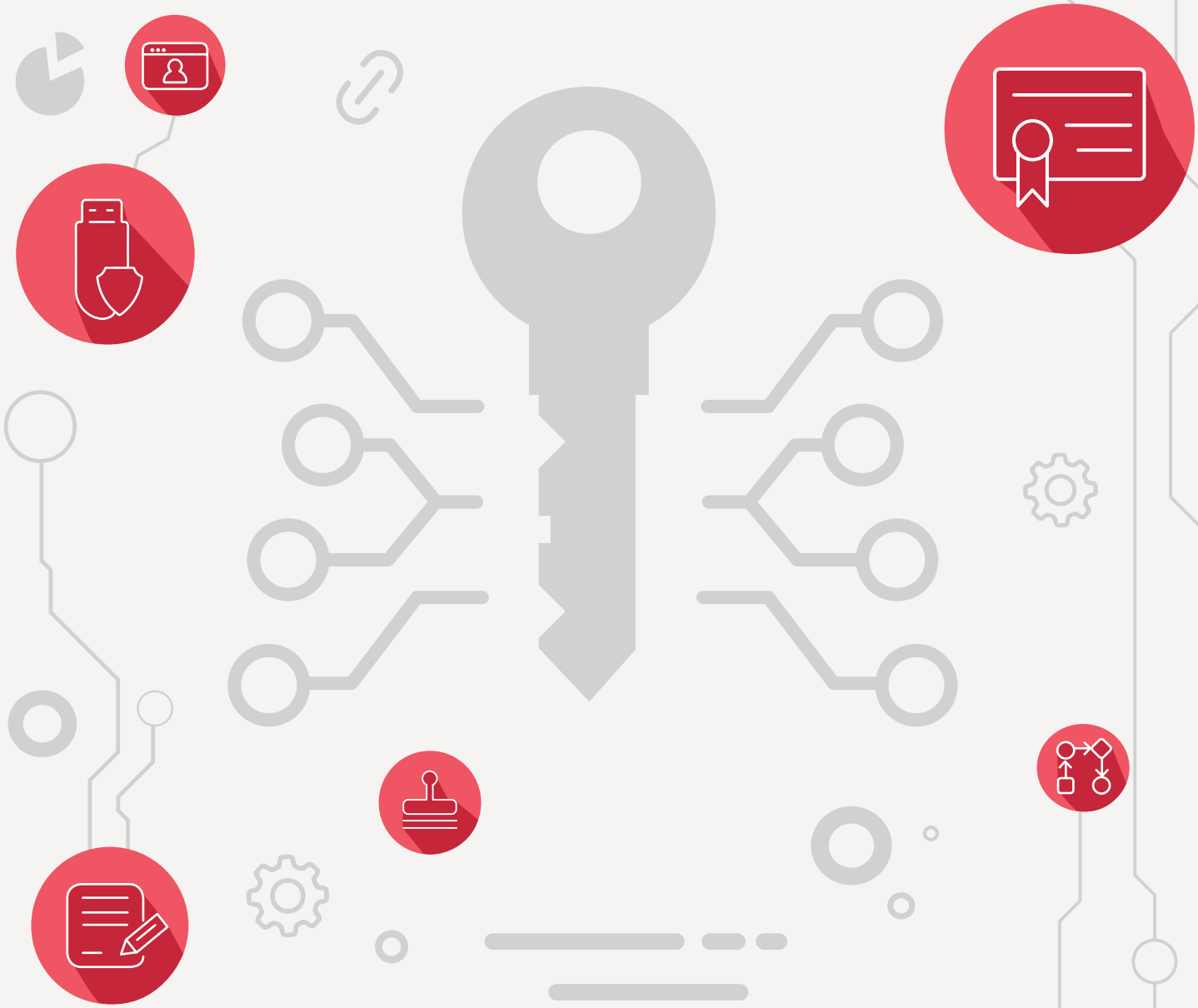
Avanpost PKI

Управление всеми элементами инфраструктуры открытых ключей из единого центра



Avanpost

Более
10 лет
опыта в ИБ

Более 100 партнеров
в России и странах СНГ

Более 2 000 000
пользователей

Более 80
успешных проектов

Avanpost PKI

Avanpost PKI — комплексная система централизованного управления всеми элементами инфраструктуры открытых ключей.

