JC-WebClient v. 4

Строгая аутентификация и электронная подпись для Web-приложений и облачных сервисов

- Работает со всеми популярными браузерами на платформах Microsoft Windows, Apple macOS и Linux
- Приложение устанавливается при первом посещении защищаемого Web-ресурса, в дальнейшем работает в фоновом режиме и не требует администрирования
- Поддерживает работу как с зарубежными, так и с российскими криптографическими алгоритмами
- Поддерживает самые популярные токены: JaCarta-2 ГОСТ, JaCarta ГОСТ, eToken ГОСТ и eToken PRO (Java)

Проблемы поддержки смарт-карт и USB-токенов в Web-приложениях

Безопасная работа в Web-приложениях требует применения механизмов строгой двухфакторной аутентификации и электронной подписи (ЭП), которые традиционно обеспечиваются с помощью смарт-карт и USB-токенов (далее — токенов).

Браузеры не предоставляют Web-страницам доступ к токенам — для этого требуется установка расширений (плагинов) для браузера или использование иных технологий. Для Microsoft Internet Explorer расширения обычно разрабатываются с помощью технологии ActiveX, для остальных браузеров — с помощью архитектуры NPAPI.

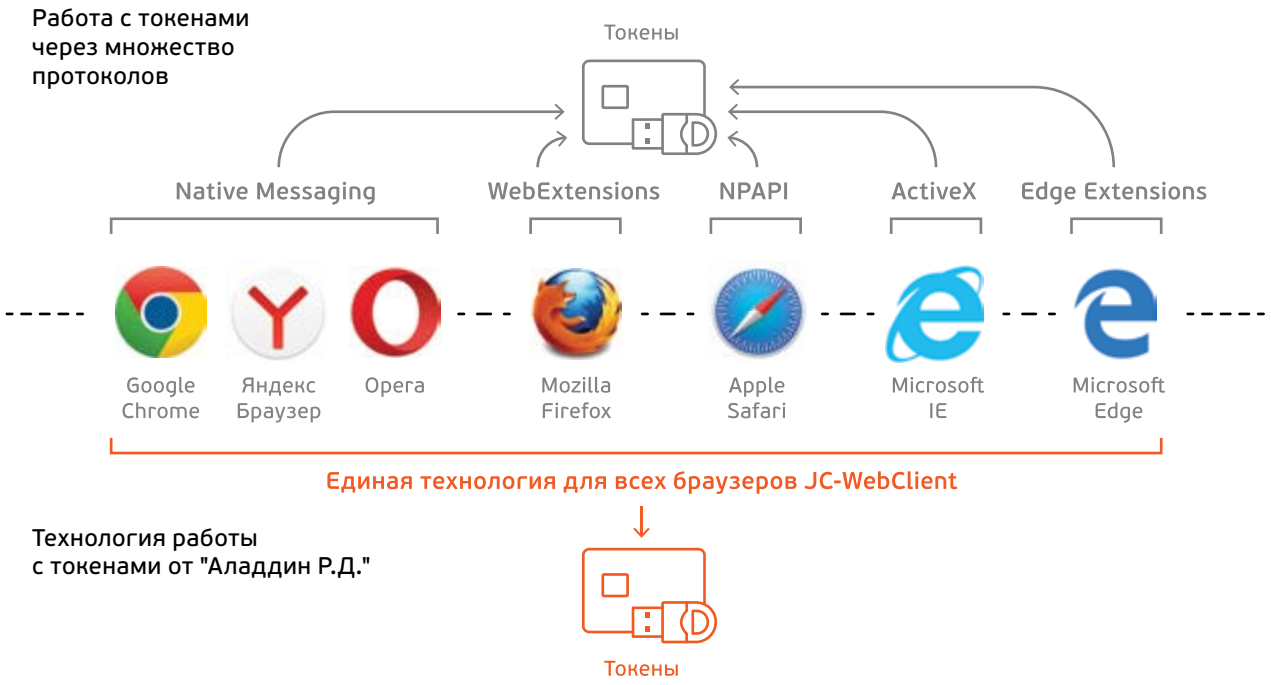
В настоящее время из-за уязвимостей и ограничений NPAPI разработчики браузеров стали отказываться от этой архитектуры в пользу собственных решений, и теперь необходимо адаптировать Web-приложения под "зоопарк" различных технологий, используемых браузерами. Это усложнило мультибраузерную поддержку токенов, создало большое число потенциальных точек отказа и стало причиной возникновения проблем с обратной совместимостью. В результате временные и финансовые затраты разработчиков Web-приложений значительно возросли.

