INFOTECH
secure identity and payments

X Infotech Government

Решения PKI (инфраструктуры открытых ключей)

- X Infotech Country Signing Certification Authority (CSCA)
- X Infotech Document Signer (DS)
- X Infotech Country Verifying Certification Authority (CVCA)
- X Infotech Document Verifier (DV)
- X Infotech Terminal Control Center (TCC)
- X Infotech Single Point of Contact (SPOC)
- X Infotech National Public Key Directory (nPKD)

INFOTECH
secure identity and payments

Термины и определения

Инфраструктура открытых ключей (PKI)- совокупность стратегий, процессов и технологий, используемых для верификации, регистрации и сертификации пользователей приложений защиты. В PKI для защиты связи используются криптография открытого ключа и практика сертификации ключа

BAC (Basic Access Control - базовый контроль доступа) – это механизм, благодаря которому только полномочные участники могут считывать персональную информацию из паспортов с чипом RFID (радиочастотной идентификации) по беспроводной связи. Этот механизм позволяет системе управления чипом убедиться, что документ открыт для проверки. Уязвимые (например, биометрические) данные держателя документа не защищаются.

EAC (Extended Access Control - расширенный контроль доступа) – это набор расширенных функций безопасности электронных паспортов, которые защищают и ограничивают доступ к уязвимым (например, биометрическим) персональным данным, содержащимся в чипе RFID.
Эти функции позволяют чипу убедиться, что система проверки (Inspection System (IS)) имеет полномочия считывать уязвимые данные.

ICAO (International Civil Aviation Organization - международная организация гражданской авиации) – это специализированное учреждение ООН.
ICAO занимается стандартизацией паспортов, пригодных для автоматического распознавания, по всему миру. Документ 9303 содержит действующие технические условия ICAO для машиносчитываемых паспортов, виз и идентификационных карт (“дорожные документы”), используемых при пересечении границ.

Технические нормы BSI точно определяют механизмы защиты для электронных машиносчитываемых дорожных документов (eMRTD). Эти нормы являются техническим базисом для европейских электронных паспортов и электронных водительских удостоверений и приводятся в Техническом отчете 03110, составленном федеральным ведомством по информационной безопасности, BSI.

Решения PKI от компании X Infotech

Решения PKI компании X Infotech являются элементами инфраструктуры , способствующими усилению безопасности при изготовлении и проверке электронных идентификационных документов на границах, обеспечивая удобную интеграцию с различными сторонними компонентами и системами. Решения с легкостью адаптируются к существующим или будущим изменениям в бизнесе.

X Infotech предоставляет полный надежный спектр решений EAC-PKI, необходимых для того, чтобы выпуск и проверка электронных паспортов или идентификационных документов соответствовали нормам ICAO.

Процесс инфраструктуры PKI можно логически разделить на следующие этапы:
1. Изготовление документа
2. Проверка личности и документов
3. Межгосударственное управление сертификатами

Для безопасного изготовления и проверки электронных паспортов требуется надежная инфраструктура открытых ключей. Для производства документов решение включает в себя следующие модули: Document Signer (DS), Country Signing Certification Authority (CSCA) and Country Verifying Certification Authority (CVCA). Другие компоненты инфраструктуры PKI, Document Verifier (DV) и Terminal Control centre (TCC), позволяют создавать безопасную среду для доступа к данным документа в режиме EAC (расширенного контроля доступа) (например, считывание отпечатков пальцев из электронного паспорта или идентификационного документа во время проверки подлинности на границе). В целях обеспечения межгосударственного управления сертификатами используются компоненты National Public Key Directory (nPKD) и Single Point of Contact (SPOC).

Изготовление документа

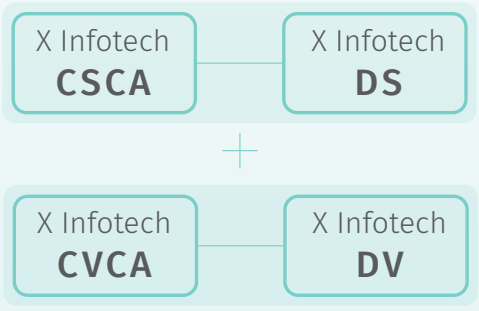
Компоненты PKI, поставляемые компанией X Infotech, создают надежную среду для производства электронных паспортов и идентификационных документов в соответствии с нормами ICAO с возможностью EAC (расширенного контроля доступа) для защиты индивидуальной биометрической информации, хранимой в чипе. Document Signer подписывает документы с сертификатами, выпущенными CSCA – корневым сертификационным центром проверки подлинности документов. CSCA выпускает сертификаты Document Signer и передает Document Signer полномочия на подписание документа. В чипе электронного паспорта также хранится сертификат Country Verifying Certification Authority (CVCA), который используется для подтверждения подлинности на терминале.