Разработанная в полном соответствии с требованиями законодательства Российской Федерации и регуляторов, система обеспечивает полную автоматизацию процессов управления жизненным циклом и учета сертификатов, ключевых носителей и средств криптографической защиты информации.

Для кого

Средние и крупные компании и холдинги

Кредитно-финансовые организации

Государственные учреждения, министерства и ведомства

РоссельхозБанк

Самый крупный проект

300 000 пользователей

Факты об эффективности

Более 500 сертификатов выпускается в день

Менее 30 секунд требуется на выпуск сертификата

В 3 раза сокращается нагрузка на УЦ

Avanpost PKI обеспечивает

Автоматизацию процесса учета и управления жизненным циклом сертификатов пользователей и информационных систем

Система сопровождает полный цикл работы с сертификатами от создания запроса как администратором, так и самим субъектом (пользователем, владельцем ИС) до выдачи готового для использования сертификата субъекту с поддержанием его в актуальном состоянии в дальнейшем (отслеживание срока действия, изменение данных и статуса субъекта сертификата).

Автоматизацию процесса учета и управления жизненным циклом ключевых носителей пользователей и информационных систем

Система сопровождает полный цикл работы с ключевыми носителями от первичного учета закупленных носителей с их возможной инициализацией до возврата от владельца с фиксацией всех действий, произведенных с ключевыми носителями. Это позволяет отследить полную историю изменений по любому учтенному в системе ключевому носителю и построить отчетные документы как по требованиям регуляторов, так и по внутренним требованиям безопасности.

Автоматизацию процесса учета и управления жизненным циклом СКЗИ и рабочих мест, на которых используются СКЗИ

Система сопровождает полный цикл работы с СКЗИ от первичного учета закупленных лицензий СКЗИ до возврата от владельца с фиксацией всех действий, произведенных с СКЗИ. Это позволяет отследить полную историю изменений по любому учтенному в системе СКЗИ и построить отчетные документы как по требованиям регуляторов, так и по внутренним требованиям безопасности. Система дает возможность в автоматическом режиме осуществлять инвентаризацию СКЗИ, установленных на АРМ, и контроль за средой функционирования СКЗИ.

Интерфейс самообслуживания пользователей для оперативного решения всех вопросов, связанных с сертификатами, ключевыми носителями и СКЗИ

Система предоставляет удобный личный кабинет пользователя, в котором он может запросить сертификат, оформить заявку на отзыв или перевыпуск сертификата, заказать ключевой носитель или лицензию на СКЗИ, разблокировать ключевой носитель и т.д.

Процессы согласования заявок по работе с сертификатами и СКЗИ

Движок бизнес-процессов позволяет настроить в системе полноценные процессы управления элементами инфраструктуры открытых ключей, например, передачу лицензий СКЗИ или токенов из центра в филиалы, согласование заявлений на выпуск сертификатов УКЭП с проверками заявлений в СМЭВ и сторонних системах. Система также поддерживает автоматический старт бизнес-процесса по какому-либо событию, например, старт процесса перевыпуска сертификата при приближении истечения срока его действия.

