГОСТ ЭЦП.

Сертификаты через систему управления SAM запрашиваются из удостоверяющих центров Microsoft Certification Authority и КриптоПро УЦ соответственно. Для организации работы КриптоПро УЦ с SAM как раз и необходим описываемый коннектор.

Таким образом, офицер безопасности (или пользователь – в сценариях самообслуживания) за один запрос на выпуск получает сертификат как из центра сертификации Microsoft, так и из КриптоПро УЦ. Это позволяет сократить время выпуска сертификатов, избежать повышенных полномочий у пользователей, а также минимизировать ошибки, связанные с человеческим фактором.

Кампусная карта

Потребность использования одной карты в разных областях. Карты, используемые для платежей (EMV). Надёжные средства аутентификации в информационных системах (PKI). Карты для систем контроля физического доступа (СКУД).

Карты заполонили нашу жизнь и карманы

Стопка пластиковых карт уже не умещается в портмоне: каждая карта выполняет только одну задачу, возрастает путаница между картами – вместо пропуска на работу прикладываешь банковскую карту, все преследуют выполнение своей задачи, не думая об удобстве пользователя.

Потребность

Потребность использования одной карты в разных областях. Карты, используемые для платежей (EMV). Надёжные средства аутентификации в информационных системах (PKI). Карты для систем контроля физического доступа (СКУД).

Возможности пластиковой карты

- Строгая двухфакторная аутентификация для доступа в корпоративную сеть и распространённые «облачные» сервисы (Microsoft Azure, Office 365, VMware Workspase ONE).
- Карта системы контроля управления доступом (СКУД) для физического прохода в помещения.
- Банковская карта.
- Контактная и бесконтактная.
- Пропуск в студенческие общежития.
- Читательский билет.
- Оплата питания в студенческих столовых.

Безопасность входа в корпоративную сеть

Вход в компьютер только при наличии карты и знании ПИН-кода (аналог банковской карты). Нельзя подсмотреть или украсть пароль. Невозможно скопировать или подделать карту.

Контроль доступа в помещения

Ограничение доступа в учебные корпуса. Ограничение прохода в студенческие общежития с возможностью соблюдения расписания. Ограничение доступа в лабораторные помещения. Визуальный пропуск для проходной.

Банковская карта

Карты выпускаются банком и предоставляются в пользование.

Корпоративный зарплатный проект для выплаты стипендий.

Оплата товаров в вендинговых автоматах на территории учебного заведения.

Оплата питания в столовых учебного заведения (бесконтактные микроплатежи – сокращение очередей).

Уровень безопасности, который требуется ассоциациями и регуляторами в области платежей и безопасности (Visa, MC, EU, ICP).

Читательский билет

Быстрая идентификация студента/аспиранта/преподавателя в библиотечной системе и плата за платные услуги библиотеки.

Расчёты с поставщиками услуг

Организация оплаты всех сервисов, предоставляющих услуги на территории учебного заведения, через бухгалтерию учебного заведения.

Постоплатный расчёт с подрядчиками, предоставляющими платные услуги на территории учебного заведения.

ISIC – международное удостоверение студента

ISIC (International student Identity Card) – международное удостоверение, подтверждающее статус учащегося во всём мире. Пропуск в мир скидок и привилегий:

- скидки и привилегии в 130 странах мира;
- более 42 000 скидок в мире;
- более 3 000 скидок в России.

Возможность бесплатного доступа в музеи, театры и культурные центры мира.

Скидки на авиаперёлеты, проживание в гостиницах и хостелах.

Посещение со скидками кинотеатров, аквапарков, центров развлечений и клубов.

Скидки в кафе, ресторанах и барах.

Привилегии на доп. образование, языковые курсы, тренинги и мастер-классы.

Скидки на покупку туров, страхование и обучение за рубежом.

Скидки на покупки в магазинах и при онлайн-заказах.

Скидки на концерты.

ITIC – международное удостоверение преподавателя

ITIC (International Teacher Identity Card) – это международное удостоверение, подтверждающее статус преподавателя во всём мире.

- Скидки и привилегии в 130 странах мира.
- Более 42 000 скидок в мире.
- Более 3 000 скидок в России.

Возможность бесплатного доступа в музеи, театры и культурные центры мира.

Скидки на авиаперёлеты, проживание в гостиницах и хостелах.

Посещение со скидками кинотеатров, аквапарков, центров развлечений и клубов.

Скидки в кафе, ресторанах и барах.

Привилегии на дополнительное образование, языковые курсы, тренинги и мастер-классы.

Скидки на покупку туров, страхование и обучение за рубежом.

Скидки на покупки в магазинах и при онлайн-заказах.

Скидки на концерты.

Задел на будущее

Удалённый доступ к личному кабинету студента, к лабораторным стендам и экзаменационным порталам.

Электронный медицинский полис для студенческих медучреждений.

Мониторинг посещаемости студентов.

Проездной в общественном транспорте.

Карта в кампусе – оптимизация расходов на электроэнергию, интернет, присутствие в комнате студентов, предотвращение ЧС и т. д.

Доступ на портал gosuslugi.ru.

Этапы внедрения кампусной карты

Кампусная карта внедряется с наращиванием функциональности на каждом этапе.

I этап. Банковская карта

- Пропуск для входа в помещения.
- Карта для входа в корпоративную сеть.

II этап. Читательский билет

- Карта для оплаты услуг на территории института.

III этап. Социальные сервисы

- Личный кабинет на студенческом портале.
- Контроль посещаемости предметов.

«СОВИНТЕГРА»

Поставщик знаний и опыта.

Проектирование и внедрение инфраструктуры (PKI) цифровых сертификатов для ЭП и аутнетификации.

Компетенции по интеграции с аппаратными носителями сертификатов.

Поставщик продуктов Gemalto.

Основной вид деятельности – системная интеграция.

Ключевые компетенции – информационная безопасность.

СОВИНТЕГРА

«СОВИНТЕГРА»
Наша основная специализация – защита ценных информационных активов и полный спектр услуг и решений в сфере ИТ.

+7 (499) 136-27-31
info@sovintegra.ru • www.sovintegra.ru

Как использовать двухфакторную аутентификацию в «облаке» и в офисе

Решения программы безопасного удалённого доступа Citrix Ready составляют полный портфель продуктов, поддерживающих безопасный доступ приложений и данных в любое время, в любом месте, на любом устройстве и в любой сети.

Основные функции внедрения

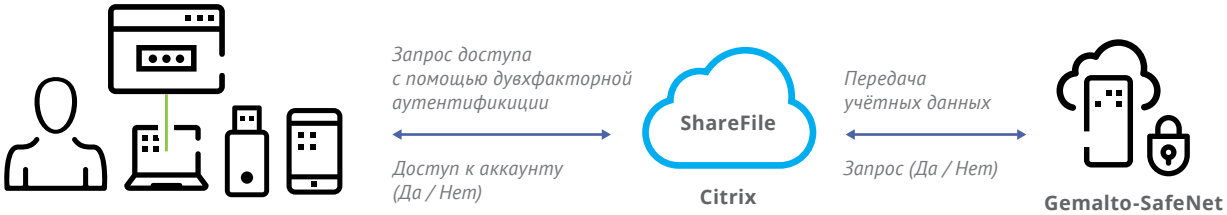
Использование всех преимуществ двухфакторной аутентификации требует внедрения системы, которая предоставляет целый ряд ключевых возможностей и особенностей использования.