Базовый уровень защиты (базовый контроль доступа,BAC) разрешает доступ и чтение открытых данных авторизованным субъектам.

Среда BAC
(базовый контроль доступа)

Расширенный уровень защиты (расширенный контроль доступа, EAC) разрешает субъектам доступ и чтение уязвимых данных, включая биометрические (отпечатки пальцев, сканирование радужной оболочки и т.д.)

Среда EAC
(расширенный контроль доступа)

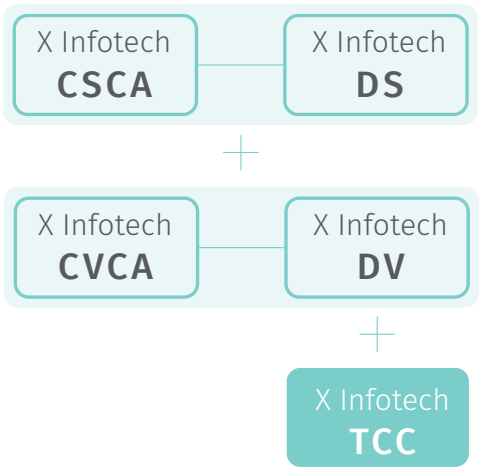


INFOTECH
secure identity and payments

Проверка подлинности документа

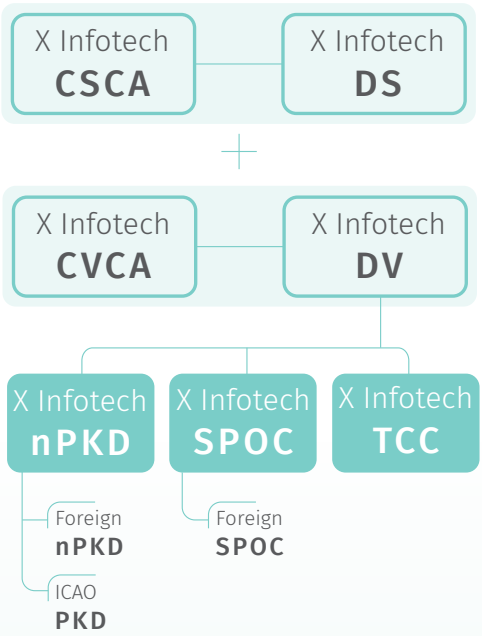
ICAO PKD - это центральная платформа для управления глобальным обменом сертификатами и списками отзыва сертификатов. Эти сертификаты и списки отзыва сертификатов используются для проверки электронной подписи данных, которые содержатся в чипе RFID электронных паспортов и других машиносчитываемых дорожных документов.
Во время проверки документа система проверки (IS) отправляет сертификат, предоставленный Document Verifier (DV), в чип электронного паспорта. Это позволяет чипу проверить сертификат системы IS. Чтобы удостовериться, что сертификат, отправленный IS, подлинный, чип отправляет в систему IS случайное число. Число подписывается системой проверки и возвращается в чип, после чего чип проверяет число. Если все шаги успешно пройдены, электронный паспорт открывает доступ к данным, защищенным базовым контролем доступа EAC.

Проверка подлинности документа



Inter-country Certificate Management

Компонент nPKD устанавливает надежную инфраструктуру для межгосударственного управления сертификатами для электронных паспортов и идентификационных документов. Каталог сертификатов nPKD связывается с ICAO PKD, затем собирает, хранит сертификаты CSCA и DS и списки отзыва сертификатов из стран по всему миру. nPKD распределяет эти сертификаты по терминалам проверки документов, где подтверждается подлинность документов, выпущенных местными органами или другими странами.
SPOC устанавливает надежную инфраструктуру в междугосударственном управлении сертификатами для электронных паспортов и идентификационных документов. SPOC упрощает обмен между местным DV и иностранным DV. При этом он разрешает доступ к биометрическим данным, соответствующим нормам ICAO, для проверки подлинности на терминалах (требуется для доступа к документу в режиме EAC) в пограничных пунктах и для других устройств проверки подлинности биометрических данных.



