"Антифрод-терминал"

Для безопасной аутентификации и работы с электронной подписью в недоверенной среде

- Визуализация и подтверждение ключевых реквизитов подписываемых документов
- Безопасная аутентификация с вводом PIN-кода на терминале, а не на компьютере
- Независимость от типа средства электронной подписи
- Формирование доказательной базы для расследований инцидентов и разбора конфликтных ситуаций
- Быстрая интеграция с прикладными программами

Проблемы работы с электронной подписью в недоверенной среде

USB-токены и смарт-карты (далее — токены) с неизвлекаемым закрытым ключом надёжно защищают ключ электронной подписи (ЭП) от кражи. Тем не менее, злоумышленники научились подписывать поддельные электронные документы без кражи ключей ЭП. Для этого они применяют вредоносное программное обеспечение (ПО), созданное с учётом специфики работы атакуемой системы.

Атаки с подписью посторонних поддельных документов

Получив удалённое управление компьютером пользователя или внедрив в него вредоносное ПО, злоумышленник может подписывать любые документы на ключах пользователя, 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. В этом случае виртуальные клавиатуры не дают гарантию защиты от перехвата PIN-кода.

Атаки с подменой подписываемого документа

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

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

Сегодня нельзя гарантировать отсутствие вредоносного ПО на компьютере пользователя, особенно при постоянном подключении к Интернету. По этой причине компьютер пользователя, как правило, является недоверенной средой.

"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 этих 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 электронного документооборота и электронных сервисов** от атак, направленных на подписание поддельных документов на ключах ЭП легального пользователя и последующее навязывание этих документов системе или сервису.

Если в качестве средства ЭП используется смарт-карта, она может быть подключена непосредственно к "Антифрод-терминалу". Если в качестве средства ЭП используется USB-токен, он подключается к одному USB-порту компьютера, а "Антифрод-терминал" — к другому.

Примеры проектов с использованием "Антифрод-терминала"

ПАО "Сбербанк России"

ПАО "БИНБАНК"

АО НПФ "САФМАР"

Поддерживаемые операционные системы

Возможности "Антифрод-терминала"

Безопасная аутентификация

"Антифрод-терминал" позволяет:

- запросить у пользователя подтверждение намерения аутентифицироваться в электронном сервисе на дисплее терминала и принять подтверждение от пользователя на клавиатуре терминала;
- запросить ввод PIN-кода для используемого средства ЭП на дисплее терминала и принять PIN-код на клавиатуре терминала.

Визуализация и подтверждение ключевых данных документа

"Антифрод-терминал" оснащён жидкокристаллическим дисплеем, отображающим текстовые данные длиной до 400 символов. На экран терминала могут выводиться ключевые данные подписываемых документов. Пользователь может сравнить данные на терминале с данными, отображаемыми на экране ПК, после чего подтвердить или отменить операцию подписания документа своей ЭП (нажав на терминале клавишу "ОК" или "С").

Ведение защищённого журнала операций

"Антифрод-терминал" ведёт внутренний журнал операций. В этом журнале фиксируется информация, которая была отображена на экране устройства и подтверждена пользователем путём нажатия кнопки "ОК" на клавиатуре терминала. Журнал операций не хранится в устройстве постоянно. Терминал начинает вести журнал каждый раз заново при начале так называемого SWYX-режима работы устройства (Sign What You eXecuted — подписываю то, что выполняется). По окончании SWYX-режима терминал подписывает журнал собственной ЭП на встроенном в терминал криптографическом чипе с использованием российской криптографии и возвращает его вместе с подписью в прикладное ПО.