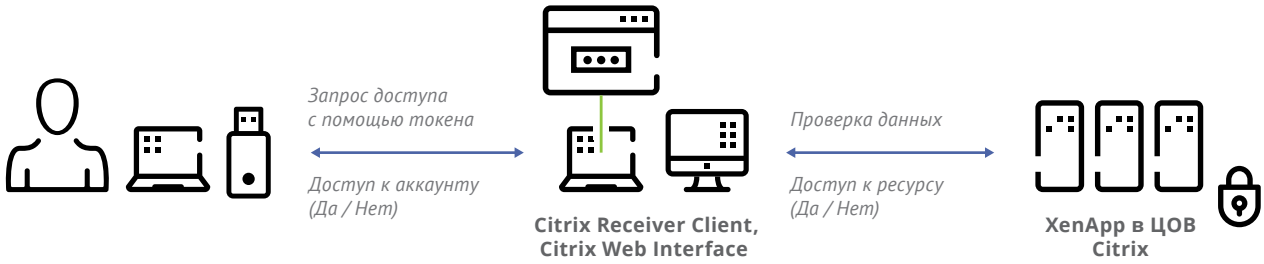
«Облачная» эффективность. «Облачные» решения двухфакторной аутентификации избавляют от необходимости устанавливать и поддерживать программное обеспечение в локальной инфраструктуре предприятия. «Облачные» решения существенно сокращают затраты на управление и сопровождение сервисов и приложений по сравнению с локально установленным ПО, в то же время увеличивая гибкость работы. Они так же позволяют осуществить быструю миграцию в многоуровневые мультиарендные «облачные» среды и могут обеспечить защиту в «облачной», локальной и виртуальной среде. Так, эти сервисы могут предложить до 60 процентов экономии в общей стоимости, почти совершенную надёжность (доступность сервисов – 99,99%) и почти девяностопроцентное сокращение административных накладных расходов.

Совместимость экосистемы. Организации сегодня используют в своей деятельности множество локальных, виртуальных и «облачных» приложений. Согласно обзору компании Gemalto, 92% лидеров в сфере ИТ, обращаясь к двухфакторной аутентификации, хотят защитить как можно больше корпоративных и «облачных» приложений. Это – основной момент, так как простота интеграции определяет количество времени, усилий и ресурсов, которые должна затратить компания, чтобы получить действительно работающее решение, а так же иметь возможность масштабировать строгую аутентификацию на дополнительные приложения при возникновении такой потребности.

Управляемость решения. Так как основной задачей использования двухфакторной аутентификации является усиление защищённости систем предприятия, решение не должно усложнять процедуру управления системой безопасности. Лучшие решения двухфакторной аутентификации обеспечивают функции, облегчающие процедуру управления. Они предлагают централизацию управления политикой безопасности вместе с обширной автоматизацией, которая существенно уменьшает потребность в ручном управлении типичными задачами администрирования, связанными с безопасностью и управлением пользователями.

Управление рисками. Диапазон угроз безопасности разнообразен и постоянно расширяется. Решение двухфакторной аутентификации должно отвечать широкому спектру различных векторов угроз и должно являться единой системой защиты от различных профилей риска.





Обзор решений

Решения программы безопасного удалённого доступа Citrix Ready составляют полный портфель продуктов, поддерживающих безопасный доступ приложений и данных в любое время, в любом месте, на любом устройстве и в любой сети.

Решения Citrix также интегрируются с решениями безопасности третьих производителей для усовершенствования уровня управления системой и защитой идентификационных данных, конечных точек и сетей. Программа безопасного удалённого доступа Citrix Ready была создана, чтобы идентифицировать и продемонстрировать продукты партнёра с доказанной интеграцией с продуктами Citrix и дополнительными уровнями безопасности для улучшения безопасного удалённого доступа. Программа безопасного удалённого доступа Citrix Ready служит средством быстрого и легкого поиска решений, помогая защищать корпоративные сети организаций от кражи данных, DDoS и других атак, которые могут быть направлены на удалённый доступ.

Как лучше всего защититься от атак удалённого доступа

Идентифицирование и доступ. Администраторы должны быть в состоянии подтвердить идентификационные данные пользователей, запрашивающих доступ к системе и ограничить степень предоставленного доступа. По сравнению с простыми системами, основанными на паролях, двухфакторная аутентификация предлагает значительное улучшение возможности корректно подтвердить пользовательские идентификационные данные в запросах на доступ. Степень доступа, предоставленного каждому отдельному пользователю, должна основываться на контексте. Принцип наименьших привилегий помогает гарантировать, что пользователям предоставляют только те права, которые требуются для выполнения их работы.

Сетевая безопасность. Растущий спрос на удалённый доступ усложняет процесс обеспечения безопасности сети. Всё же целостность сетевой безопасности должна сохраняться при поддержке удалённого доступа для мобильных и сторонних пользователей. Сегментация сети и хоста может быть полезной для сокращения числа уязвимых для атаки мест. Реализация многоуровневого подхода помогает улучшить сетевую безопасность при обеспечении доступности.

Безопасность приложений. Все типы приложений – потенциальные цели для хакеров, но взрыв их использования создал много дополнительных точек уязвимости для большинства предприятий. Приложения на мобильных устройствах особенно подвержены взлому. Важный шаг в снижении риска выполняет централизация и зашифрованная доставка приложений. Контейнеризация для мобильных приложений и контроль входящих потоков данных может помочь уменьшить уязвимость системы безопасности, связанную с использованием приложений.

Безопасность данных. Безопасность данных предприятия может быть улучшена централизацией и передачей данных с помощью усиления безопасности совместного доступа к файлам (для уменьшения потерь данных) и контейнеризацией данных (как в пути, так и в покое).

Мониторинг и реагирование. Бдительность и быстрое реагирование необходимы для успешного противостояния атакам. Быстрая реакция на попытки взлома так же критически важна, учитывая, что даже наиболее защищённые системы могут быть уязвимы к успешным атакам. Быстрое обнаружение и реагирование на успешные атаки позволяют минимизировать ущерб и помогают снизить чувствительность к неизбежным новым атакам. Непрерывная видимость трафика приложений обеспечивает более быстрое выявление нарушений безопасности и системных отклонений.

Главные особенности решений Gemalto

- Эффективное управление рисками. Решения Gemalto позволяют гарантировать различные уровни безопасности, и соответствовать ожиданиям пользователей, предлагая самый широкий диапазон методов аутентификации и форм-факторов.
- Простота администрирования. Полностью автоматизированные процессы администрирования жизненного цикла пользователей, токенов и прав доступа вместе с полностью автоматизированными предупреждениями угроз и созданием отчётов, приводят к сокращению времени на управление на целых 90%.
- Эффективность «облаков». Когда строгая аутентификация развёрнута как услуга (опционально), организации могут экономить до 60% на затратах внедрения и поддержки.
- Надёжность производителя. Более 30 лет неизменного превосходного уровня качества сервиса завоевали для Gemalto доверие тысяч предприятий по всему миру.

CITRIX® Ready

Citrix

www.citrixready.citrix.com

Распознавание лиц

Биометрическая идентификация лица и обнаружение движущихся транспортных средств или пешеходов и других объектов с использованием данных с цифровых камер видеонаблюдения высокого разрешения в реальном времени.