Условия и определения

Пассивная проверка подлинности – это протокол BAC (базового контроля доступа), разработанный для борьбы с изготовлением фальшивых документов и махинациями. Система проверки считывает MRZ-код и электронную подпись документа, чтобы убедиться, что данные чипа подлинные и не изменялись.

Проверка подлинности на терминале – это протокол EAC (расширенного контроля доступа), который используется для того, чтобы определить, разрешается ли системе проверки (IS) считывать уязвимые данные из электронного паспорта. Механизм основан на цифровых сертификатах, имеющих формат card verifiable certificates (CVC - сертификат проверяемой карты).

Система проверки (IS) – это одно или группа электронных устройств, предназначенных для проверки подлинности документа (например, устройства считывания и сканеры электронных паспортов/идентификационных документов, eGates и т.д.)

HSM (Hardware Security Module - аппаратный модуль безопасности) представляет собой электронное устройство, которое хранит цифровые ключи и управляет ими для проверки подлинности, а также обеспечивает криптографическую обработку.

INFOTECH
secure identity and payments

Описание решений PKI от компании X Infotech

X Infotech CSCA

X Infotech Country Signing Certification Authority (CSCA) устанавливает государственный пункт доверия PKI в отношении электронных документов. CSCA выпускает сертификаты открытого ключа для одного или более Document Signer и, опционально, для других субъектов, таких как Master List Signers. CSCA хранит закрытые ключи в криптографическом устройстве HSM и работает в оффлайн-среде, хорошо защищенной от любого неправомочного доступа или доступа извне.

Особенности:
- Сертификаты CSCA и профили ключей в соответствии с техническими условиями ICAO 9303
- Создание и защита пар ключей криптографичесими устройствами HSM
- Графический интерфейс пользователя для конфигурирования, управления и отслеживания
- Поддерживает несколько CSCA, посвященных различным типам документов
- Универсальные методы управления доступом пользователей (m-из-n)

X Infotech DS

X Infotech Document Signer (DS) является компонентом решения PKI, который ставит цифровую подпись в электронных документах. Цифровая подпись DS гарантирует целостность и подлинность документа. В свою очередь она проверяется при помощи сертификата CSCA во время пассивной проверки подлинности, чтобы подтвердить правильность данных чипа.

Особенности:
- Сертификаты и профили ключей DS полностью соответствуют техническим условиям ICAO 9303
- Создание и защита пар ключей криптографическими устройствами HSM
- Графический интерфейс пользователя для конфигурирования, управления и отслеживания
- Интеграция с решением для персонализации с целью упрощения и снижения стоимости

X Infotech CVCA

X Infotech Country Verifying Certification Authority (CVCA) является государственным пунктом доверия PKI , который дает местным и иностранным Document Verifiers (DVs) доступ к уязвимым данным электронных документов таким как отпечатки пальцев или биометрия радужной оболочки, защищенным расширенным контролем доступа (EAC).

CVCA хранит частные ключи в криптографическом устройстве HSM и работает в оффлайн-среде, хорошо защищенной от любого неправомочного доступа или доступа извне.

Особенности:
- Сертификаты и профили ключей CVCA полностью соответствуют техническим указаниям BSI TR03110
- Создание и защита пар ключей криптографическими устройствами HSM
- Графический интерфейс пользователя для конфигурирования, управления и отслеживания
- Универсальные методы управления доступом пользователей (m-из-n)

X Infotech DV

X Infotech Document Verifier (DV) является компонентом решения PKI , который определяет, какая из систем проверки (IS) получит право считывать из электронных документов с защитой расширенного контроля доступа (EAC) уязвимые данные, такие как отпечатки пальцев или биометрия радужной оболочки.

Document Verifier (DV) запрашивает и получает сертификаты DV от CVCA каждой страны, к электронным документам которой DV имеет право доступа.

DV выпускает сертификаты системы проверки в ответ на запросы сертификатов от систем проверки. Эти сертификаты дают системе проверки право доступа к защищенным уязвимым данным, которые находятся в чипах электронных документов.