Возможности Avanpost PKI

Учет и управление жизненным циклом сертификатов и ключей пользователей и информационных систем:

- Генерация ключей и запросов на сертификаты с использованием как отечественных криптографических алгоритмов (ГОСТ), так и международных (RSA)
- Автоматический выпуск, отзыв, приостановка и возобновление действия сертификатов на удостоверяющих центрах (программных комплексах)
- Поддержка работы с удостоверяющими центрами в offline-режиме
- Импорт выпущенных ранее сертификатов в систему с целью их постановки на учет и контроля сроков действия
- Создания дубликатов ключей с последующим восстановлением на ключевом носителе или экспортом в PFX-файл
- Контроль срока действия сертификатов и закрытых ключей

Учет и управление жизненным циклом ключевых носителей пользователей и информационных систем:

- Учет ключевых носителей в единой базе данных системы
- Сбор информации обо всех ключевых носителях, подключенных к системе с использованием агентской подсистемы, и удаленное администрирование (форматирование, смена ПИН-кодов, блокировка, требование внеплановой смены ПИН-кода)
- Автоматическое ведение журналов действий с ключевыми носителями
- Управление политикой ПИН-кодов для ключевых носителей
- Разблокировка ключевого носителя пользователем из личного кабинета

Учет и управление жизненным циклом СКЗИ пользователей и информационных систем:

- Учет лицензий СКЗИ пользователей, информационных систем, автоматизированных рабочих мест (компьютеров)
- Автоматическое ведение журналов действий с лицензиями СКЗИ
- Дистрибуция СКЗИ в крупных территориально распределенных организациях — размещение дистрибутивов СКЗИ в системе и обеспечение доступа для скачивания дистрибутива с контролем легитимности

Учет автоматизированных рабочих мест:

- Учет автоматизированных рабочих мест (АРМ) и поддержка автоматической регистрации АРМ с использованием агентской подсистемы
- Наличие возможности первичного импорта перечня АРМ в систему
- Удаленная блокировка и разблокировка СКЗИ, установленного на АРМ

Подготовка отчетности о всех объектах учета в системе, в том числе и по требованиям регуляторов

Оповещение пользователей и администраторов о событиях в системе:

- Оповещения по e-mail
- Оповещения с использованием PUSH-уведомлений и агентской подсистемы (при отсутствии у пользователей доступа к электронной почте)

Полный аудит всех действий администраторов и пользователей системы:

- Аудит событий безопасности (входы в систему, попытки неуспешного входа, предоставление ролей пользователям, изменение состава ролей и т.д.)
- Аудит бизнес-событий в системе (создание запросов на сертификаты, создание заявок, смена ПИН-кодов на ключевом носителе и т.д.)
- Поддержка возможности отправки событий аудита во внешние информационные системы корреляции событий (по протоколу syslog)

Соответствие требованиям Федерального закона 63-ФЗ «Об электронной подписи»

Система интегрирована с сервисами СМЭВ и ЕСИА, проверяет данные запроса на сертификат для физического лица через сервисы МВД РФ и Пенсионного фонда России, а для юридического лица запрашивает и проверяет данные с использованием сервиса Федеральной налоговой службы РФ. Avanpost PKI ищет или регистрирует новый субъект в каталоге ЕСИА и публикует выпущенный для него сертификат.

Внутренняя модель субъектов

Модель организации каталога субъектов в системе является иерархической и представлена в виде центров регистрации и компаний. В качестве субъектов может выступать как пользователь (сотрудник, физическое лицо), так и информационная система (например, веб-сервер).

Avanpost PKI поддерживает механизмы эффективного разграничения доступа администраторов в рамках существующей иерархии, а также возможность учета владельцев информационных систем и организации бизнес-процессов, основанных на данной информации (например, подача заявления на выпуск или перевыпуск сертификата для информационной системы).

Каталог субъектов в системе может вестись как вручную, так и автоматизированно с использованием интеграционных решений с внешними системами - источниками через особый интерфейс адресной книги Avanpost PKI. Система поддерживает различные сценарии синхронизации, в том числе:

- Полную автоматическую загрузка данных
- Частичную загрузку данных (по решению администратора)
- Синхронизацию изменений

Управление бизнес-процессами и самообслуживание

Процесс выпуска сертификата включает не только действия администратора, но и подготовку соответствующего заявления пользователем. При этом данная заявка может потребовать дополнительного согласования, например, непосредственным руководителем или администратором безопасности. Наличие удобного сервиса самообслуживания, в котором пользователь сможет быстро составить запрос на выпуск сертификата, система подставить все необходимые данные пользователя, а согласующее лицо одобрить или отклонить его одним кликом мыши, позволит значительно повысить эффективность всего процесса.

