
Рекомендации по обеспечению информационной безопасности при работе с мобильными решениями

В документе описаны механизмы защиты информации, используемые в мобильных решениях к системе Directum RX.

Согласно ГОСТу Р50922-2006 «Защита информации», информация считается защищенной при условии обеспечения ее конфиденциальности, доступности и целостности. В системе Directum RX это достигается с помощью использования программно-технических средств:

- управление доступом: идентификация пользователей в системе и контроль прав доступа;
- регистрация и учет данных: логирование и ведение истории работы с объектами;
- криптография: подписание ЭП.

Содержание

Рекомендации по обеспечению информационной безопасности при работе с мобильными решениями	1
Содержание.....	2
Общие механизмы защиты информации в Directum RX	2
Аутентификация.....	2
Криптография.....	2
Мобильные приложения	3
Безопасность сети предприятия.....	3
Использование DMZ и брандмауэров для защиты веб-сервера.....	3
Безопасность передачи данных.....	4
Безопасность устройства.....	5
Электронная подпись.....	7
Безопасность данных	9

Общие механизмы защиты информации в Directum RX

Аутентификация

В мобильных решениях Directum Jazz и Directum Solo предусмотрено два способа аутентификации:

- аутентификация путем ввода реквизитов и их последующей передачи по каналам связи (Windows-аутентификация, аутентификация по паролю). Для использования этих типов аутентификации рекомендуется обеспечить безопасность [каналов связи](#) и [устройства пользователя](#);
- аутентификация с помощью клиентского сертификата – можно использовать только для входа пользователей, которые авторизуются в системе Directum RX с помощью Windows-аутентификации. Данный тип аутентификации является наиболее безопасным, поскольку:
 - реквизиты пользователя не хранятся на устройстве и не передаются по сети;
 - для его работы требуется настройка HTTPS-соединения и блокировка устройства с помощью пароля или PIN-кода.

Криптография

В системе Directum RX есть возможность подписывать документы электронной подписью.

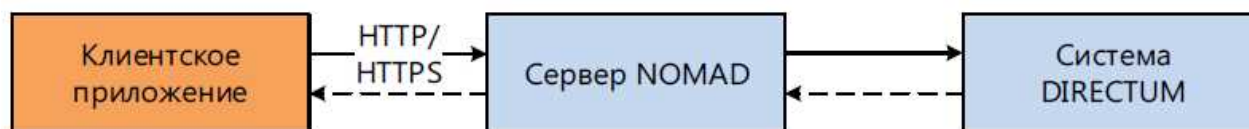
Подписание документов электронной подписью (ЭП) позволяет заменить традиционные печать и подпись, гарантируя авторство подписи и неизменность текста. После подписания текст документа становится недоступным для изменения.

В системе предусмотрено 2 вида ЭП: простая и усиленная. Усиленная подпись устанавливается уполномоченным сотрудником с использованием зарегистрированного в системе персонального

сертификата ЭП. Различают усиленную неквалифицированную ЭП и усиленную квалифицированную ЭП. Их отличие заключается в аккредитации удостоверяющего центра, выдавшего сертификат ЭП.

Мобильные приложения

Архитектура мобильных приложений Directum представляет собой классическую клиент-серверную архитектуру. Клиентское приложение настроено на определенный адрес веб-сервиса NOMAD. Взаимодействие происходит по протоколу HTTP или HTTPS:



Взаимодействие сервера NOMAD с мобильными устройствами рекомендуется организовывать по протоколу HTTPS с использованием порта TCP **443**. Подробнее о настройке протокола см. в разделе [«Безопасность передачи данных»](#).

При использовании мобильных приложений требуется обеспечить безопасность:

- сервера-посредника между внутренней сетью предприятия и сетью Интернет;
- канала связи;
- устройства пользователя;
- электронной подписи;
- данных приложения.

О политике конфиденциальности читайте [на сайте Directum](#).

Безопасность сети предприятия

Одним из вариантов обеспечения безопасности сети предприятия является настройка демилитаризованной зоны. Подробнее см. статью [«Безопасность: Настройка демилитаризованной зоны»](#) на Directum Club.