Особенности:
- Сертификаты и профили ключей DV соответствуют требованиям BSI-EAC и BSI TR-03139
- Работает в соответствии с протоколами BSI TR-03129
- Создание и защита пар ключей криптографическими устройствами HSM
- Графический интерфейс пользователя для конфигурирования, управления и отслеживания

INFOTECH
secure identity and payments

X Infotech TCC

Решение X Infotech Terminal Control Centre (TCC) автоматизирует проверку подлинности национальных и иностранных машиночитаемых дорожных документов (MRTD) как ручными, так и полностью автоматизированными системами проверки при пограничном контроле.

TCC обеспечивает Document Terminal Authentication (TA) (проверку подлинности на терминале) - сервис, который дает системам проверки доступ к уязвимым персональным данным (отпечатки пальцев, радужная оболочка) в чипе документа и использовать усовершенствованные механизмы биометрической проверки. Механизм основан на интеграции с Document Verification (системой проверки подлинности документов) (DV), которая выпускает сертификаты CVC (card verifiable certificates) , действующие в течение короткого периода времени, обычно от 1 дня до 1 месяца.

Кроме того, решение TCC осуществляет сервис пассивной проверки подлинности документов посредством сравнения сертификата документа с сертификатами, полученными от ICAO PKD или National PKD. Решение соответствует стандартам и директивам ICAO и BSI и обеспечивает удобную интеграцию со сторонними системами. Поддерживает централизованное внедрение, когда один TCC действует как центральный пункт распределения сертификатов по всей стране или когда экземпляры TCC децентрализованы и размещаются в удаленных пунктах, таких как аэропорты, морские порты или пограничный контроль.

X Infotech SPOC

X Infotech Single Point of Contact (SPOC) управляет обменом сертификатами CVCA между различными странами с целью обеспечения доступа к уязвимым биометрическим данным в документах EAC, соответствующих требованиям ICAO, в пунктах пограничного контроля.

Архитектура расширенного контроля доступа (EAC) PKI в настоящее время является самым современным стандартом безопасности дорожных документов.

SPOC реализует управление международными стандартами, протоколами и сертификатами для электронных паспортов EAC с целью обмена сертификатами Document Verifying (проверки подлинности) (DV) между странами. Решение соответствует стандартам и директивам ICAO и BSI и обеспечивает простоту использования и интеграции со сторонними системами.