Avanpost PKI предоставляет удобный личный кабинет пользователя, в котором он может запросить сертификат, оформить заявку на отзыв или перевыпуск сертификата, заказать ключевой носитель или лицензию на СКЗИ. Также данный сервис является единым центром управления всеми объектами пользователя, в том числе ключевыми носителями и сертификатами, и предоставляет соответствующую вспомогательную информацию (например, напоминания об окончании срока действия сертификата), позволяет разблокировать собственный ключевой носитель или получить от него ПИН-код.

Возможность подачи заявок как из личного кабинета работника так и администратором:

- На выпуск новых сертификатов
- На отзыв и перевыпуск сертификатов
- На получение ключевых носителей
- На получение и возврат СКЗИ

Возможность конструирования бизнес-процессов обработки и согласования заявок с использованием графического редактора бизнес-процессов, основанного на модели BPMN:

- Поддержка этапов простого и параллельного согласования
- Поддержка корректировки заявок и дополнительного согласования
- Поддержка взаимодействия с внешними системами и сервисами в рамках исполнения бизнес-процесса (внешние системы документооборота, СМЭВ и ЕСИА и т.д.)
- Поддержка сложных действий, таких как взаимодействие с ключевыми носителями и удостоверяющими центрами в рамках исполнения бизнес-процессов

Возможность автоматического старта бизнес-процесса на основании событий, происходящих в системе:

- Перевыпуск сертификата при истечении его срока действия
- Отзыв сертификатов и открепления объектов от уволенных работников
- Перевыпуск сертификатов при изменении данных работника и т.д.

Поддержка юридической значимости электронного документооборота с использованием электронной подписи при создании и согласовании заявок

Бизнес-кейсы

ЕГР ЗАГС

20 000 пользователей

8 месяцев

Задача: Организовать первичный выпуск подготовленных носителей, своевременный перевыпуск сертификатов и обновление профилей VDI на смарт-картах пользователям ЕГР ЗАГС.

Решение: В данном проекте было две значительные особенности. Первая — инфраструктура ЕГР ЗАГС построена на открытых решениях, соответственно, требовалась поддержка рабочих станций на базе Linux. Вторая — для работы пользователя в ПАК требуется носитель (смарт-карта ESMART), содержащий три сертификата и один объект в закрытой области памяти — профиль доступа к VDI. Для поддержки инфраструктуры был разработан PKI-агент для ОС Linux, который дает возможность управлять смарт-картой, подключенной на рабочем месте пользователя.

Avanpost PKI была интегрирована с УЦ КриптоПро 2.0, а новый плагин публикации помог создать унифицированный механизм информирования инфраструктуры ЕГР ЗАГС об изменениях сертификатов пользователей.

Задача упрощения выпуска карты с необходимыми объектами была решена путем ввода новой сущности — приложения, которое агрегирует в себе требования информационной системы или ПАК к носителю. Запрос приложения позволяет одновременно сформировать запросы на объекты и сертификаты, необходимые для работы в этом приложении.

Выполненные доработки и настройки позволили не только уложиться в жесткий график первичного выпуска носителей, но и сократить трудозатраты операторов как минимум в 12 раз по сравнению с использованием стандартных интерфейсов УЦ, PKI-клиента и VDI для подготовки и регистрации носителя. Перевыпуск носителей спустя год использования был произведен абсолютно прозрачно для пользователей: без сбора носителей, участия и какого-либо вовлечения в процесс.

МегаФон

20 000 пользователей

1 год

Задача: Автоматизировать деятельность УЦ и сократить издержки на выпуск сертификатов и учет основных объектов инфраструктуры PKI.