Использование DMZ и брандмауэров для защиты веб-сервера

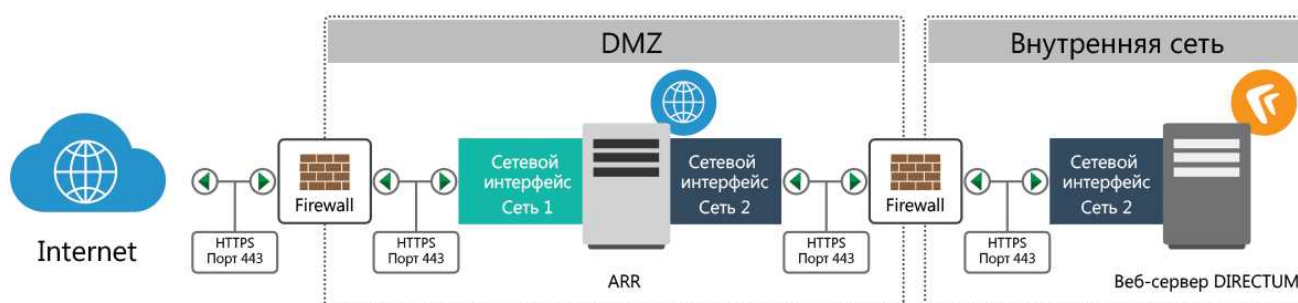
Чтобы защитить веб-сервер от атак из внешних сетей, в организации можно настроить демилитаризованную зону (англ. Demilitarized Zone, DMZ) – конфигурацию сети, направленную на усиление безопасности сети организации. В рамках этой конфигурации сервера, открытые для общего доступа, находятся в отдельном изолированном сегменте сети. Данная концепция обеспечивает отсутствие контактов между открытыми для общего доступа серверами и другими сегментами сети в случае взлома сервера.

Примечание

Данные рекомендации также можно использовать для обеспечения безопасности сервера NOMAD и серверов с другими веб-приложениями.

Для этого понадобится настроить сервера:

- сервер ARR – физический или виртуальный сервер, предназначенный для балансировки нагрузки веб-фермы IIS и реализованный с помощью продукта Microsoft Application Request Routing (ARR);
- сервер веб-доступа – физический или виртуальный сервер, на котором развернут сервер веб-доступа к системе Directum.



Сервер ARR использует два сетевых интерфейса. Пример настройки сетевых интерфейсов сервера ARR и сервера веб-доступа:

- сетевой интерфейс ARR сети 1 – 210.220.230.240/255.255.255.0;
- сетевой интерфейс ARR сети 2 – 192.168.1.1/255.255.255.0;
- сетевой интерфейс сервера веб-доступа сети 2 – 192.168.1.2/255.255.255.0.

Настройка сервера ARR

На сервере ARR развернута веб-ферма, в которую добавлен сервер веб-доступа. Благодаря веб-ферме сервер ARR используется как прокси для веб-запросов из Интернета, адресованных серверу веб-доступа к системе Directum RX.

Чтобы минимизировать возможные способы доступа к серверу ARR, настройте правила брандмауэра ARR для входящих и исходящих соединений. Для сетевых интерфейсов сетей 1 и 2 разрешите входящие и исходящие соединения только через порт 443.

Безопасность передачи данных

Можно выделить следующие виды передаваемых данных:

- аутентификация:
 - логин и пароль при аутентификации по паролю (SOAP);
 - SSL Client Certificate authentication при аутентификации по сертификатам;
- бинарные данные:
 - тела документов;
 - фотографии сотрудников;
- метаданные (SOAP). Например, карточки документов, справочников, заданий, переписка по заданиям.

Приложения могут взаимодействовать с сервисом по протоколу HTTP – открытому небезопасному каналу связи. Использовать его рекомендуется только в условиях работы с тестовой средой или демо-стендом.

При попытке подключения по открытым каналам приложения Directum Jazz и Directum Solo для Android сообщают о возможной угрозе безопасности.

Для безопасной передачи данных применяются:

- VPN для подключения к сети организации;
- HTTPS для шифрования трафика.

VPN

Мобильное устройство можно подключить к VPN как нативными средствами операционной системы, так и с помощью сторонних решений: OpenVPN Connect, ViPNet Client VPN, Checkpoint Capsule.

Для шифрования канала ГОСТ-алгоритмами рекомендуется использовать ViPNet Client VPN.

HTTPS

Наиболее распространенным способом защиты передаваемых данных в веб-приложениях является HTTPS. Он включает в себя несколько криптографических протоколов транспортного уровня.

Мобильные приложения Directum используют протоколы TLS 1.1 и TLS 1.2. Протокол и версия, с которой клиент будет взаимодействовать с сервером, зависит от настроек IIS на сервере.

При попытке подключения по HTTPS с использованием невалидного сертификата мобильное приложение сообщает пользователю о возможной угрозе безопасности. Дальнейшая работа с сервисом невозможна.

Если сертификат выдан внешним доверенным центром сертификации (ЦС), то дополнительная настройка не требуется.

Если сертификат выдан внутренним ЦС, то необходимо настроить доверие к ЦС. Для этого установите сертификат удостоверяющего центра в соответствующее хранилище устройства.

Примечание

Сертификат [SHA-1](#) считается небезопасным. С версии iOS 10.3 для работы с ним требуется дополнительная [настройка](#).