JC-WebClient — новая технология работы с токенами в Web-приложениях

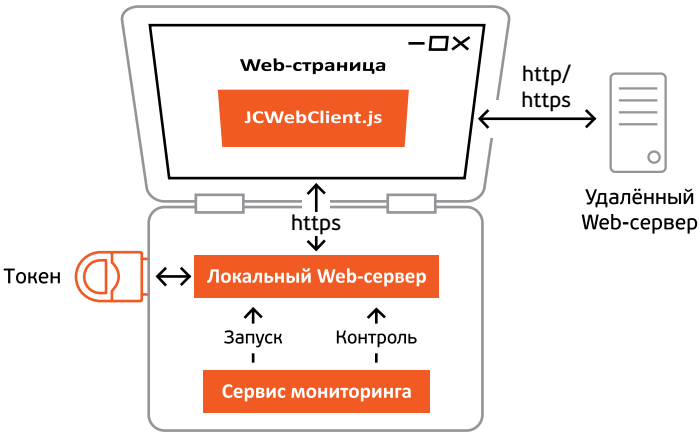
JC-WebClient позволяет легко встроить в Web-приложения функции:

- строгой двухфакторной взаимной аутентификации пользователя и Web-сервера;
- формирования и проверки ЭП с использованием российских или зарубежных криптоалгоритмов;
- шифрования данных, передаваемых между клиентским ПК и Web-сервером.

Особенность JC-WebClient состоит в том, что для работы со всеми популярными браузерами используется единая технология локального Web-сервера, не зависящая от нативных технологий различных браузеров. При этом канал связи между браузером и локальным Web-сервером защищён с использованием TLS.



Состав JC-WebClient



Приложение JC-WebClient

Реализует технологию локального Web-сервера

- Обеспечивает взаимодействие между Web-страницей и токеном по протоколу HTTPS
- Предоставляет Web-страницам JavaScript API для доступа к функциям токена через клиентский скрипт JCWebClient.js, который загружается на Web-страницу от локального Web-сервера
- Работает в фоновом режиме, не предоставляя никаких элементов управления пользователю

Сервис мониторинга

Запускает приложение JC-WebClient при загрузке операционной системы (ОС)

- Контролирует целостность приложения и перезапускает его при возникновении нештатных ситуаций в ОС
- Обеспечивает надёжность и отказоустойчивость решения

Токен

USB-токен или смарт-карта JaCarta или eToken

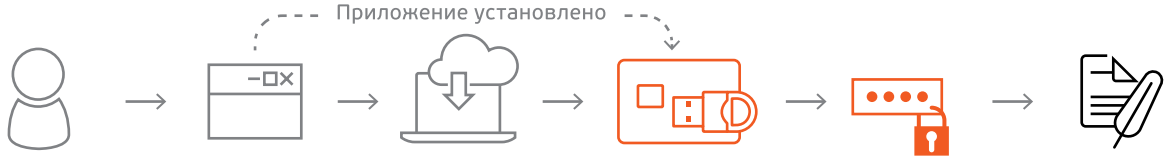
- JaCarta-2 ГОСТ — средства ЭП нового поколения с аппаратной поддержкой новых российских криптографических алгоритмов ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012
- JaCarta ГОСТ и eToken ГОСТ — персональное средство строгой двухфакторной аутентификации и усиленной квалифицированной ЭП с неизвлекаемым закрытым ключом, в котором реализованы российские криптоалгоритмы
- JaCarta PRO и eToken PRO (Java) — персональное средство строгой двухфакторной аутентификации и усиленной ЭП с неизвлекаемым закрытым ключом, в котором реализованы зарубежные криптоалгоритмы

Опция "Антифрод-терминал"