Решение: Avanpost PKI обеспечивает учет всех объектов инфраструктуры открытых ключей: ключевые носители, лицензии на СКЗИ, АРМ-ы. В соответствии с требованиями ФСБ в системе автоматизирована печать всех отчетных документов по этим объектам. Система поддерживает все процессы, связанные с выпуском сертификатов электронной подписи (ЭП) для сотрудников компании.

В личном кабинете любой сотрудник может самостоятельно заказать себе сертификат ЭП, сформировать необходимые сопроводительные документы и просматривать характеристики всех выпущенных для него сертификатов. Для операторов УЦ также предусмотрен эргономичный пользовательский интерфейс — единое окно, где собран весь комплекс инструментов рассмотрения поступающих запросов пользователей и вся необходимая информация для принятия решений: заявления, сканы документов, параметры запросов и т.д.

В систему встроены различные механизмы автоматизации, резко сократившие объем ручной работы, задержки и технические ошибки. Один из таких механизмов позволяет получать доверенные данные о сотрудниках компаний непосредственно из кадровой системы организации, исключая саму возможность появления и дальнейшей обработки недостоверной информации. Другой механизм обеспечивает автоматическую публикацию выпущенных пользовательских сертификатов во всех информационных системах (ИС) компании, где эти сертификаты используются.

В рамках проекта создан базис системы сбора и аналитической обработки данных, которая уже сегодня позволяет объективно оценивать эффективность работы сотрудников УЦ, а также проводить всесторонний анализ случаев нарушения параметров SLA.

ГАЗПРОМБАНК

20 000 пользователей

1, 5 года

Задача: Автоматизировать деятельность УЦ Департамента защиты информации в рамках обеспечения глобальной задачи модернизации инфраструктуры и сокращения временных издержек и трудозатрат на типовые процессы обеспечения работников сертификатами для доступа к сетевой инфраструктуре (двухфакторная аутентификация) и для использования возможностей шифрования и электронной подписи в корпоративной электронной почте.