Рекомендации к сертификату см. в разделе [«Настройка защищенного соединения»](#).

Безопасность устройства

Безопасность устройства с установленным мобильным приложением обеспечивается:

- защитой от перебора паролей. После пяти неудачных попыток входа IP-адрес, с которого производится подключение, блокируется на 30 минут;
- ограниченным временем жизни сессии пользователя при отсутствии его активности. Для поддержания сессии пользователя используется идентификатор сессии, передаваемый в Cookie. По умолчанию продолжительность жизни сессии составляет один час с момента последней активности пользователя. Продолжительность жизни сессии настраивается администратором;
- централизованным управлением мобильными устройствами с помощью [MDM-решений](#). Например, с помощью решения [SafePhone](#) администратор может удаленно установить доверенное приложение или запретить его использование;
- подтверждением подключения мобильного устройства пользователя к серверу NOMAD. Выполняется при входе пользователя в приложение. В зависимости от настроек подключение подтверждает администратор или пользователь. Запрос подтверждения приходит на

электронную почту. Без подтверждения подключения данные не будут передаваться с сервера NOMAD на устройство.

Далее в разделе приведены рекомендации по обеспечению безопасности устройств на базе [iOS](#) и [Android](#).

Устройства на Android

При авторизации приложение передает реквизиты для подключения пользователя в открытом виде. Для безопасной передачи данных рекомендуется использовать HTTPS-соединение. При этом необходимо использовать сертификат, выданный доверенным центром сертификации.

Особенности хранения данных приложения:

- логин и пароль пользователя хранятся в системных аккаунтах устройства, пароль хранится в зашифрованном виде;
- при аутентификации по сертификату логин и пароль не используются и не хранятся на устройстве;
- загруженные документы хранятся в системной папке приложения в незашифрованном виде. Рекомендуется ограничивать доступ к устройству;
- данные пользователя хранятся в системной базе данных SQLite без шифрования;
- закрытый ключ для подписания документов хранится в KeyChain – системном хранилище учетных данных;
- поддерживается работа с зашифрованной файловой системой [Full Disk Encryption](#).

Примечание

Не рекомендуется использовать устройства с root-доступом, так как это снижает безопасность использования приложения.

Устройства на iOS

Приложение работает в изолированной области памяти устройства. Другие приложения не имеют к ней доступ. Безопасность данных пользователя обеспечивается средствами операционной системы.

Логин и пароль для подключения хранятся на устройстве с использованием сервисов [Keychain](#) и передаются в SOAP-пакете по HTTP-каналу. При аутентификации по сертификату логин и пароль не используются и не хранятся на устройстве.

Документы пользователя загружаются в контейнер приложения, доступ к которому из других приложений или с компьютера невозможен. Сторонние приложения могут получить доступ к документам, только если экспортировать их из Directum Solo.

Документы шифруются AES-алгоритмом. Для сохранности данных необходимо использовать блокировку устройства. Рекомендуется использовать PIN-код. Графический ключ или отпечаток пальца не являются достаточными мерами защиты.

Примечание

Не рекомендуется использовать устройства с jailbreak, так как это снижает безопасность использования приложения.

Электронная подпись

Мобильное приложение Directum Solo использует для подписания механизмы:

- [КриптоПро CSP](#);
- [аппаратный ключ \(токен\)](#);
- [базовые СКЗИ, встроенные в ОС](#).

КриптоПро CSP

Подписание с использованием КриптоПро CSP поддерживается во всех мобильных приложениях Directum. Для подписания требуется клиентская лицензия СКЗИ «КриптоПро CSP».

На компьютере пользователя генерируется контейнер с закрытым ключом. Далее контейнер копируется на мобильное устройство и во внутреннее хранилище КриптоПро CSP. После успешного копирования контейнера псевдоним (алиас) сертификата и его пароль записываются в локальную БД SQLite на мобильном устройстве. В дальнейшем рекомендуется удалить контейнер из папки на устройстве и с компьютера пользователя.

При запуске мобильного приложения происходит инициализация КриптоПро CSP.

Работа с КриптоПро CSP различается в зависимости от ОС:

- Android – мобильное приложение регистрируется в ОС как реализация ГОСТ-криптографических алгоритмов. Это позволяет работать с ними, как с любыми другими алгоритмами, используя базовые средства ОС;
- iOS – КриптоПро CSP встроен в приложение. Настраивается в разделе «Сертификаты» настроек приложения. Использует Microsoft Crypto API, реализуя ГОСТ-алгоритмы. Установка каких-либо дополнительных модулей не требуется.