Trust Screen-устройство для безопасной аутентификации, работы с электронной подписью и подтверждения операций/транзакций в недоверенной среде

- Надёжно защищает от атак со стороны вредоносного ПО и злоумышленников, пытающихся выполнить несанкционированные операции от лица пользователя
- При интеграции со средствами ЭП обеспечивает визуализацию и подтверждение ключевых данных подписываемых документов

Как это работает



1. Пользователь заходит на Web-портал
2. Web-портал проверяет, установлен ли JC-WebClient
3. Web-портал загружает инсталлятор JC-WebClient на компьютер пользователя.
   Пользователь выполняет установку
4. Web-портал находит подключенный токен JaCarta или eToken
5. Web-портал запрашивает PIN-код к токену и выполняет строгую двухфакторную аутентификацию пользователя
6. Web-портал предоставляет пользователю возможность работать с ЭП и шифровать данные

Преимущества JC-WebClient

Согласно опыту наших партнёров, встраивание JC-WebClient в Web-приложения занимает не более 10 человеко-дней.

Требования к уровню квалификации программиста: знание JavaScript и навыки Web-разработки.

Примеры проектов с использованием JC-WebClient

СБЕРБАНК РОССИИ
НПФ Сбербанка

Система ДБО для юридических лиц "Мой бизнес" Промсвязьбанка

Личный кабинет Индивидуального предпринимателя на Портале ФНС

R•Style Softlab
Система ДБО InterBank Corporate
Система ДБО InterBank Start

iSimple Lab
Система ДБО iSimpleBank 2.0

Board Maps
Решение для результативного проведения совещаний и заседаний

Для разработчиков

Лёгкость интеграции и поддержки

- Поддержка всех популярных браузеров и ОС.
- Отсутствие проблем совместимости нативных технологий, свойственных различным браузерам.
- Независимость от типа Web-сервера и языка разработки Web-приложений.
- Работа как с зарубежными, так и с российскими криптографическими алгоритмами, что даёт свободу выбора модели токенов и вида применяемой ЭП.
- Поддержка работы с самыми распространёнными в России токенами: JaCarta-2 ГОСТ, JaCarta ГОСТ, eToken ГОСТ и eToken PRO (Java).
- Простой API, понятный даже начинающим Web-разработчикам, и исчерпывающие примеры интеграции с исходными кодами.
- В процессе интеграции разработчикам доступны бесплатные консультации специалистов "Аладдин Р.Д.".

Безопасность

- Обеспечение односторонней или взаимной строгой двухфакторной аутентификации пользователя и Web-сервера с помощью токена.
- Поддержка токенов с неизвлекаемым закрытым ключом ЭП.
- Ограничение доступа к операциям с закрытым ключом токена вкладкой браузера, из которой был введён PIN-код.
- Возможность шифровать данные между клиентским ПК и сервером по ГОСТ 28147-89.
- Построение защищённого канала между приложением JC-WebClient и устройством JaCarta-2 ГОСТ, подключенным в USB-порт.
- Отказ от использования плагинов и небезопасной архитектуры NPAPI.
- Сохранении сессии работы с токеном при переходах между Web-страницами без сохранения PIN-кода в памяти ПК.
- Автоматическая блокировка сессии при отключении токена.

Надёжность и отказоустойчивость

- Контроль целостности приложения, автоматический запуск при старте ОС и перезапуск при возникновении сбоев в ОС с помощью сервиса мониторинга.
- Снижение количества возможных точек отказа за счёт использования единой для всех браузеров технологии локального Web-сервера.

Опция "Антифрод-терминал"

- Поддержка устройства "Антифрод-терминал" для безопасной аутентификации, безопасной работы с ЭП, безопасного подтверждения транзакций и операций при работе пользователя в недоверенной среде.

Для пользователей

- Простота установки — приложение JC-WebClient устанавливается при первом посещении защищаемого Web-ресурса, не требует установки драйверов для токенов и дополнительных плагинов.
- Простота использования — приложение автоматически запускается при загрузке ОС и работает в фоновом режиме. Пользователю недоступны элементы управления приложением, что делает его работу простой и прозрачной.
- Снижение затрат — приложение JC-WebClient бесплатно. Оплачивается только токен. Не нужно приобретать дополнительные программные СКЗИ.