Функции и возможности

- Распознавание лиц в режиме реального времени, извлечение шаблона и сопоставление с базой данных.
- Одновременное отслеживание нескольких лиц или объектов, передвигающихся в видео в реальном времени.
- Расширенное определение движущихся объектов и классификация отслеживаемых пешеходов и транспорта. Определение пола, оценка возраста, выражения лица и определение очков.
- Автоматическое создание журнала событий и отчётов, также как и регистрирование новых лиц с видеотрансляции и автоматическое добавление их в список наблюдения.
- Поддержка больших систем наблюдения за счёт подключения нескольких камер к компьютеру и быстрой синхронизации между компьютерами в сети. Разумные цены, гибкое лицензирование и бесплатная техническая поддержка клиентов.

Принцип действия

Модуль распознавания лиц работает с камерой и детектором лиц. Сначала детектор определяет появление в кадре лица и захватывает его изображение. Далее возможны две схемы работы модуля распознавания лиц: идентификация и верификация.

В режиме идентификации захваченное лицо сравнивается со всеми изображениями лиц, хранящимися в базе данных. Таким образом выясняется, в частности, наличие человека в базе данных нежелательных посетителей или VIP-клиентов какого-либо заведения.

В режиме верификации лицо человека, воспользовавшегося карточкой-пропуском или каким-либо другим идентификатором личности для прохода через турникет или дверь с электронным замком, сравнивается с фотографией владельца пропуска, хранящейся в базе данных. Таким образом можно выяснить, является ли человек, пытающийся получить доступ, тем, за кого он себя выдаёт.

В настройках модуля задаются значения степени сходства, соответствующие границам так называемых зон сходства. Допускается задание трёх зон: красной – высокая степень сходства, жёлтой – средняя степень сходства и зелёной – низкая степень сходства. При высокой степени сходства распознанное лицо, а также дата, время распознавания, номер камеры, захватившей лицо, и процент сходства сохраняются в базе распознанных лиц. Степень сходства визуально отображается на мониторе оператора при помощи соответствующего цвета, что облегчает контроль работы системы.

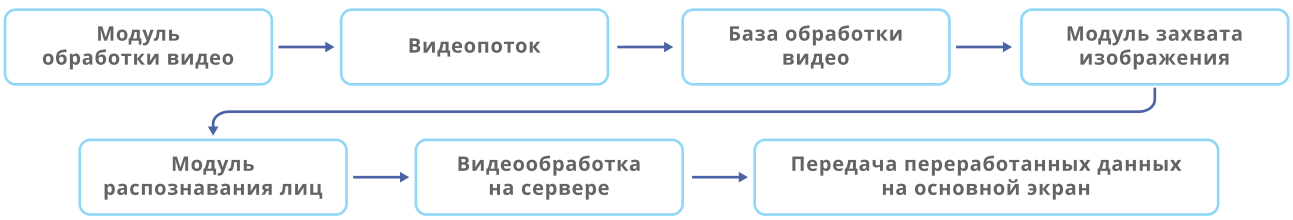
Помимо распознавания модуль позволяет удалять существующие записи из базы данных эталонных изображений, с которыми производится сравнение, или вносить новые записи, содержащие изображение и личные данные человека: ФИО, отдел, комментарий. В качестве эталонного изображения может использоваться как цифровая фотография, заранее загруженная в базу данных модуля, так и изображение, захваченное камерой системы при проходе человека через пост видеоконтроля. Модуль позволяет проверить одну фотографию или все фотографии в базе на соответствие биометрическим стандартам систем автоматической идентификации личности.

Алгоритмы системы видеонаблюдения

В зависимости от проектирования системы видеонаблюдения используются различные алгоритмы.

Биометрический алгоритм распознавания лиц предоставляет следующие возможности для систем видеонаблюдения.

- Множественное обнаружение лиц, функции извлечения и сопоставления шаблона с внутренней базой данных в режиме реального времени.
- Автоматическое распознавание лиц осуществляется во всех последовательных кадрах видео-



источника, пока лица не исчезнут из поля зрения камеры. Алгоритм слежения за лицом использует динамические модели прогнозирования лица и движения, которые делают его устойчивым к преграждениям как другими объектами, так и другими лицами. Алгоритм может продолжать отслеживать лицо, даже когда оно снова появляется, после того как полностью скроется за преградой.

- Определение пола человека в кадре.
- Определение возраста каждого человека.
- Обнаружение улыбки, открытого рта, закрытых глаз, очков и солнцезащитных очков.

Алгоритм отслеживания движения и слежения выполняет расширенное определение движущихся объектов в поле зрения, классифицирует их и отслеживает, пока они не исчезнут. Ниже представлены функции, доступные для систем видеонаблюдения.

- Классификация объектов на основе размера и скорости движения. Например, пользователи могут настроить систему наблюдения, чтобы определить, является ли отслеживаемый объект транспортным средством, пешеходом или группой пешеходов.
- Контроль запретных зон. Алгоритм может обнаруживать и сообщать, если люди или объекты входят, находятся или покидают запретную зону. События срабатывают, когда люди или объекты пересекают заранее определённые границы или входят в многоугольную область.
- Устойчивость к погодным условиям. Алгоритм игнорирует дождь и снег, а также деревья и кустарники, на которые дует ветер.
- Автоматический режим работы. Система может записывать в журнал появление, исчезновение и отслеживание лиц, пешеходов или объектов. Обнаруженные лица сопоставляются со списком наблюдения во внутренней базе данных, и распознанные лица немедленно передаются в систему. Система использует отслеживаемое лицо для автоматического приёма из видеопотока и добавления новых шаблонов для него «на лету».
- Поддержка больших систем видеонаблюдения. Есть возможность интегрировать свои технологии в системы видеонаблюдения с несколькими камерами и несколькими узлами обработки данных. Один компьютер может обрабатывать видеоданные с нескольких камер одновременно.
- Обработка видеофайлов. Также можно принимать данные из видеофайлов. Видеофайлы обрабатываются в режиме реального времени как поступающие от виртуальной камеры, поэтому часовое видео будет обработано в течение часа.

Детектор скоплений людей

Детектор скоплений людей позволяет предупредить опасные моменты, массовые беспорядки на улицах города, площадях, в парках, на вокзалах, в торговых комплексах и других общественных местах. Функция автоматически оповещает оператора, если количество людей в зоне превышает заданное пороговое значение. Возможно задать два пороговых значения, при которых будут генерироваться сообщения «Внимание» и «Тревога».

Детектор оставленных предметов

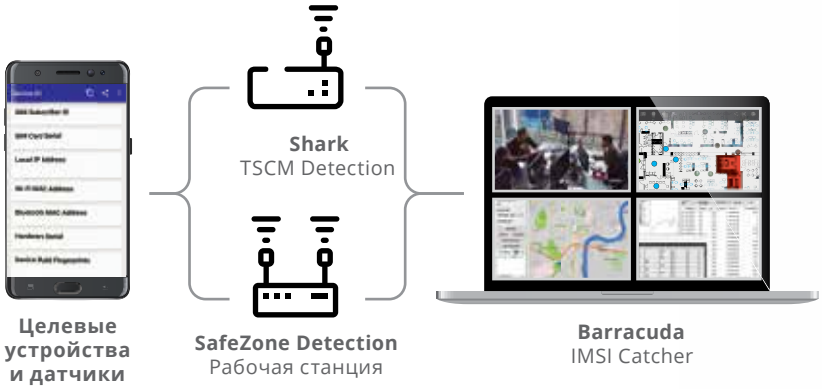
Детектор оставленных предметов позволяет задать время нахождения неподвижного объекта в зоне наблюдения, по истечении которого оператор будет получать тревожный сигнал. При работе с архивом возможно найти время появления и исчезновения предмета, а также быстро найти человека, который оставил или забрал предмет.