Подписание с использованием КриптоПро CSP состоит из этапов:

1. Закрытый ключ загружается из хранилища по известному алиасу сертификата.
2. Подписываемый документ хешируется по указанному в сертификате алгоритму. Хеш формируется:
 - в ОС Android – средствами ОС с использованием КриптоПро CSP;
 - в ОС iOS – средствами встроенного модуля КриптоПро CSP.
3. Полученный хеш вместе атрибутами, необходимыми для формирования подписи, подписывается в зависимости от ОС аналогично п.2.

Аппаратный ключ (токен)

Мобильные приложения поддерживают токены:

- Solo для iOS – RutokenBT;
- Solo для Android – RutokenBT и JaCarta microUSB.

С токенов можно использовать сертификаты с поддержкой алгоритмов ГОСТ и RSA. Для взаимодействия с токенами используется интерфейс стандарта PKCS#11.

Перед использованием токен рекомендуется отформатировать и установить использование шифрованного соединения.

Процесс подписания с помощью токена состоит из этапов:

1. Поиск подключенных токенов и формирование соединения с токеном.

2. Сопоставление пользовательских сертификатов сертификатам, найденным на токене, и определение используемого сертификата.
3. Аутентификация пользователя путем ввода PIN-кода токена.
4. Получение ID закрытого ключа, соответствующего найденному сертификату.
5. Тело подписываемого документа хешируется указанным в сертификате алгоритмом. Хеш формируется средствами ОС. Подробнее см. в разделе [«КриптоПро CSP»](#).
6. Полученный хеш передается в токен и подписывается закрытым ключом с указанным ID. При этом закрытый ключ не покидает токен, все криптографические преобразования выполняются аппаратно.

Базовые СКЗИ, встроенные в ОС

Для подписания используются средства, встроенные в ОС. Механизм зависит от используемой операционной системы: [Android](#) или [iOS](#).

Поддерживается подписание сертификатами [Microsoft CA](#).

Устройства на Android

Для подписания используются базовые средства ОС Android. Поддерживаются только RSA-сертификаты.

Примечание

В ОС Android для работы с криптографией используется набор библиотек Spongy Caste из стандартной поставки ОС.

На компьютере пользователя создается контейнер с закрытым ключом с расширением .pfx или .p12. После этого контейнер копируется на мобильное устройство. На устройстве сертификат с закрытым ключом устанавливается в системное хранилище KeyChain. В дальнейшем контейнер рекомендуется удалить из папки на устройстве и с компьютера пользователя.

Подписание базовыми средствами ОС Android состоит из тех же этапов, что и подписание средствами [КриптоПро CSP](#).

Устройства на iOS

Подписание реализовано средствами платформы .NET – обертки Microsoft RSACryptoServiceProvider. Поддерживаются только RSA-сертификаты.

Примечание

Платформа .NET в мобильных приложениях – это входящая в состав приложения кроссплатформенная реализация платформы .NET [Mono](#).

На компьютере пользователя создается контейнер с закрытым ключом с расширением .pfx. После этого контейнер копируется на мобильное устройство через iTunes в раздел «Документы» приложения.

Далее в разделе «Настройки» приложения ключ импортируется в закрытое хранилище и автоматически удаляется из открытого раздела «Документы».

Подписание базовыми средствами платформы .NET состоит из тех же этапов, что и подписание средствами [КриптоПро CSP](#).

Хранение контейнера с закрытым ключом сертификата Microsoft CA на мобильном устройстве

Устройства на Android

Контейнер с закрытым ключом сертификата Microsoft CA хранится в системном хранилище [KeyChain](#). Приложение разово запрашивает у пользователя доступ к контейнеру и сохраняет полученный алиас в локальную БД SQLite на мобильном устройстве. Последующие обращения к контейнеру происходят по уже известному алиасу без отдельного запроса.

При хранении закрытых ключей в хранилище KeyChain на устройстве должна быть установлена блокировка экрана. Рекомендуется использовать пароль или пин-код.

Устройства на iOS

Контейнер с закрытым ключом помещается в файловый каталог приложения и доступен только для процессов, авторизованных на обращение. Контейнер хранится в зашифрованном виде.

Чтобы получить доступ к ключу, мобильное приложение Directum Solo генерирует уникальное имя для каждого сохраняемого контейнера. Приложение сохраняет алиас и пароль для контейнера в системное шифрованное хранилище [KeyChain](#). Доступ к хранилищу запрещен, если устройство заблокировано пин-кодом или TouchID.

Безопасность данных

Блокировка приложения по истечении определенного времени бездействия пользователя

В Directum Solo можно настроить блокировку приложения, которая будет срабатывать по истечении 15 минут неактивности пользователя. Снять блокировку можно по пин-коду или отпечатку пальца. После 5 неудачных попыток входа ввод пин-кода или отпечатка пальца блокируется на некоторое время.