Проблемы работы с электронной подписью в недоверенной среде

Атаки с подменой подписываемого документа

Пользователь видит на экране компьютера один документ, а в момент его подписания вредоносное программное обеспечение (ПО) незаметно подменяет его на другой. В результате в токен для вычисления ЭП отправляется хэш подменённого документа. Например, в случае успешной подмены платёжного поручения деньги с банковского счёта отправителя могут быть переведены на счёт злоумышленника. Такие атаки могут быть реализованы следующими способами:

- перехват трафика по протоколу USB-CCID;
- внедрение в код приложения или браузера (в этом случае шифрованный канал, который может быть установлен между банковским приложением и токеном, не помогает).

Атаки с подписью посторонних поддельных документов

Получив удалённое управление компьютером пользователя или внедрив в него вредоносное ПО, злоумышленник может подписывать любые документы на его ключах, пока токен подключен к компьютеру. Такие атаки могут быть реализованы следующими способами:

- использование состояния "залогиненности" (когда токен подключен к ПК и пользователь уже ввёл PIN-код). В этот момент вредоносное ПО отправляет в токен хэш постороннего документа и вычисляет ЭП;
- перехват PIN-кода с помощью вредоносного ПО с последующей аутентификацией и подписанием любого документа. Виртуальные клавиатуры не дают гарантию защиты от перехвата PIN-кода.

Описанные атаки показывают, что сегодня нельзя гарантировать отсутствие вредоносное ПО на компьютере пользователя, особенно если он постоянно подключен к сети Интернет. По этой причине компьютер пользователя всегда следует считать недоверенной средой.

Токены с неизвлекаемым закрытым ключом надёжно защищают ключ ЭП от кражи. Тем не менее, злоумышленники научились подписывать поддельные электронные документы без кражи ключей ЭП. Для этого они применяют вредоносное программное обеспечение, созданное с учётом специфики работы атакуемой системы.

"Антифрод-терминал" — решение для работы с электронной подписью в недоверенной среде

Для борьбы с атаками злоумышленников в недоверенной среде применяются Trust Screen-устройства, обеспечивающие возможность подтвердить операцию подписания документов в доверенной среде таких устройств. Компания "Аладдин Р.Д." совместно с компанией VASCO разработала собственное Trust Screen-устройство — "Антифрод-терминал".