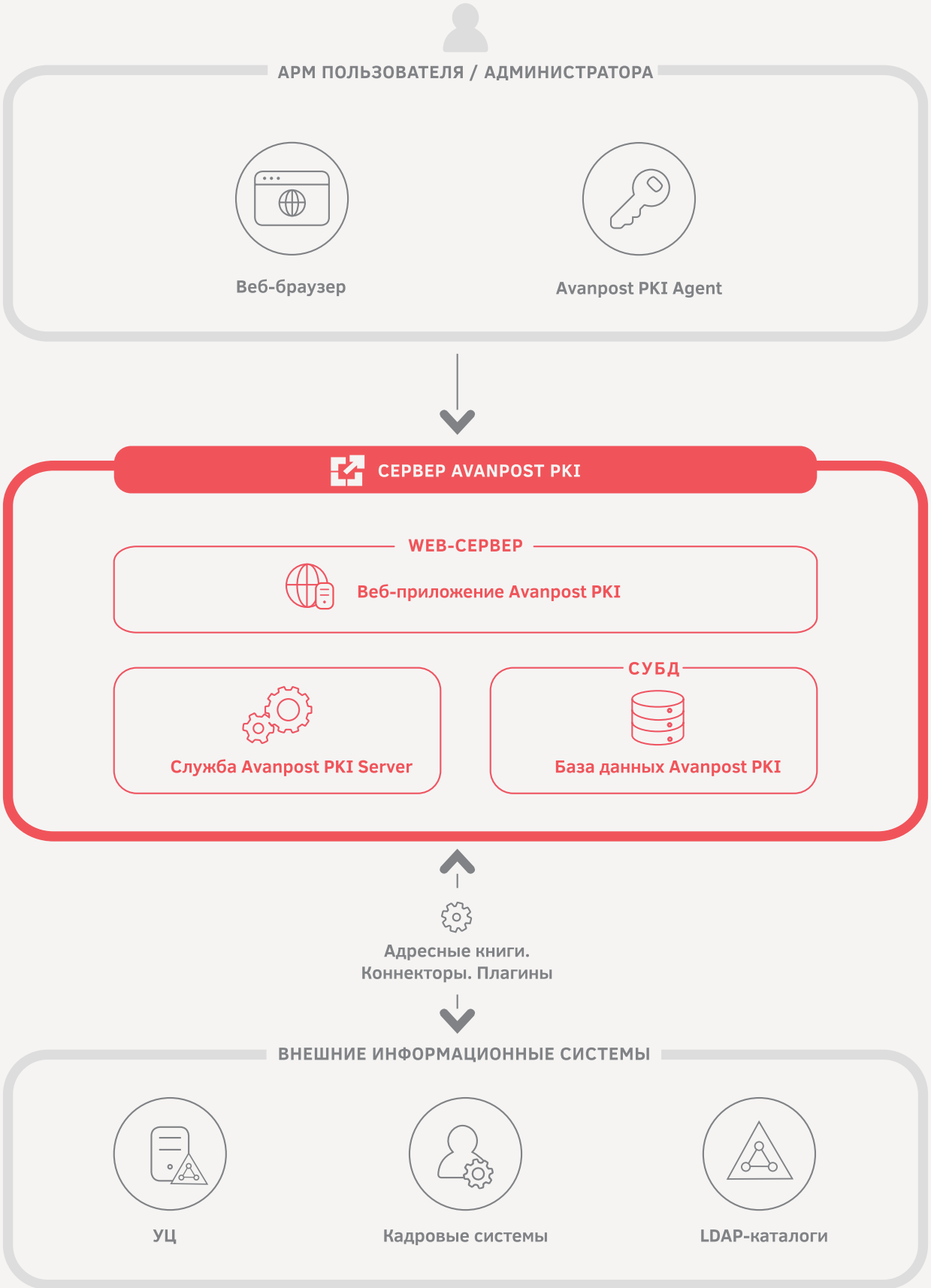
Решение: Комплексная система управления инфраструктурой открытых ключей, созданная на основе Avanpost PKI 6, позволила не только эффективно решить первичную задачу по учету ключевых носителей и сертификатов работников, контролю своевременной смены пин-кодов пользователями, но и выстроить и автоматизировать процессы выдачи и перевыпуска сертификатов в рамках обеспечения процессов приема на работу, переводов, изменения данных работников и т.д.

Технологии работы с реестрами ОС и удаленной работы с ключевыми носителями с использованием агентской подсистемы дали возможность автоматизировать ряд процессов банка и оперативно решать задачи, обусловленные сложившейся в мире эпидемиологической ситуацией. Например, по факту приема на работу система автоматически создает заявку на выпуск для нового работника базового набора сертификатов, которые могут быть оперативно установлены.

С использованием функционала продукта были реализованы и процессы контроля выданных сертификатов и ключевых носителей. Для временного использования были созданы жесткие правила, контролирующие выдачу строго на один рабочий день, по истечении которого пропуск автоматически открепляется от работника, а временные сертификаты отзываются.

Автоматизация типовых процессов с появлением нового инструмента управления инфраструктурой открытых ключей позволила банку эффективно решить как текущие задачи, так и заложить потенциал для дальнейшего развития и автоматизации процессов, не увеличив при этом численность персонала УЦ ДЗИ.

Архитектура системы



Компоненты системы

Служба Avanpost PKI Server реализует бизнес-логику системы, логику обработки запросов и электронных заявок, управления жизненным циклом субъектов и объектов. Содержит подсистему адресных книг, коннекторов и плагинов для взаимодействия с УЦ и внешними информационными системами

Веб-приложение Avanpost PKI предоставляет веб-интерфейс администраторам и пользователям системы в части настройки и управления, личный кабинет в части самообслуживания

Avanpost PKI Agent — программный компонент, работающий в фоновом режиме на АРМ пользователя/администратора и реализующий взаимодействие с ключевыми носителями и криптографическими провайдерами

База данных Avanpost PKI является хранилищем всех данных системы

Адресные книги, коннекторы, плагины — модули сопряжения Avanpost PKI с различными внешними информационными системами: УЦ, источниками данных о субъектах, потребителями информации о выпускаемых сертификатах.