Особенности решения

- Распознавание лиц в реальном времени – быстрые и точные алгоритмы обработки.
- Поддержка огромного количества камер.
- Возможность получения видеопотока из других решений.
- Интеграция с системами безопасности.
- Гибкая лицензионная политика.
- Отечественная разработка.

SafeZone Detection Suite

Тактическое обнаружение и блокировка мобильных телефонов, устройств Wi-Fi и широкополосных передатчиков в общественных и закрытых зонах как внутри помещений, так и снаружи.



Как это работает

Идентифицируйте широкий диапазон беспроводных передатчиков, мобильных телефонов, Wi-Fi устройств, камер и других радиопередающих устройств.

Манипуляционный сенсор

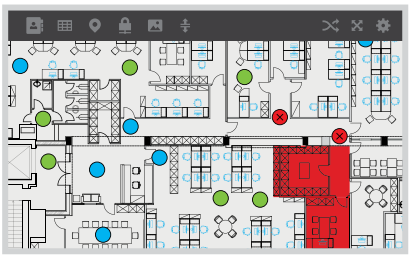
Barracuda X56 IMSI Catcher выполняет подмену ячейки сотовой связи с широким охватом территории, заставляя мобильные телефоны регистрироваться через собственную ячейку. Когда мобильные телефоны в зоне охвата зарегистрированы, Barracuda X56 идентифицирует уникальные номера IMSI и TMSI, связанные с каждым телефоном. Манипуляционный сенсор BLER Barracuda X56 поддерживает функции белого и чёрного списков, изменение частоты с 3G до 4G или 2G, а также более продвинутые функции.

Контролируемая территория

Комбинация из RF Detection и IMSI Catcher Sensor, управляемая через SafeZone Monitoring Suite, позволяет обнаруживать и идентифицировать радиопередающие устройства в запретной зоне в режиме реального времени. Уведомляет соответствующий персонал. Получает идентифицирующую информацию о подозрительном телефоне или радиопередатчике и предотвращает его использование подозреваемым.

Сенсор обнаружения

SHARK – это наблюдательно-противодействующее решение, которое позволяет организациям выявлять и контролировать широкий спектр беспроводных передатчиков, мобильные телефоны, устройства Wi-Fi, камеры и другие устройства с РЧ-передатчиком.



Обнаружение мобильных устройств

Mobile Device ID. Идентифицирует IMSI- и TMSI-номера, уникальные для каждого телефона.

Trigger Control. Опция, позволяющая получить контроль над функциональностью целевого телефона.

Device Alerts. Получение оповещений и уведомлений, когда телефоны из белого или чёрного списка идентифицированы.

Device Compatibility. Обнаружение любого устройства, включая сети 2G, 3G и 4G.

Компоненты системы

- SafeZone Monitoring Suite.
- RF Detection Sensor (GSM, UMTS, LTE, Wi-Fi).
- IMSI catcher Sensor (GSM, UMTS, LTE).

Команда экспертов

BLER Ltd. – это компания производитель технологий, предлагающая решения, помогающие клиентам осуществлять сбор информации, а также увеличивать уровень защищённости.

Наш обширный опыт включает успешное развёртывание систем для поставщиков телекоммуникационных услуг, правительств и многих других компаний и организаций во всём мире.

Системы компании BLER Ltd. являются важными инструментами в работе профессионалов в области безопасности и защищают жизни людей.

СОВИНТЕГРА

«СОВИНТЕГРА»
Наша основная специализация – защита ценных информационных активов и полный спектр услуг и решений в сфере ИТ.

+7 (499) 136-27-31
info@sovintegra.ru • www.sovintegra.ru

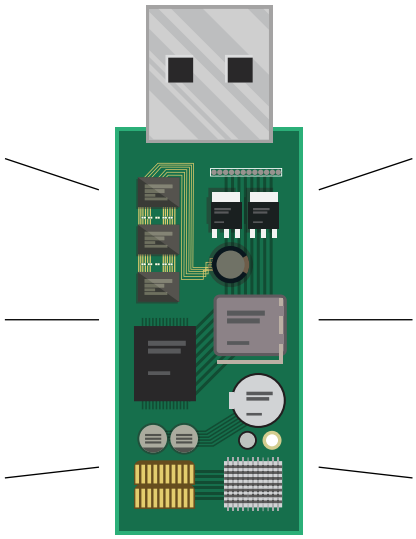
Безопасный VDI в кармане

eToken VDI – это комплексное решение для обеспечения безопасного доступа мобильным сотрудникам без привязки к определённому устройству. eToken VDI работает как загрузочное устройство с преднастроенной средой безопасного доступа для работы с VDI либо удалённым рабочим местом.

Live OS
Операционная система, не требующая установки и готовая к работе сразу после загрузки с носителя. Такое решение позволяет предоставить единую среду работы вне зависимости от аппаратного обеспечения, которое может быть использовано для работы.

Флэш-память
Используется для хранения пользовательских данных и преднастроенной операционной системы. Хранимые данные могут быть зашифрованы.

User Content
В образ операционной системы можно добавить любой пользовательский контент либо программное обеспечение, совместимое с используемой операционной системой.



Чип смарт-карты
Чип смарт-карты используется для аппаратных криптографических преобразований, таких как генерация ключевой пары, электронная подпись и шифрование. Чип токена защищён от вскрытия и взлома.

VPN-клиент
VPN-клиент позволяет установить защищённое соединение с удалённым криптографическим шлюзом для дальнейшей работы по защищённому каналу связи из любой недоверенной среды.

VDI-клиент
Позволяет подключиться к виртуальной либо удалённой машине и использовать её в качестве рабочего места.

eToken VDI Client | IBM-совместимый компьютер | Криптографический шлюз | Виртуальная или удалённая машина

Решаемые задачи

Загрузка Live-режима доверенной операционной системы с VDI Flash при подключении к любому поддерживаемому устройству. Защита входа в операционную систему.

- Защита канала передачи данных от VDI Flash до информационной системы.
- Подключение к удалённому рабочему столу пользователя с использованием клиента VDI.
- Обеспечение двухфакторной аутентификации в операционную систему удалённого рабочего стола с помощью USB-токенов.

Безопасность

Многоуровневая защита пользовательских данных, сетей передачи информации, доступа к информационным ресурсам.

Требования к системе

Необходимо обеспечить работу в недоверенной системе через недоверенные сети передачи данных с применением сертифицированных средств защиты информации, обеспечивающих защиту данных пользователя, защиту канала передачи данных, защищённый вход в систему.

Простота встраивания

Решение без проблем интегрируется в любую корпоративную инфраструктуру.