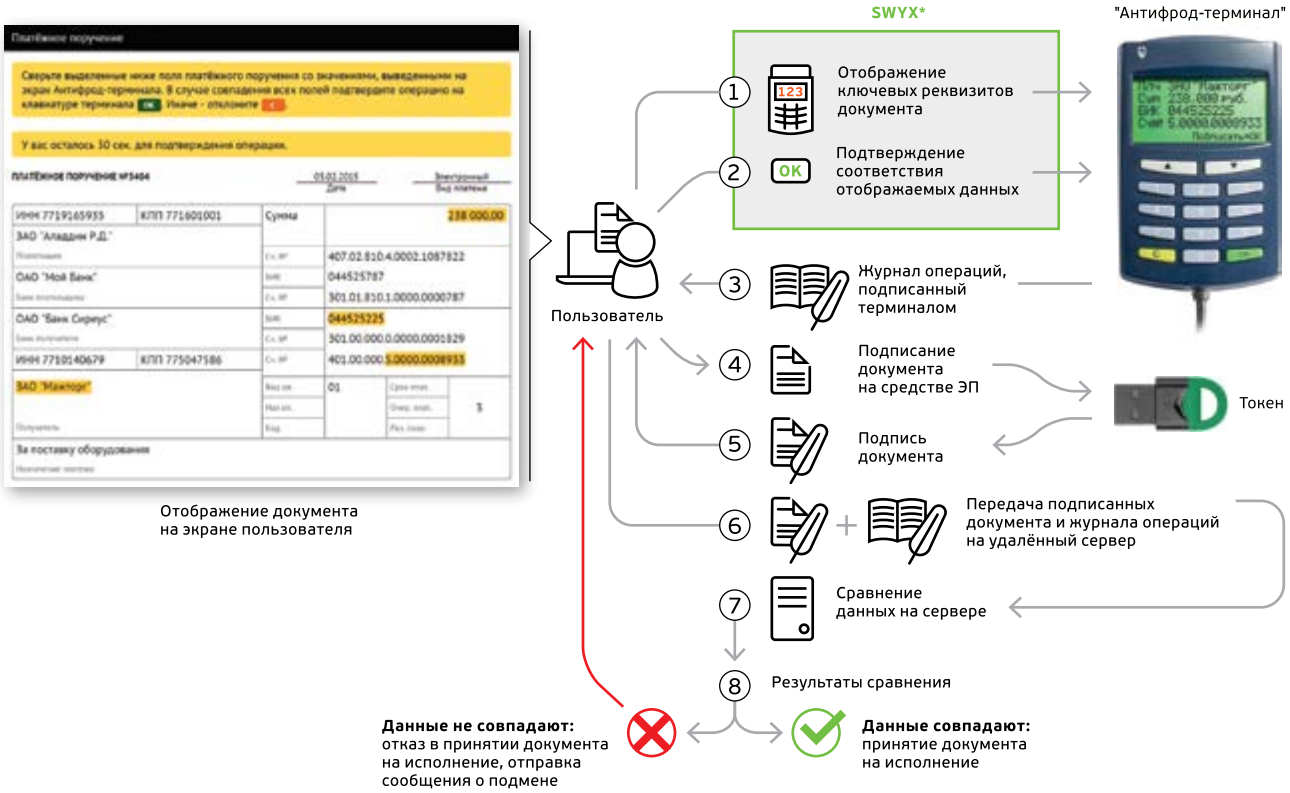
Основными областями применения "Антифрод-терминала" являются:

- **защита систем дистанционного банковского обслуживания (ДБО)** от атак, направленных на кражу денежных средств со счетов клиентов банка;
- **защита систем ЭДО и электронных сервисов** от атак, направленных на подписание поддельных документов на ключах ЭП легального пользователя и последующее навязывание этих документов системе или сервису.

Возможности "Антифрод-терминала"

- Безопасная аутентификация пользователя
- Безопасное подтверждение транзакций
- Визуализация и подтверждение ключевых данных подписываемого документа
- Ведение защищённого журнала операций, который терминал подписывает собственной ЭП на встроенном в устройство криптографическом чипе
- Безопасное ведение "белых списков" доверенных контрагентов для удобного выполнения групповых операций

Схема работы "Антифрод-терминала"



Отображение документа на экране пользователя

Преимущества "Антифрод-терминала"

Строгая аутентификация терминала на сервере. Сервер может гарантированно убедиться в том, что пользователь подтвердил операцию на доверенном зарегистрированном терминале. Терминал в системе подменить нельзя.

Формирование доказательной базы. Журнал операций, формируемый "Антифрод-терминалом" и сохраняемый на сервере, может быть использован электронным сервисом в качестве доказательной базы при расследовании инцидентов и разборе конфликтных ситуаций.

Контроль полноты подтверждаемых данных. Если данные для подтверждения не вмещаются на один экран, предусмотрена их прокрутка на устройстве. Терминал не примет подтверждения от пользователя, пока тот не прокрутит данные до конца и не убедится в их корректности (что злоумышленники их не подменили). Это также важно с точки зрения доказательной базы, так как такая реализация позволяет при необходимости доказать, что пользователь ознакомился со всеми данными, отображёнными на устройстве, а не только с их частью.

Независимость прошивки терминала от типа используемой смарт-карты или USB-токена. "Антифрод-терминал" может быть интегрирован со смарт-картами стандарта ISO 7816, а также любыми USB-токенами и программными СКЗИ. При смене средства ЭП не требуется вносить какие-либо изменения в прошивку "Антифрод-терминала", что избавляет от проблем с совместимостью и удешевляет эксплуатацию устройства.

Удобная реализация групповых операций. Возможность безопасного ведения "белых" списков доверенных контрагентов позволяет существенно сократить количество документов, которые потребуется подтверждать на "Антифрод-терминале" при выполнении групповых операций.