Возможности интеграции

На сегодняшний день Avanpost PKI располагает самым широким набором возможностей для интеграции по следующим направлениям:

Интеграция с удостоверяющими центрами предназначена для решения задач управления сертификатами (выпуск, отзыв и т.д.) на программных комплексах удостоверяющих центров

Интеграция с ключевыми носителями предназначена для решения задач управления ключевыми носителями (создание запросов на сертификаты, установка сертификатов и ключей, смена ПИН-кодов, разблокировка и т.д.)

Интеграция с источниками данных о субъектах предназначена для решения задач автоматической загрузки и синхронизации данных о субъектах из внешних доверенных систем-источников (кадровые системы, каталоги и т.д.)

Интеграция с внешними системами – потребителями информации о выпущенных сертификатах предназначена для решения задач публикации информации о выпущенных сертификатах для нужд внешних информационных систем (системы электронного документооборота, LDAP-каталоги и т.д.)

Особые виды интеграций — интеграции, реализованные для решения более узких задач, к которым можно отнести:

- Интеграцию с сервисами СМЭВ
- Интеграцию с системами ДБО
- Интеграцию с системами обучения и тестирования

Интеграция с удостоверяющими центрами

Интеграция с УЦ обеспечивается коннектором Avanpost PKI, который представляет собой программный модуль, реализующий интерфейс ICA Avanpost PKI.

Он служит для обеспечения взаимодействия Avanpost PKI Server с программными компонентами УЦ с целью управления жизненным циклом сертификатов (выпуск, отзыв, приостановка и возобновление деятельности сертификата)

В Avanpost PKI имеются готовые коннекторы к следующим УЦ:

- Microsoft CA
- ПАК КриптоПро УЦ 1.5, 2.0
- CheckPoint ICA
- ПК VipNet УЦ
- ПАК УЦ Notary-PRO v. 2.2 и выше
- АПК Валидата УЦ
- GlobalSign

Интеграция с ключевыми носителями

Интеграция с ключевыми носителями в основном реализуется с использованием агентской подсистемы Avanpost PKI (за исключением «облачных» ключевых носителей) и подразумевает реализацию следующих функций (в зависимости от наличия поддержки у производителей ключевых носителей):

- Форматирование
- Генерация ключей и создание запросов на сертификаты
- Установка сертификатов и ключей (восстановление)
- Смена ПИН-кодов
- Удаление сертификатов и ключей
- Разблокировка
- Запись и обновление объектов

Avanpost PKI поддерживает работу со следующими аппаратными и программными ключевыми носителями:

- eToken
- RuToken
- ESMART
- JaCarta
- YubiKey
- KAZTOKEN
- СберТокен
- «Облачные»: КриптоПро HSM и КриптоПро DSS
- USB флэш-накопители
- Реестр ОС Windows

Интеграция с источниками данных о субъектах

Интеграция с источниками данных о субъектах обеспечивается адресной книгой Avanpost PKI, которая представляет собой подключаемую библиотеку, реализующую программный интерфейс IPersonAddressBook Avanpost PKI. Она служит для обеспечения взаимодействия Avanpost PKI Server с внешней системой – источником данных о субъектах сертификатов (сотрудниках).

В качестве систем-источников данных Avanpost PKI поддерживает все самые распространенные LDAP-каталоги и кадровые системы:

- MS Active Directory, OpenLDAP, FreeIPA и т.д.
- Системы на базе платформы 1С
- SAP HR
- Oracle HR и многие другие

Интеграция с внешними системами – потребителями информации о выпущенных сертификатах

Интеграция с внешними системами – потребителями информации о выпущенных сертификатах обеспечивается плагином публикации Avanpost PKI, который представляет собой подключаемую библиотеку, реализующую программный интерфейс ICertificatePublisher Avanpost PKI. Он служит для обеспечения взаимодействия Avanpost PKI Server с внешними информационными системами с целью публикации информации о выпущенных сертификатах. Основные функции плагина публикации — это передача во внешнюю ИС информации о выпущенном сертификате и о необходимости удаления (деактивации) сертификата.