Завершённость

Решение уже содержит всё необходимое для удалённого доступа и не требует никаких дополнительных аппаратных либо программных средств, кроме IBM-совместимого компьютера.

Сертифицированные средства защиты

Применяются сертифицированные средства защиты и средства криптографической защиты информации.

Универсальность

Решение работает с любыми IBM-совместимыми компьютерами, подключается к любым виртуальным либо удалённым рабочим столам вне зависимости от используемого гипервизора.

ТОНКости безопасности

VDI-клиенты, как замена традиционным ПК и переход к централизованным вычислениям, повышют продуктивность, дают колоссальные преимущества и возможности для роста.

Разнообразие клиентского оборудования

Тонкие клиенты, нулевые клиенты, серверы, ноутбуки, планшеты и мобильные устройства, так или иначе участвующие в корпоративной жизни пользователя требуют унифицированной и устройствонезависимой политики безопасности. ИТ- и ИБ-службы организации должны решить сложную задачу – одновременно сохранить уникальные возможности различных типов устройств и обеспечить их равно высоким уровнем безопасности.

Уязвимости статических паролей

Организации, использующие для доступа к корпоративным системам исключительно пароли, ставят под угрозу стабильность бизнеса, подвергая свои информационные активы таким рискам, как фишинг, «человек посередине», социальная инженерия, подбор пароля, кража учётных данных. И как итог, несанкционированный доступ к корпоративным ресурсам, приводящий к разглашению коммерческой тайны, финансовым и репутационным потерям.

Доступ из любой точки

Некоторые организации разрешают доступ к своим инфраструктурам только внутри периметра корпоративной защиты, другим же компаниям, наоборот, требуется разрешить доступ из-за пределов контролируемой зоны (DMZ) внешним консультантам, партнёрам или удалённым сотрудникам.

Всё это приводит к тому, что усиленный контроль за доступом пользователей с различных устройств и из любого места становится очень важной задачей и частью информационной системы.

Надёжное решение

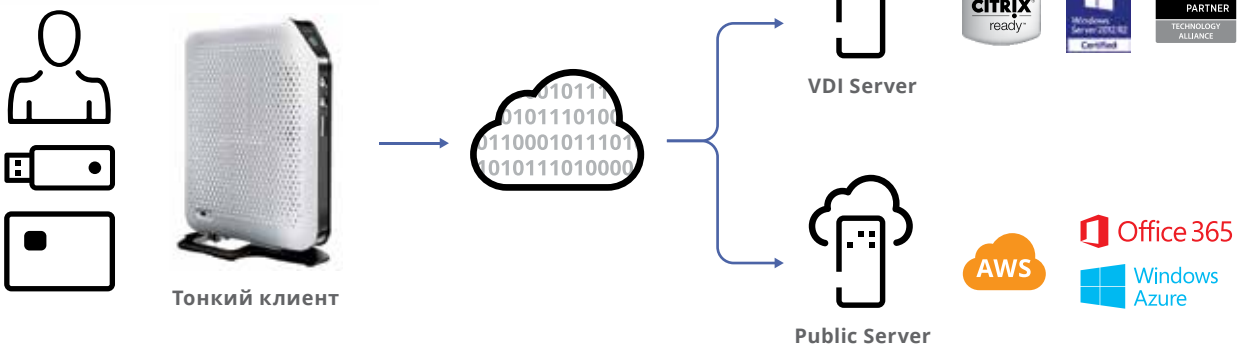
Совместное использование тонких клиентов ТОНК и решений по безопасности компании Gemalto-SafeNet с лёгкостью может устранить описанные сложности и получить все преимущества централизованных вычислений.

Возможности

- Двухфакторная аутентификация пользователей в корпоративной системе в различных сценариях: терминальных сеансах, VPN-соединениях, доступе к «облачным» платформам VDI.
- Блокирование терминального сеанса при отсоединении токена или смарт-карты.
- Возможность использования электронной подписи в прикладных приложениях.
- Карта может служить пропуском в помещение (наличие RFID-метки), также может являться платёжной (MasterCard или Visa) или транспортной картой с корпоративным стилем организации.
- Наличие сертификата ФСТЭК позволяет соответствовать требованиям регуляторов рынка информационной безопасности и упрощает аттестацию ИС.
- Встроенная поддержка SSL VPN.
- Готовые интеграции с большинством популярных отечественных или западных решений.

3 года гарантии

Если ваш тонкий клиент сломался, мы в течение трёх лет безоговорочно его заменим.



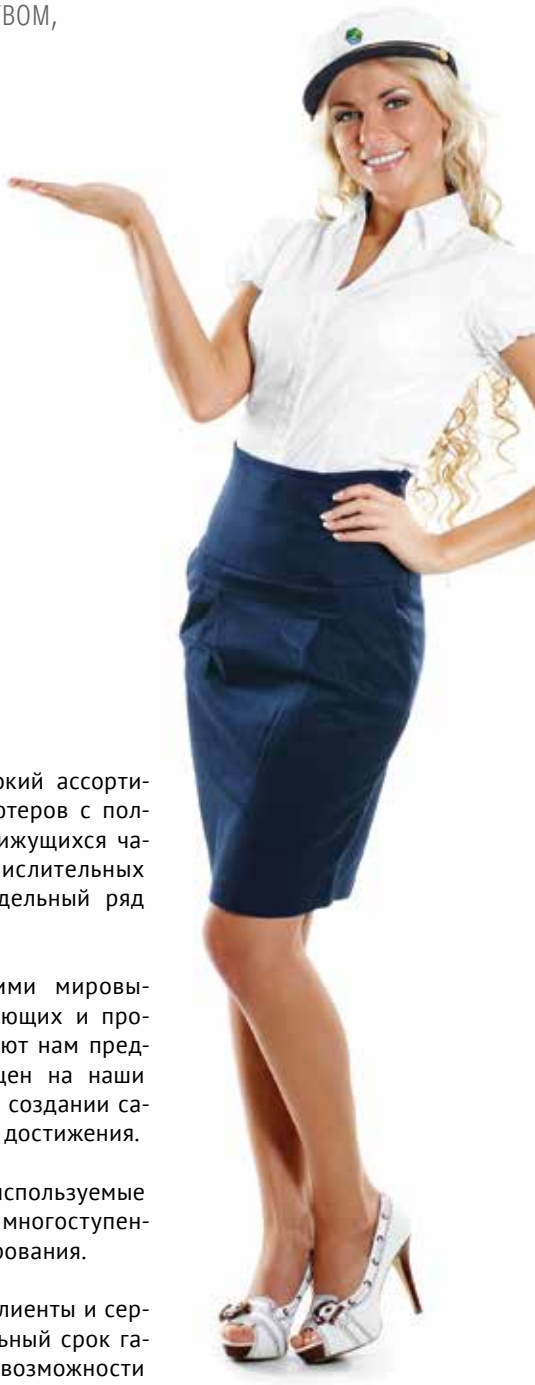
рабочих мест сотрудников

Компании ищут согласие между максимальной безопасностью и удобством, минимизацией затрат и продуктивностью.

Платформа TN1400

SafeNet eToken 5110

АПМДЗ «Соболь»



Уровни применения двухфакторной аутентификации

АПМДЗ, локально (в ОС тонкого клиента, или в каталоге LDAP) и удалённо – на VDI-сервере или в «облачном» решении.