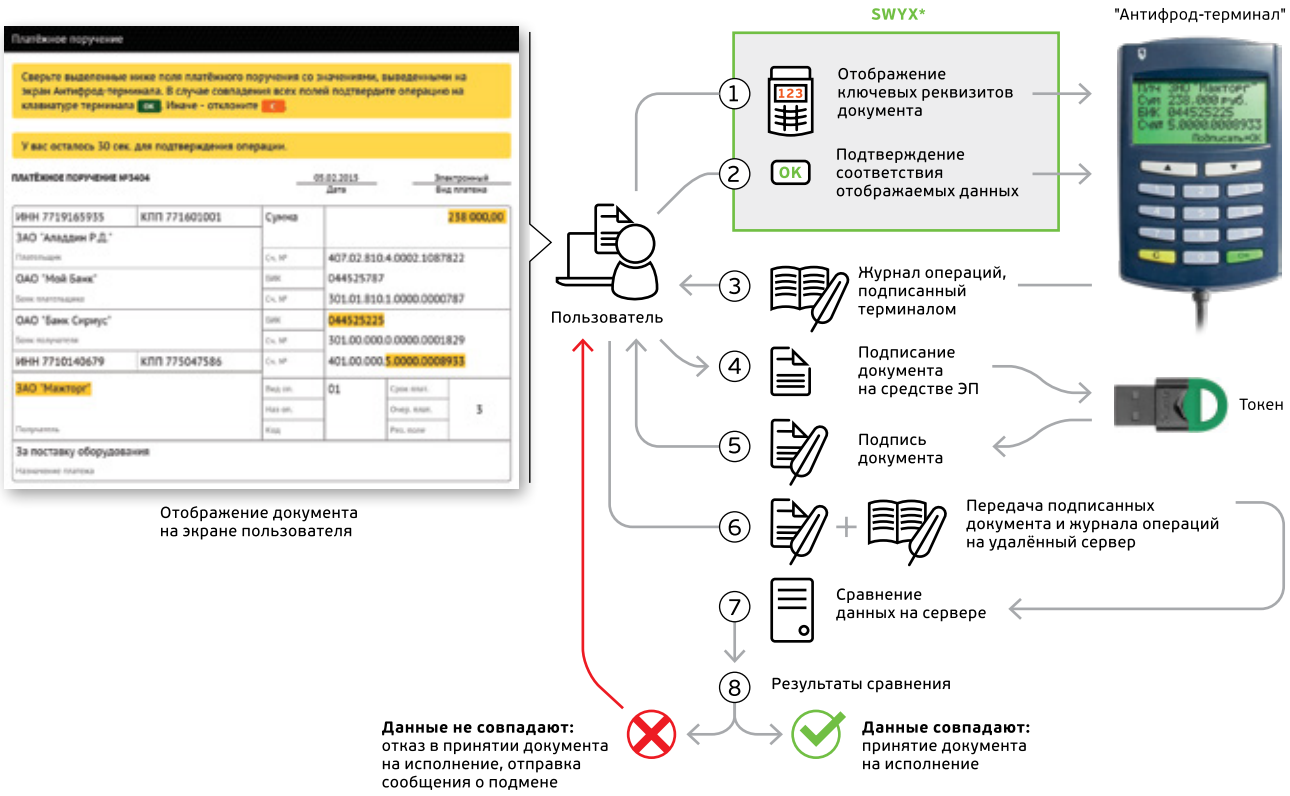
Защита от повторного навязывания перехваченного журнала операций

Терминал предоставляет возможность защититься от атак, направленных на повторное навязывание серверу перехваченного ранее журнала операций вместе с копией соответствующего этому журналу ранее одобренного и принятого на исполнение документа. Для реализации такой защиты следует использовать поле Reference журнала операций, значение которого связывает журнал с конкретным экземпляром подписанного документа или группой документов.

Ведение "белых списков" доверенных контрагентов

Использование "белых списков" позволяет существенно сократить количество документов, которые требуется подтверждать на "Антифрод-терминале" при выполнении групповых операций. Важным при работе с "белыми списками" является то, каким образом такие списки создаются и изменяются. Если злоумышленник сможет несанкционированно добавить себя в "белый список", вся идея таких списков теряет смысл. "Антифрод-терминал" позволяет безопасно создавать и изменять "белые списки" доверенных контрагентов. Для этого достаточно подтверждать на устройстве все операции, связанные с созданием и изменением "белого списка".