Avanpost PKI имеет готовые плагины публикации к таким системам, как:

- LDAP-каталоги — MS Active Directory, OpenLDAP, FreeIPA и т.д.
- «Шины» — IBM MQ, RabbitMQ
- ЕСИА
- Файловая система и многие другие

Интеграция с сервисами СМЭВ

Avanpost PKI поддерживает интеграцию с сервисами Системы межведомственного электронного взаимодействия (СМЭВ 3) в части покрытия требований 63 ФЗ из коробки и обеспечивает следующие возможности:

- Проверка данных о соответствии СНИЛС, ФИО и даты рождения заявителя (по данным заявки и/или запроса на сертификат) в сервисах ПФР
- Получение выписки в электронном виде из ЕГРЮЛ/ЕГРИП с использованием сервисов ФНС

- Проверка паспортных данных заявителя (по данным заявки и/или запроса на сертификат) в сервисах МВД

- Публикация выпущенного квалифицированного сертификата в ЕСИА и возможность регистрации подтвержденной учетной записи по требованию заявителя

- Хранение результатов обращений к сервисам СМЭВ в системе (в виде электронных ответов с электронной подписью ведомств) для обеспечения возможности разбора конфликтных ситуаций

Интеграция с системами ДБО

Задачей интеграции с системами ДБО и АБС является обеспечение возможности выпуска сертификата для клиента банка по запросу, сформированному клиентом в системе дистанционного банковского обслуживания. В рамках обеспечения данного процесса Avanpost PKI поддерживает:

- Импорт сведений о клиентах банка

- Импорт запросов на сертификаты, дальнейшее рассмотрение и выпуск сертификатов

- Экспорт выпущенных сертификатов для систем ДБО

Особенностью реализации подобных процессов с использованием Avanpost PKI является автоматическое выполнение операций по учету ключевых носителей, СКЗИ, сопроводительных документов и т.д. в рамках обеспечения процесса. Avanpost PKI имеет наработки по интеграции со всеми популярными системами ДБО:

- Банк-Клиент (BS-Client)

- Telebank (StepUp)

- ЦФТ Банк (IBSO) и другие

Интеграция с системами обучения и тестирования

Avanpost PKI может быть интегрирован с внешней системой обучения и тестирования с целью контроля за прохождением работниками обучения по использованию средств криптографической защиты информации. В рамках подобной интеграции могут быть реализованы такие процессы, как контроль и обновлении информации о своевременном прохождении работниками обучения и запуск соответствующих бизнес-процессов в случае непрохождения, например, блокировки СКЗИ на рабочем месте до прохождения обучения.

Avanpost PKI поддерживает интеграцию с системой WebTutor.

О компании Аванпост

Аванпост — ведущий российский разработчик систем идентификации и управления доступом. Компания работает на рынке информационной безопасности с 2007 года и к настоящему моменту является технологическим лидером в сегменте Identity Management.

Наши решения

Avanpost IDM

система централизованного управления доступом к корпоративным ресурсам организации

Avanpost FAM

система единой аутентификации сотрудников в корпоративных ресурсах организации

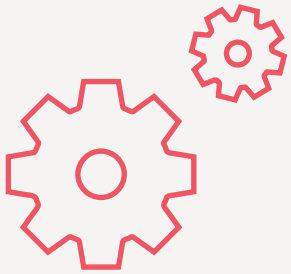
Avanpost PKI

система управления всеми элементами PKI-инфраструктуры из единого центра

Avanpost Web SSO

система единой аутентификации клиентов в порталах и внешних приложениях

Нам доверяют



109129, Россия, Москва,
ул. 8-я Текстильщиков, д. 11, стр. 2

+7 (495) 641-80-80

info@avanpost.ru

www.avanpost.ru