SafeNet

SafeNet eToken 5110 входит в состав программно-аппаратного комплекса аутентификации и хранения ключевой информации «Электронный ключ SafeNet eToken 8» (сертифицирован по требованиям ФСТЭК сертификат №2730).

«Соболь»

Платформы TN1400, TN1600, TN1900 и TN2800 могут поставляться совместно с аппаратно-программным модулем доверенной загрузки (АПМДЗ) «Соболь», и это позволяет решить дополнительные задачи:

- создание доверенной программной среды для повышения класса защиты СКЗИ;
- защита компьютеров от несанкционированного доступа и обеспечение доверенной загрузки.

ТОНК

Решения по безопасности Gemalto-SafeNet поддерживаются всей действующей линейкой решений компании ТОНК под управлением Microsoft Windows, защищённых российских ОС ALT Linux, Astra Linux.

С 2007-го года ТОНК осуществляет серийное производство и дистрибуцию компьютерного оборудования под собственной торговой маркой.

Сегодня ТОНК предлагает широкий ассортимент тонких клиентов и компьютеров с полным отсутствием каких-либо движущихся частей, специализированных вычислительных систем, а также обширный модельный ряд серверов.

Прямые соглашения с ведущими мировыми производителями комплектующих и программного обеспечения позволяют нам предложить оптимальный уровень цен на наши продукты и использовать при их создании самые последние технологические достижения.

Выпускаемая продукция и все используемые нами комплектующие проходят многоступенчатую систему проверки и тестирования.

На все продукты ТОНК: тонкие клиенты и серверы – предоставляется длительный срок гарантии – 3 года. Опираясь на возможности созданной сервисной сети, мы обеспечиваем доступное и качественное обслуживание на всей территории России.

СОВИНТЕГРА

«СОВИНТЕГРА»
Центр компетенции по информационной безопасности, системный интегратор и поставщик решений Gemalto-SafeNet и ТОНК.

+7 (499) 136-27-31
info@sovintegra.ru • www.sovintegra.ru

Новые времена, новые возможности и решения по 2FA в ЦОД

Смарт-карты и USB-токены eToken – специализированные устройства, обеспечивающие двухфакторную аутентификацию (2FA) для доступа к информационным ресурсам с использованием стойких криптографических алгоритмов.

Технология One Time Password (OTP) – усиленная аутентификация, где пароль действует только в течение одного сеанса.

Новые времена и новые возможности

Изменения продуктовых линеек и бизнес-моделей ключевых производителей сферы ИТ меняют рынок. Стремительный рост потребления «облачных» сервисов Microsoft, легкость использования и продажи конечным потребителям порождают новую высококонкурентную среду.

Для уверенного роста на быстрорастущем рынке «облачных» услуг необходимо дополнять сервисы уникальными возможностями, один из путей – использование 2FA в качестве дополнительной услуги к сервисам ЦОД.

Новые решения по 2FA

- Получить выгодное отличие от конкурентов за счёт уникального сервиса безопасного доступа.
- Значительно повысить безопасность предоставляемых услуг.
- Увеличить лояльность и доверие клиентов к поставщику услуг.
- Расширить покрытие клиентской сети за счёт лёгкого входа заказчиков с уже внедрённой 2FA.
- Увеличить доходность путём расширения продуктового портфеля.
- Упростить продажи сервисов в государственные структуры применяя сертифицированные решения.

Новые решения с ЦОД

- By-Design поддержка многопользовательской архитектуры.
- Готовая интеграция с большинством решений отечественных и западных производителей.
- Быстрое встраивание новых сервисов.
- Зрелость технологий и продуктов к масштабным внедрениям.
- Соответствие требованиям российских регуляторов в области ИБ. Программно-аппаратный комплекс аутентификации и хранения ключевой информации «Электронный ключ SafeNet eToken 8», сертифицирован ФСТЭК России. Сертификат соответствия №2730.

Практическая ценность для клиентов

- Избавление от недостатков статических паролей.
- Применение аппаратных устройств значительно усиливает безопасность и устраняет необходимость в использовании паролей.
- Повышение мобильности.
- Технология OTP интегрирует в ИС мобильные устройства и минимизирует «теневую» ИТ.
- Безопасная гибридная среда.
- Лёгкость объединения/добавления «облачных» и локальных сервисов.
- Повышение доверия к «облачному» провайдеру.
- Разделение зон контроля – служба ИБ заказчика полностью контролирует учётные данные пользователей без передачи их в «облако».
- Удобство использования и администрирования.
- Не требуется высоких компетенций пользователей, простота самообслуживания, снижение административной нагрузки.
- Модернизация систем, требующих аутентификации (корпоративный портал, электронная почта, CRM-система, удаленный VPN-доступ, Wi-Fi).

Безопасный доступ

SaaS. Microsoft – Пакет Office 365, MS Dynamics CRM Online, SharePoint Online, OneDrive for Business, Project Online, Power BI, Azure Backup и т. д.

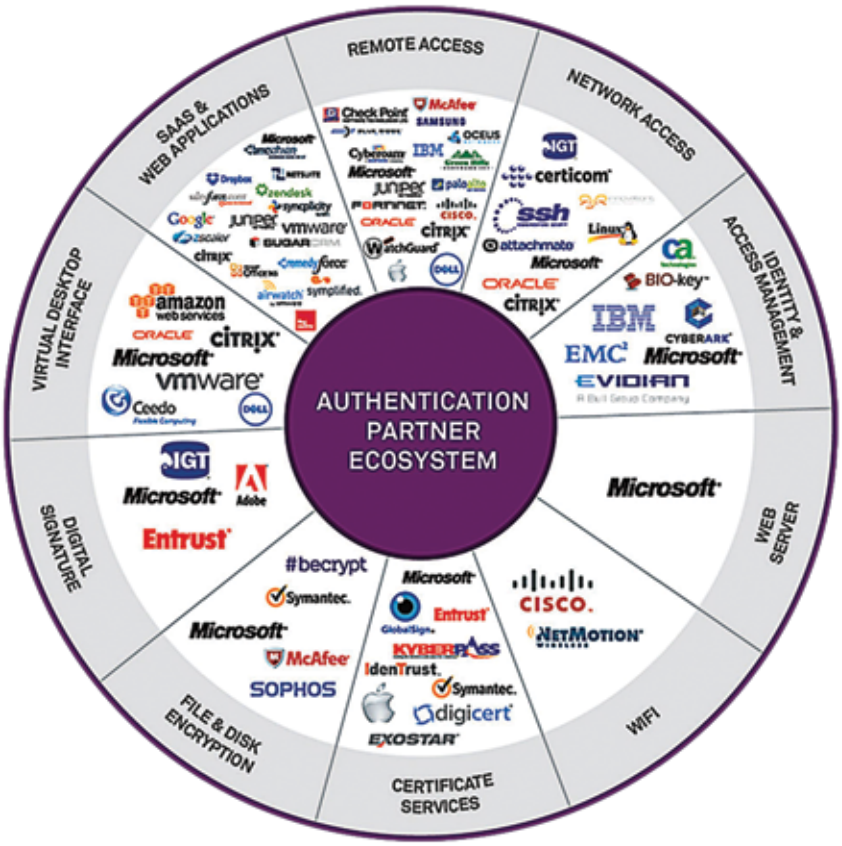
Сотни SaaS и 2500 приложений Azure Marketplace – SAP, Sales Force, Dropbox, Citrix, VMWare, BizTalk, Google, Facebook, Twitter, LinkedIn.