Схема работы "Антифрод-терминала"

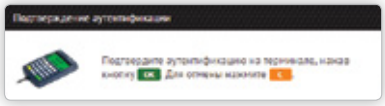


1. Приложение просит пользователя подтвердить ключевые данные документа на терминале.
2. Если данные, отображённые на экране терминала, корректны, пользователь подтверждает их на клавиатуре устройства.
3. "Антифрод-терминал" фиксирует факт подтверждения данных во внутреннем журнале, подписывает журнал собственной ЭП на собственном криптографическом чипе и возвращает подписанный журнал приложению.
4. Документ пользователя подписывается средством ЭП (смарт-картой или USB-токеном).
5. ЭП документа возвращается приложению.
6. Приложение отправляет подписанный ЭП пользователя документ и подписанный ЭП терминала журнал на сервер.
7. Сервер проверяет ЭП документа и ЭП журнала, чтобы убедиться в подлинности заранее зарегистрированного терминала. Затем сервер сверяет данные из журнала с данными из документа.
8. В случае совпадения документ принимается на обработку. В случае расхождения сервер блокирует операцию и уведомляет пользователя о возможной атаке со стороны злоумышленников и необходимости проверить рабочее место на наличие вредоносного ПО.

   Сохранённый на сервере подписанный журнал терминала может в дальнейшем использоваться в качестве доказательной базы при разборах конфликтных ситуаций.

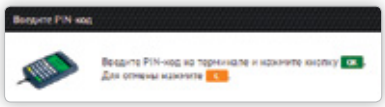
* SWYX (Sign What You eXecuted = "Подписываю то, что выполняется") — "Антифрод-терминал" ведёт защищённый журнал операций и подписывает его своей ЭП с помощью встроенного криптографического чипа, поддерживающего российскую криптографию.

Примеры сценариев работы



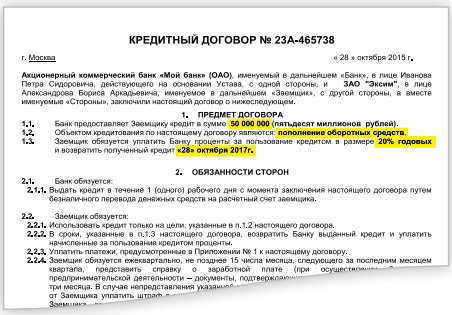
Безопасная аутентификация

При входе в личный кабинет электронного сервиса "Антифрод-терминал" выводит на своём экране запрос на подтверждение аутентификации. Пользователь подтверждает на клавиатуре терминала своё намерение войти в личный кабинет электронного сервиса. Это позволяет защититься от вредоносного ПО, которое смогло перехватить или подобрать PIN-код пользователя и пытается с его помощью получить несанкционированный доступ в личный кабинет от лица легального пользователя.



Дополнительно пользователь вводит PIN-код на "Антифрод-терминале", а не на клавиатуре компьютера. Это обеспечивает защиту от вредоносного ПО, способного перехватывать данные с клавиатуры.

Подписание произвольных неструктурированных документов



КРЕДИТНЫЙ ДОГОВОР № 23А-465738

г. Москва «28» октября 2015 г.

Акционерный коммерческий банк «Мой банк» (ОАО), именуемый в дальнейшем «Банк», в лице Иванова Петра Сидоровича, действующего на основании Устава, с одной стороны, и **ЗАО "Экспи"**, в лице Александрова Бориса Аркадьевича, именуемое в дальнейшем «Заемщик», с другой стороны, а вместе именуемые «Стороны», заключили настоящий договор о нижеследующем.

1. ПРЕДМЕТ ДОГОВОРА

1.1. Банк предоставляет Заемщику кредит в сумме **50 000 000 (пятьдесят миллионов рублей)**.
1.2. Объектом кредитования по настоящему договору являются **пополнение оборотных средств**.
1.3. Заемщик обязуется уплатить Банку проценты за пользование кредитом в размере **20% годовых** и возвратить полученный кредит **«28» октября 2017г.**

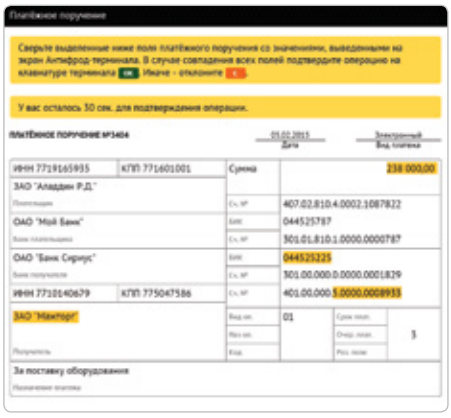
2. ОБЯЗАННОСТИ СТОРОН

2.1. Банк обязуется:
2.1.1. Выдать кредит в течение 1 (одного) рабочего дня с момента заключения настоящего договора путем безналичного перевода денежных средств на расчетный счет заемщика.