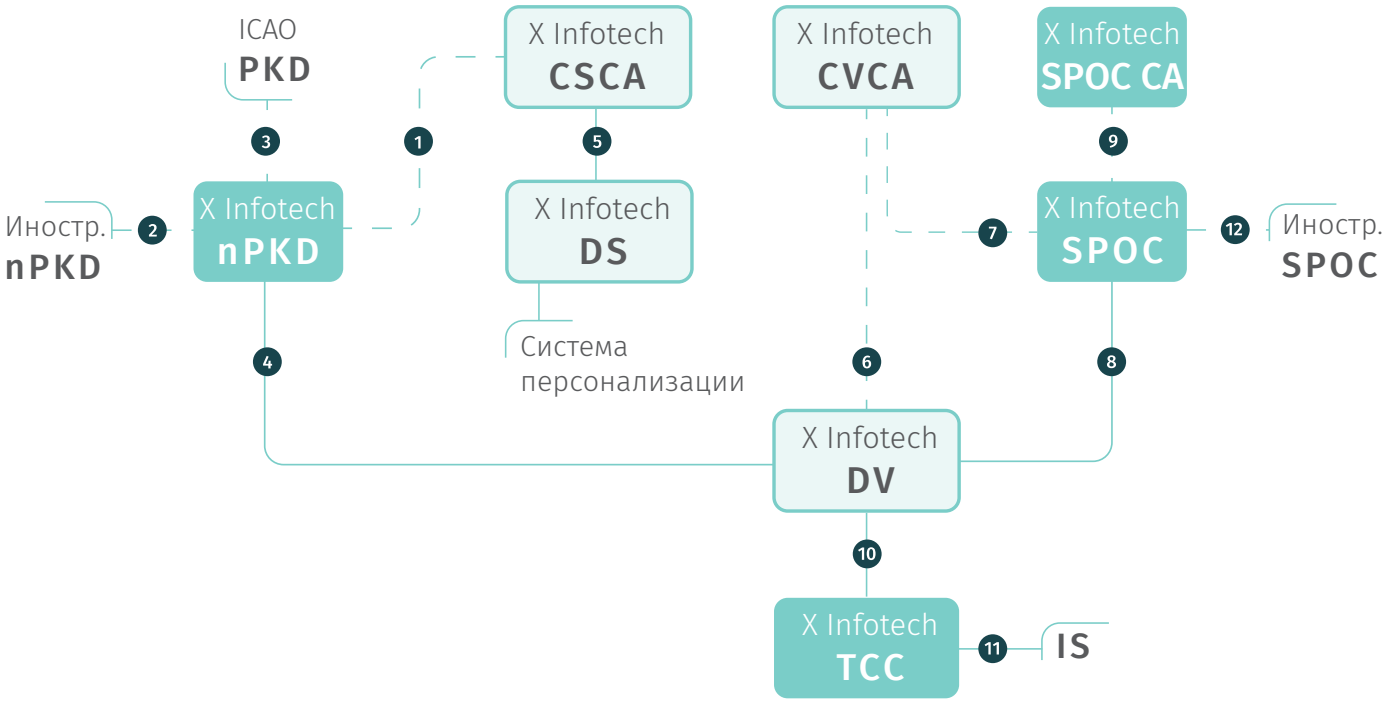
Особенности:
- Онлайн- и ручная интеграция с системами PKI Document Verifier (DV) для управления сертификатами DV.
- Интеграция с системами PKI Country Verifying Certification Authority (CVCA) для подписывания сертификатов DV.
- Полная встроенная интеграция с продуктами X Infotech
- Онлайн-связь с иностранными системами SPOC для обмена данными
- Интерфейс с иностранной системой SPOC защищается сертификатом SPOC CA
- TLS-защита для системных интерфейсов
- Соответствие международным стандартам BSI TR-03129, ICOA 9303 и CSN 36 9791:2009
- Контроль доступа через профили пользователей (оператор, администратор, аудитор, регистрирующий орган)
- Ведение контрольных журналов для системных событий.

X Infotech nPKD

X Infotech National Public Key Directory (nPKD) является компонентом решения PKI, который управляет сертификатами PKI электронных документов на государственном уровне.
Действует как центральный посредник для управления обменом сертификатами PKI документа и списками отзыва сертификатов на национальном уровне. Создает централизованную базу данных сертификатов, полученных из многих источников, таких как Country Signing Cerification Authority (CSCA), ICAO PKD и иностранные системы nPKD.

INFOTECH
secure identity and payments

Последовательность операций для решений PKI компании X Infotech



1. nPKD связывается интерфейсом с CSCA для подписания сертификата Master List signing, а также для получения сертификатов DS и CSCA. Обмен данными выполняется в ручном режиме.
2. nPKD связывается с иностранным nPKD для получения сертификатов, выпущенных не ICAO PKD DS и CSCA. Обмен данными выполняется в ручном режиме.
3. nPKD связывается с ICAO PKD, чтобы получить файлы ICAO PKD Files и отправить сертификаты в ICAO PKD.
4. DV связывается с nPKD, чтобы получить сертификаты для пассивной проверки подлинности.
5. DS связывается с CSCA, чтобы подписать сертификаты DS. Обмен данными выполняется в ручном режиме.
6. DVCA связывается с CVCA, чтобы подписать сертификаты DV. Обмен данными выполняется в ручном режиме.
7. SPOC связывается с CVCA, чтобы подписать DV и другие запросы на сертификаты, отправленные и полученные от иностранного SPOC
8 DV связывается с SPOC, чтобы получить подписанные сертификаты DV.
9. SPOC связывается с SPOC CA, чтобы получить сертификат, который защищает SPOC, а также связывается с иностранным SPOC. Обмен данными выполняется в ручном режиме.
10. TCC связывется с DV, чтобы подписать сертификаты системы проверки IS, требуемые для Terminal Authentication (проверки подлинности на терминале) (TA). Таким образом, TCC также получает сертификаты для пассивной проверки подлинности.
11. IS связывается с TCC, чтобы осуществлять пассивную проверку подлинности и проверку подлинности на терминале.
12. SPOC связывается с иностранным SPOC, чтобы отправять/получать сообщения и сертификаты.