Быстрое встраивание в прикладные системы. Согласно опыту наших партнёров, встраивание "Антифрод-терминала" занимает около 10 человеко-дней. Программист должен знать JavaScript и иметь навыки Web-разработки.

* SWYX (Sign What You eXecute = "Подписываю то, что выполняется") — "Антифрод-терминал" ведёт защищённый журнал операций и подписывает его своей ЭП с помощью встроенного криптографического чипа, поддерживающего российскую криптографию.

Технические спецификации JC-WebClient

Параметр	Описание	
Поддерживаемые ОС	**Microsoft** • Microsoft Windows 10 • Microsoft Windows 8-8.1 • Microsoft Windows 7 • Microsoft Windows Vista • Microsoft Windows XP **Apple** • macOS 10.12 (Sierra) • OS X 10.11 (El Capitan) • OS X 10.10 (Yosemite) • OS X 10.9 (Mavericks)	**Linux** • CentOS 7 (64-бит) • Debian 8.4 • Debian 7.10 (64-бит) • Fedora 23 (64-бит) • openSUSE Leap 42.1 (64-бит) • openSUSE 13.2 • Red Hat Enterprise 7.2 (64-бит) • Ubuntu 16.04 • Ubuntu 14.04
Поддерживаемые браузеры	• Google Chrome • Mozilla Firefox • Microsoft Internet Explorer 8-11 • Microsoft Edge	• Apple Safari • Opera • Яндекс.Браузер
Поддержка USB-токенов и смарт-карт	**Есть**	
Поддерживаемые типы токенов	**JaCarta** • JaCarta-2 ГОСТ • JaCarta ГОСТ • JaCarta PRO • Комбинированные токены семейства JaCarta-2 и JaCarta, поддерживающие функциональность ГОСТ и/или PRO	**eToken** • eToken ГОСТ • eToken PRO (Java)
Типы аутентификации	Строгая взаимная двухфакторная аутентификация пользователя и Web-сервера с выработкой общего симметричного ключа шифрования по ГОСТ (при использовании JaCarta ГОСТ, eToken ГОСТ) или по AES-128 и 3DES (при использовании JaCarta PRO, eToken PRO (Java))	
Интеграция с PKI	• Поддержка цифровых сертификатов X.509 • Генерация запросов на сертификат в формате PKCS#10 • Формирование и разбор конвертов в формате PKCS#7	
Поддерживаемые криптоалгоритмы	**При работе с токенами JaCarta-2 ГОСТ (СКЗИ "Криптотокен 2 ЭП")** • ГОСТ 28147-89 (симметричное шифрование) • ГОСТ Р 34.11-94 (функция хэширования) • ГОСТ Р 34.10-2001 (генерация ключевых пар, формирование и проверка ЭП) • ГОСТ Р 34.10-2012 (генерация ключевых пар, формирование и проверка ЭП) • ГОСТ Р 34.11-2012 (функция хэширования) • выработка ключа парной связи на основе преобразований по алгоритмам VKO GOST R 34.10-2001 (в соответствии с RFC 4357) и VKO_GOSTR3410_2012_256 (в соответствии с рекомендациями Технического комитета 026) **При работе с токенами JaCarta ГОСТ и eToken ГОСТ (СКЗИ "Криптотокен ЭП")** • ГОСТ 28147-89 (симметричное шифрование) • ГОСТ Р 34.11-94 (функция хэширования) • ГОСТ Р 34.10-2001 (генерация ключевых пар, формирование и проверка ЭП) **При работе с токенами JaCarta PRO и eToken PRO (Java)** • 3DES (симметричное шифрование) • AES-128 (симметричное шифрование) • SHA-1 (функция хэширования) • RSA 1024 (генерация ключевых пар, формирование и проверка ЭП)	
Поддерживаемые типы ЭП	• Усиленная (с использованием российских или зарубежных криптоалгоритмов) • Усиленная квалифицированная (при выпуске сертификата ЭП в аккредитованных УЦ)	
Срок хранения закрытого ключа ЭП	**3 года**	
Дополнительный PIN-код для операции формирования ЭП	Есть при использовании устройств JaCarta-2 ГОСТ	