2.2. Заемщик обязуется:
2.2.1. Использовать кредит только на цели, указанные в п.1.2 настоящего договора.
2.2.2. В сроки, указанные в п.1.3 настоящего договора, возвратить Банку выданный кредит и уплатить начисленные за пользование кредитом проценты.
2.2.3. Уплатить платежи, предусмотренные в Приложении № 1 к настоящему договору.
2.2.4. Заемщик обязуется ежеквартально, не позднее 15 числа месяца, следующего за последним месяцем квартала, представить справку о заработной плате (при осуществлении предпринимательской деятельности – документы, подтверждающие три месяца. В случае непредставления указанных от Заемщика уплатить штраф.

При подписании неструктурированных документов (договоров, актов, соглашений) на "Антифрод-терминал" выводятся ключевые данные этих документов, которые могут изменяться от пользователя к пользователю. Например, при подписании кредитного договора в качестве таких данных могут выступать поля "сумма", "срок", "процент" и "цель кредита". Подмена таких данных вредоносным ПО на клиентской стороне будет обнаружена сервером при сверке данных из подписанного документа и журнала операций. В случае, когда эталонные шаблоны документов хранятся на сервере, вредоносное ПО также не сможет незаметно подменить данные, которые не выводились на "Антифрод-терминал", так как такая подмена также будет обнаружена сервером путём сверки подписанного и эталонного документов.

Подписание платёжных поручений в системах ДБО



Платёжное поручение

Сверьте выделенные ниже поля платёжного поручения со значениями, выведенными на экран Антифрод-терминала. В случае совпадения всех полей подтвердите операцию на клавиатуре терминала OK. Иначе - отклоните C.

У вас осталось 30 сек. для подтверждения операции.

ПЛАТЁЖНОЕ ПОРУЧЕНИЕ №1404 — 05.02.2015 — Электронный

ИНН 7719165935	КПП 771601001	Сумма	238 000,00
ЗАО "Аладдин Р.Д."		Сч. №	407.02.810.4.0002.1087822
ОАО "Мой Банк"		БИК	044525787
		Сч. №	301.01.810.1.0000.0000787
ОАО "Банк Сириус"		БИК	044525225
		Сч. №	301.00.000.0.0000.0001829
ИНН 7710140679	КПП 775047586	Сч. №	401.00.000.5.0000.0008933
ЗАО "Макторг"		Вид оп. 01	Срок плат.
		Наз. пл.	Очер. плат. 3
Получатель		Код	Рез. поле
За поставку оборудования			
Назначение платежа			

Для защиты от кражи денежных средств необязательно подтверждать все реквизиты платёжного поручения на "Антифрод-терминале" — достаточно подтвердить ключевые реквизиты (например, "получатель", "счёт получателя", "банк получателя" и "сумма платежа"). Если злоумышленник подменит хотя бы один из этих реквизитов в подписанном платёжном поручении, это будет выявлено на сервере, и такая операция будет заблокирована. Подмена других реквизитов не приведёт к краже денежных средств.

Для существенного сокращения количества документов, которые требуется подтверждать на "Антифрод-терминале" при выполнении групповых операций, следует использовать "белые списки" доверенных контрагентов.

Преимущества "Антифрод-терминала"

Строгая аутентификация терминала на сервере

Сервер осуществляет проверку ЭП журнала операций "Антифрод-терминала", что позволяет гарантировать факт подтверждения операции на зарегистрированном доверенном устройстве. Тем самым обеспечивается защита от подмены терминала на клиентской стороне.

Контроль полноты подтверждаемых данных

Для защиты от недобросовестной (неполной) проверки ключевых реквизитов пользователем в "Антифрод-терминале" реализован дополнительный контроль того, что пользователь ознакомился со всеми данными, которые были отображены на экране терминала. Если данные не вместились на один экран, то терминал не позволит подтвердить операцию до тех пор, пока пользователь не прокрутит их до конца. Это также важно и с точки зрения доказательной базы, так как такая реализация позволяет при необходимости доказать, что пользователь собственноручно прокрутил все данные до конца, проверив все реквизиты, и подтвердил операцию, ознакомившись со всеми реквизитами.