IaaS. Локальный и удалённый доступ, поддержка VPN, SSL, EFS, Wi-Fi, Secure Mail, VDI – RDP, ICA, PCoIP.

PaaS. Лёгкое встраивание через SDK и поддержка за счёт готовых клиентов и использования стандартов RADIUS, SAML, WS-Fed.

Возможные кросс-проекты

- Внедрение электронной подписи.
- Единая карта сотрудника, кампусная карта (СКУД, транспорт, платёжное приложение, PKI-приложение).



Компоненты, необходимые для внедрения

- Устройства безопасности (смарт-карты/токены) или лицензии на OTP-сервис (одно устройство или лицензия на пользователя).
- Подписка на «облачный» сервис (SAP, Azure, Office 365, CRM Online, и т. д.).
- Работы на стороне локальной инфраструктуры клиента:
  - внедрение PKI (Public Key Infrastructure) при использовании смарт-карт и токенов;
  - развёртывание и настройка федеративных сервисов, сервиса синхронизации и SSO.
- Работы на стороне поставщика услуг:
  - запуск в эксплуатацию IDaaS на базе решения SafeNet Authentication Service (при использовании технологии OTP);
  - опциональная интеграция с действующими системами ЦОД: репозитории пользователей, порталы управления, биллинга.
- Программно-аппаратный комплекс SafeNet Authentication Service сертифицирован ФСТЭК России.
- Сертификат соответствия №3070. Действителен до 27.01.2020.

Целевая аудитория

Все бизнес-вертикали как в государственном, так и коммерческом секторах экономики, сегменты от SMB, где более востребованы OTP-решения и до LB, где более применимы смарт-карты и USB-токены, а так же любые организации, где:

- есть потребность в усилении информационной безопасности;
- требуется обеспечить единую среду доступа при переходе к «облачным» сервисам;
- необходимо повысить управляемость и контроль за удалённым доступом мобильных пользователей;
- необходимо разграничить внутрикорпоративную «теневую» ИТ;
- есть наличие широкого мультивендорного ИТ-ландшафта.

СОВИНТЕГРА

«СОВИНТЕГРА»
Наша основная специализация – защита ценных информационных активов и полный спектр услуг и решений в сфере ИТ.

+7 (499) 136-27-31
info@sovintegra.ru • www.sovintegra.ru

Gemalto-SafeNet Authentication Service обеспечивает безопасную аутентификацию в Инбанке

Для обеспечения защищённого доступа к своим ресурсам и расширения возможностей доступа с мобильных устройств Инбанк внёс изменения в существующие процедуры контроля доступа, не усложняя доступ для конечных пользователей за счёт внедрения Gemalto-SafeNet Authentication Service.

«Благодаря своему опыту Gemalto выполнила все требования Инбанка по внедрению гибкой, но надёжной двухфакторной аутентификации.»

Юрий Кузьмин
технический директор компании DPS «Системы защиты данных»

Бизнес-требования

Ранее Инбанк использовал парольную аутентификацию для проверки подлинности. Однако угрозы безопасности эволюционируют, и сейчас этот подход не в полной мере удовлетворяет высоким требованиям безопасности, которым традиционно соответствует банк. В то же время банк борется с растущим числом кибератак и решает задачу работы в своих системах мобильных пользователей, привыкших к планшетам и смартфонам. При оценке решений, дополняющих существующие решения по контролю доступа, начальник службы информационной безопасности Евгений Соколов требовал выполнения следующих условий.

- **Усиление безопасности.** Необходима система контроля доступа, обеспечивающая безопасную двухфакторную аутентификацию с использованием, помимо традиционных статических паролей, одноразовых паролей, генерирующихся случайным образом для каждой попытки логина (OTP).
- **Гибкость.** Служба информационной безопасности Инбанка стремилась внедрить решение, которое не зависело бы от аппаратных или программных платформ, обеспечивая аутентификацию на любых пользовательских устройствах без необходимости использовать считыватели смарт-карт или USB-порты, необходимые для аппаратных токенов. Кроме того, не на последнем месте была возможность обеспечить двухфакторную аутентификацию пользователей в других странах, не заставляя их зависеть от ненадёжных и легко взламываемых SMS-сообщений.
- **Эффективность администрирования.** Команда Инбанка стремилась избежать проблем, связанных с управлением сертификатами в токенах путём внедрения централизованного администрирования и средств контроля, которые будут соответствовать конкретным требованиям информационной безопасности банка.

Задача

Построить надёжную систему двухфакторной аутентификации, чтобы обеспечить доступ сотрудников к виртуальным рабочим столам и в то же время обеспечить удобство использования.

Решение

Инбанк использовал Gemalto-SafeNet Authentication Service, включая программные аутентификаторы MobilePass (PCE).

Преимущества

Gemalto-SafeNet Authentication Service позволяет службе информационной безопасности Инбанка управлять политиками доступа для сотрудников и обеспечивает сотрудникам доступ к ресурсам.

Мнение Юрия Кузьмина

«Gemalto-SafeNet Authentication Service обеспечивает полностью автоматизированную усиленную аутентификацию как в виде «облачного» решения, так и в виде локальной инсталляции с большим количеством как программных, так и аппаратных токенов, состав которых легко подобрать для обеспечения уникальных потребностей любой организации. В решении были рассмотрены требования банка к эффективному управлению системой двухфакторной аутентификации, а так же поддержка других подходов и форм-факторов, в том числе Gemalto-SafeNet MobilePASS, приложение OTP для мобильных устройств, настольных компьютеров и компьютеров Mac. Предложенное решение так же упростило управление пользователями разграничением доступа и токенами в сочетании с автоматизацией рутинных процессов и лёгкой интеграцией с приложениями и службами каталогов, такими как Microsoft Active Directory. Неотъемлемой частью решения о выборе SafeNet Authentication Service было то, что оно было предложено компанией Gemalto, которая является лидером на рынке аутентификации, признанным Gartner и другими независимыми отраслевми аналитиками.»

Цель

Специализация компании «Data Protection Systems» – информационная безопасность банков и кредитных организаций.

Наша цель при выполнении проектов – при минимальном вмешательстве в бизнес-процессы банка и его ИТ-инфраструктуру обеспечить соответствие требованиям регуляторов и повысить реальный уровень информационной безопасности.

gemalto
security to be free

Gemalto

www.safenet.gemalto.com
www.gemalto.com

TESSIS

***TESSIS** – официальный дистрибьютор в России*

www.tessis.ru

«Инфозащита» и Gemalto предотвратили перехват паролей

Исполнитель

Компания «Инфозащита», ведущий специализированный интегратор, реализующий комплексные проекты в области информационной безопасности, завершила работы по внедрению системы двухфакторной аутентификации на базе продукта Gemalto в крупнейшей железорудной компании в России и СНГ. В результате внедрения были минимизированы угрозы, связанные с несанкционированным подключением к корпоративной сети компании через VPN-подключения.

Заказчик

Крупнейшая железорудная компания в России и СНГ является мировым лидером в производстве товарного горячебрикетированного железа, ведущим производителем и поставщиком железорудной и метализованной продукции и одним из региональных производителей высококачественной стали.