Параметр	Описание
Разблокировка PIN-кодов пользователя и ЭП по PUK-коду	Есть
Поддержка доверенных открытых ключей JaCarta-2 ГОСТ	С их помощью осуществляется построение цепочек доверия к сертификатам подписантов и сертификатам получателей/отправителей зашифрованных сообщений. Срок жизни доверенных ключей — 15 лет
Построение защищённого канала между приложением и токеном	Есть при использовании устройств JaCarta-2 ГОСТ
Поддержка программного (быстрого) шифрования и вычисления хэш-функции	Есть
Необходимость наличия прав администратора для первичной установки JC-WebClient	Есть
Обновление установленной версии JC-WebClient	Обновление, как правило, может быть осуществлено путём скачивания и запуска специального инсталлятора, не требующего прав локального администратора
Поддерживаемые типы Web-серверов	Любые
Лицензионные отчисления	Нет
Территориальные ограничения	Только РФ (поскольку в составе решения используются сертифицированные СКЗИ "Криптотокен ЭП" и "Криптотокен 2 ЭП", распространение и использование ограничено только территорией РФ (см. Приказ ФСБ РФ от 9 февраля 2005 г. № 66). Web-серверы также должны быть расположены на территории РФ (см. Федеральный закон от 31.12.2014 № 531-ФЗ))
Комплект разработчика JC-WebClient SDK	Состав • Примеры интеграции в виде демо-портала с исходными кодами на Microsoft ASP.NET • Документация для разработчиков *При встраивании в прикладное ПО СКЗИ или средств ЭП с использованием российских криптоалгоритмов разработчик должен иметь лицензию ФСБ России*
Поддержка устройств для работы в недоверенной среде	"Антифрод-терминал"
Демонстрация работы JC-WebClient	Для демонстрации работы JC-WebClient доступен демо-портал **demo.aladdin-rd.ru**, представляющий собой упрощённый вариант личного кабинета системы ДБО. Обеспечена поддержка токенов JaCarta ГОСТ и "Антифрод-терминала"
Сертификация	**В состав решения JC-WebClient входят токены JaCarta, имеющие сертификаты ФСТЭК России и ФСБ России.** • **Сертификат соответствия ФСБ России № СФ/124-3112** подтверждает, что СКЗИ "Криптотокен 2 ЭП" в составе JaCarta-2 ГОСТ соответствует требованиям ГОСТ 28147-89, ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012, а также требованиям к СКЗИ класса КС1 и КС2 и требованиям к средствам ЭП класса КС1 и КС2, и может использоваться для криптографической защиты информации, не содержащей сведений, составляющих государственную тайну. • **Сертификат соответствия ФСБ России № СФ/111-2750** подтверждает, что персональное средство электронной подписи "Криптотокен ЭП", предназначенное для использования совместно с СКЗИ "Криптотокен" в составе изделия JaCarta ГОСТ (eToken ГОСТ), соответствует требованиям к средствам ЭП по классам КС1 и КС2 и может использоваться для реализации функций ЭП в соответствии с 63-ФЗ «Об электронной подписи» от 6 апреля 2011 года. • **Сертификат соответствия ФСТЭК России № 2799** подтверждает, что JaCarta является программно-техническим средством защиты информации, не содержащей сведений, составляющих государственную тайну, от несанкционированного доступа, и соответствует требованиям по 4 уровню контроля отсутствия недекларированных возможностей (НДВ 4) и требованиям Технических условий.

Лицензии ФСТЭК России № 0037 и № 0054 от 18.02.03, № 2874 от 18.05.12
Лицензии ФСБ России № 12632Н от 20.12.12, № 30419 от 16.08.17
Лицензия Министерства обороны РФ № 1384 от 22.08.16
Система менеджмента качества компании соответствует требованиям стандарта ISO/ИСО 9001-2011
Сертификат СМК ГОСТ Р ИСО 9001-2011 № РОСС RU.ИС72.К00082 от 10.07.15
Apple Developer

+7 (495) 223-00-01 aladdin@aladdin-rd.ru **Web**: www.aladdin-rd.ru

ID: 6012-060917