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.

Поддержка любых типов средств электронной подписи

"Антифрод-терминал" может быть интегрирован с любыми типами средств ЭП: смарт-картами стандарта ISO 7816, USB- и MicroUSB-токенами, а также 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.

Подписание оригинального документа

Благодаря тому, что операция подписания документа с помощью средства ЭП логически отделена от операции подтверждения его ключевых реквизитов на "Антифрод-терминале", ЭП документа формируется непосредственно от самого документа, а не от некой структуры, содержащей этот документ (или его хэш) и прочие служебные данные. Это позволяет сохранить для пользователей возможность открывать подписанные документы в наиболее распространённых форматах (PDF, DOCX, TXT и др.) и с помощью любых, в том числе сторонних, средств ЭП убеждаться в том, что они или их контрагенты подписали именно этот документ.

Удобная реализация групповых операций в системах ДБО

Для всех получателей, попавших в "белый список", пользователь подтверждает только одно сводное платёжное поручение. Оно содержит общую сумму платежа в адрес всех получателей, попавших в "белый список", а также число получателей, попавших в "белый список". После этого пользователю останется подтвердить на терминале только те платёжные поручения, получатели которых не попали в "белый список". Такая реализация групповых операций позволяет значительно сократить количество платёжных поручений, которые требуется подтверждать на "Антифрод-терминале".

Быстрое встраивание в прикладные системы

Согласно опыту наших партнёров, встраивание "Антифрод-терминала" занимает около 10 рабочих дней. Для интеграции "Антифрод-терминала" в прикладное ПО подготовлены два типа комплектов разработчика:

- JaCarta SDK — для интеграции в настольные приложения;
- JC-WebClient SDK — для интеграции в Web-приложения с поддержкой всех популярных браузеров на платформах Microsoft Windows, Apple macOS и Linux.

Технические подробности

Параметр	Описание
Размеры (Д × Ш × В), мм	97 × 61.7 × 11
Дисплей	Матричный, 4-х строчный, с возможностью прокрутки до 400 символов
Цвет экрана	Зелёный
Кабель	1.5 м с интерфейсом USB типа A
Интерфейс подключаемой смарт-карты	• 8-ми контактный • Частота до 4 МГц • Поддержка ISO 7816 смарт-карт класса A и B (5V, 3V) • До 200,000 подключений смарт-карты
Клавиатура	• 10 цифровых и 4 функциональных клавиши с эпоксидным нанесением надписей • Надписи устойчивы к 100 000 нажатиям
Интерфейс/разъём подключения терминала к рабочей станции	• USB 2.0 Full-speed (12 Мбит/с) • Разъём USB Type A
Тип электронной подписи	Усиленная электронная подпись по ГОСТ Р 34.10-2001 (устройство не является средством ЭП. С помощью собственной ЭП терминал подписывает собственный журнал операций, а не документ)
Поддерживаемые операционные системы	**Microsoft** • Microsoft Windows 10 • Microsoft Windows 8-8.1 • Microsoft Windows 7 • Microsoft Windows Vista • Microsoft Windows XP **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 **Apple** • OS X 10.11 (El Capitan) • OS X 10.10 (Yosemite) • OS X 10.9 (Mavericks) • OS X 10.8 (Mountain Lion)
Поддерживаемые браузеры	• Google Chrome • Mozilla Firefox • Microsoft Internet Explorer 8-11 • Microsoft Edge • Apple Safari • Opera • Яндекс.Браузер
Поддерживаемые устройства	• **Смарт-карты:** JaCarta-2 ГОСТ, JaCarta ГОСТ, eToken ГОСТ, а также другие смарт-карты стандарта ISO 7816 (по запросу) • **USB-токены:** любые
Поддерживаемые программные СКЗИ	• Любые

Лицензии ФСТЭК России № 0037 и № 0054 от 18.02.03, № 3442 от 10.11.17.
Лицензии ФСБ России № 12632 Н 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: 6014-060917