Задача

Перед заказчиком стояла задача свести к минимуму перехват паролей пользователей при установлении VPN-подключения к корпоративной сети и данным компании.

Решение

Перехват паролей становится бесполезным для злоумышленников, если в процедуру аутентификации добавляется второй фактор – в данном случае одноразовый пароль (OTP – one time password). Поскольку OTP уникален для каждого сеанса, даже при перехвате им нельзя воспользоваться для повторной аутентификации и несанкционированного доступа. Двухфакторная аутентификация гарантирует, что доступ к корпоративной сети информации надёжно защищён.

Компания «Инфозащита» и решение SafeNet Authentication Services компании Gemalto помогли крупнейшей железорудной компании в России и СНГ решить важную задачу по получению защищённого доступа к корпоративной инфраструктуре.

Специалисты «Инфозащиты» качественно и в срок развернули и интегрировали решение SafeNet Authentication Service в существующую инфраструктуру крупнейшей железорудной компании в России и СНГ – в межсетевой экран Cisco ASA, обеспечивающий доступ через VPN-соединение. Для получения доступа к корпоративной сети через ПО Cisco AnyConnect сотрудник вводит привычный логин и пароль Microsoft Active Directory, автоматически получает OTP, сгенерированный на сервере безопасности SafeNet, на свой мобильный телефон посредством SMS и завершает процесс аутентификации вводом OTP.

Использование мобильного телефона сотрудника в качестве аутентификатора (источника OTP) увеличивает безопасность системы и минимизирует риски потери сотрудниками отдельных аппаратных аутентификаторов, к примеру, в форм-факторе брелока, и лишить себя возможности выполнить удалённое подключение.

Помимо решения конкретной задачи в крупнейшей железорудной компании специалисты «Инфозащиты» учли потенциальные возможности масштабируемости системы при выборе производителя. Внедрённая система позволит заказчику использовать механизм двухфакторной аутентификации в смежных системах и повысить уровень информационной безопасности компании в целом.

gemalto
security to be free

Gemalto

www.safenet.gemalto.com
www.gemalto.com

TESSIS

TESSIS *– официальный дистрибьютор в России*

www.tessis.ru

ИНФОЗАЩИТА

«Инфозащита»

+7 (495) 786-34-93
sales@itprotect.ru
www.itprotect.ru

Календарь мероприятий 2017

1 июля
Санкт-Петербург • Конференция
Web Science Summer School
www.wwsss17.com

1 июля
Москва • Олимпиада
SIA 2017
www.impacthubmoscow.net

3 июля
Санкт-Петербург • Курс
Системный и бизнес-анализ в разработке ПО. Полный курс
Организатор: Центр IT-Образования Level UP
info@levelp.ru

5 июля
Санкт-Петербург • Конференция
PG Day Russia
www.pgday.ru

6 июля
Конференция
Про взаимодействие будущего. Онлайн-конференция
alexapost@gmail.com

6 июля
Вебинар
Автоматизация управления по целям и KPI
Организатор: ТопФактор
marketmbo@volga-soft.ru

8 июля
Москва • Курс
Интенсив по продвижению в Вконтакте
Организатор: MyAcademy
daria@myacademy.ru

9 июля
Санкт-Петербург • Турнир
Турнир по кикеру «IT´s KICKER #4»
Организатор: Айти-Событие
diana@it-dominanta.ru

13 июля
Тула • Турнир
Campus Party Russia
ronkov@bk.ru

15 июля
Одесса • Конференция
Конференция 8P 2017 + «Одессея»
Организатор: Netpeak
www.8p.ua

16 июля
Москва • Конференция
PYCON RUSSIA 2017
Организатор: it-people.ru
www.pycon.ru

27 июля
Вебинар
Ключи от бизнеса: Управление по KPI и BSC для собственников и топ-менеджеров
Организатор: ТопФактор
darma@topfactor.pro

28 июля
Минск • Конференция
B.E.E.R – ДЕНЬ СИСТЕМНОГО ИНЖЕНЕРА 2017
www.beer.itg.by

4 августа
Москва • Фестиваль
Музыкальный фестиваль IT SUMMER FEST
sales@incentiveclub.ru

5 сентября
Санкт-Петербург • Курс
Обучающий курс «IT-рекрутер»
Организатор: IT-Доминанта
irina@it-events.com

9 сентября
Санкт-Петербург • Турнир
Велотурнир «IT Bike Fest #4»
Организатор: Айти-Событие
denis@it-domianta.ru

12 сентября
Одесса • Мастер-класс
Виртуальная и дополненная реальность: что нового?
Организатор: HubHubhub
www.hubhubhub.com

15 сентября
Санкт-Петербург • Семинар
Занятие по программированию
Организатор: T.T.Консалтинг
inform@ttcsoft.ru

20 сентября
Санкт-Петербург • Конференция
AINL 2017
www.ainlconf.ru

22 сентября
Киев • Фестиваль
QA Fest 2017
info@qafest.com

22 сентября
Санкт-Петербург • Семинар
Занятие по ООП
Организатор: T.T.Консалтинг
inform@ttcsoft.ru

23 сентября
Новосибирск • Конференция
DevFest Siberia 2017
devfest@gdg-siberia.com

23 сентября
Санкт-Петербург • Турнир
Беговая эстафета «IT Run #2»
Организатор: Айти-Событие
diana@it-dominanta.ru

29 сентября
Санкт-Петербург • Курс
Занятие по LAMP
Организатор: T.T.Консалтинг
inform@ttcsoft.ru

2 октября
Санкт-Петербург • Курс
Занятие по продвижению сайтов
Организатор: T.T.Консалтинг
inform@ttcsoft.ru

12 октября
Красноярск • Выставка
itCOM – Информационные технологии Телекоммуникации – 2017
zeller@krasfair.ru

12 октября
Москва • Конференция
Большие данные в России: новые проекты
Организатор: CNews Conferences
an.sokolova@rbc.ru

14 октября
Санкт-Петербург • Турнир
Турнир по шахматам «IT Chess #4»
Организатор: Айти-Событие
diana@it-dominanta.ru

20 октября
Санкт-Петербург • Конференция
Научно-практическая конференция «Разработка ПО/SECR 2017»
Организатор: Интернет Хелп
pr@secr.ru

21 октября
Санкт-Петербург • Турнир
Турнир по мини-футболу «IT Goal #4»
Организатор: Айти-Событие
denis@it-dominanta.ru

3 ноября
Санкт-Петербург • Конференция
Piter Py #4 – Python-конференция на Неве
Организатор: Айти-Событие
diana@it-events.com

Лучшие в мире решения для информационной безопасности

Дистрибуция

Сертифицированные решения

Мобильные технологии

Канальное шифрование

TESSIS является официальным дистрибутором компаний Gemalto и CYREN, имеет статус Reseller у компании Blackberry и предлагает решения, обеспечивающие комплексную защиту и использующие технологии шифрования для защиты систем коммуникаций, программных разработок и контроля цифровой идентификации, а также решения для корпоративных и частных виртуальных сред.

TESSIS
TECHNOLOGIES, SYSTEMS AND SOLUTIONS FOR INFORMATION SECURITY

Научный проезд, 6, Москва
Тел.: +7 (495) 228-02-08
www.tessis.ru info@tessis.ru