

Платформа JaCarta

для обеспечения безопасности
в системах ДБО



Сергей Груздев
Ген. директор
Аладдин Р.Д.

Влияние кризиса

2015 г. начался с жёсткого кризиса

- Главная проблема во время любого кризиса - урезание бюджетов и "кризис в головах"
 - Во время экономических проблем и кризисов на рынке всегда обостряются проблемы с ИБ
 - И внешние (хакеры, конкуренты), и внутренние (с персоналом)
 - Что мы видим
 - Первым делом режут невидимые ("неоправданно высокие") затраты на ИБ
 - Запрет на новые проекты (только поддержание существующих)
 - ▶ **Возникает опасная положительная обратная связь**
 - К чему это приведёт
 - К накоплению нерешённых проблем с ИБ
 - После громких инцидентов - будут готовы на всё, лишь бы закрыть проблему (так было после предыдущих кризисов)
 - Уход профессионалов, снижение уровня компетенции
 - ▶ **Выиграют те, кто не стал экономить на ИБ**

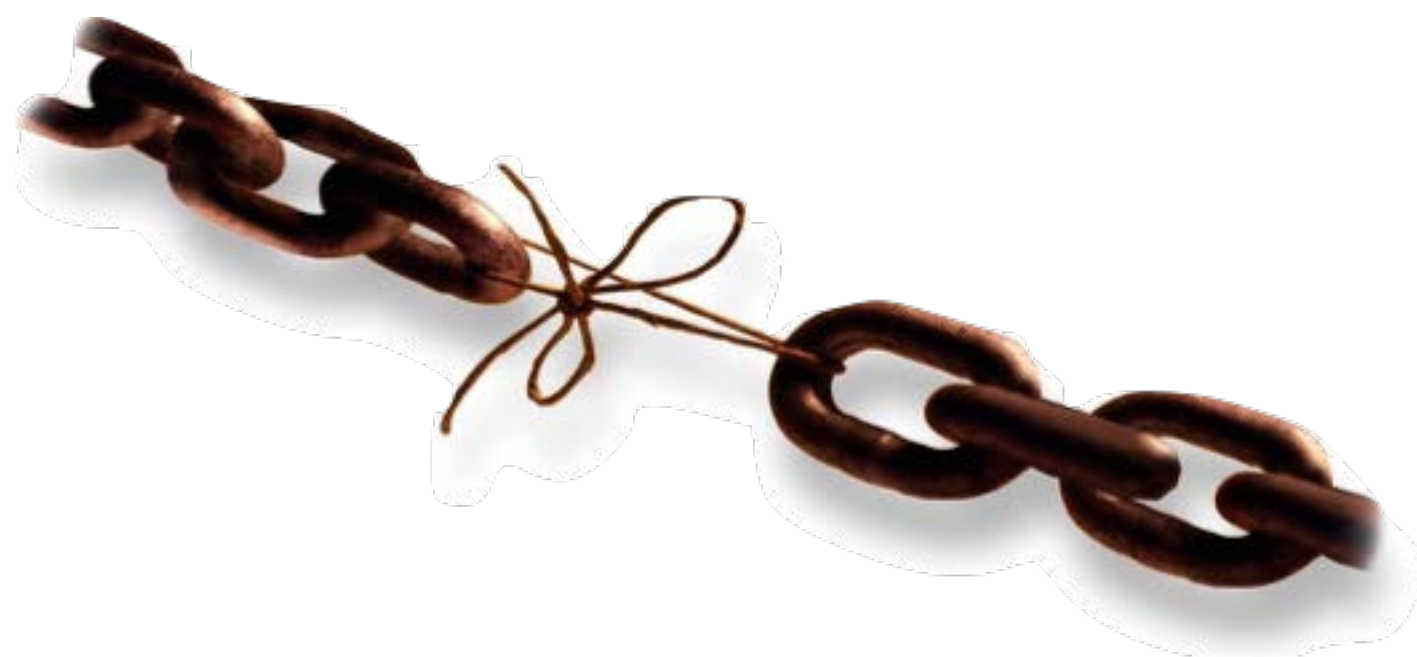


Изменение рынка

- Тенденции, определяющие развитие рынка
 - "Нет денег"
 - Мобильность
 - Многоплатформенность
 - Нужна УКЭП (на смену "А зачем она нужна?")
 - Как бороться с атаками с подменой подписываемого документа?
- Что часто слышим
 - Срезали/заморозили бюджет на ИБ - не на что покупать токены
 - Пользователям не нравится что-то втыкать в компьютер, мы внедряем программные решения
 - Внедрили красивое программное решение, а клиенты ему не доверяют, требуют токен - привыкли
 - Мы нашли эффективное решение:
 - Мобильный программный (виртуальный) токен
 - OTP-генератор в телефоне
 - Считыватель QR-кода (штрих-, динамического и пр.) с платёжной информацией с экрана
 - SMS с одноразовым паролем
 - ЭП на сервере



Вспомним теорию



► Надёжность системы определяется по её самому слабому звену

- Аутентификация и ЭП должны рассматриваться как **единый связанный процесс**
 - Чтобы получить УКЭП (или гарантированное подтверждение транзакции) при удалённой работе необходимо обеспечить **надёжную** аутентификацию клиента
 - ЭП на сервере (в облаке) со слабой аутентификацией?
 - Тип (надёжность) аутентификации напрямую определяет тип ЭП, которую можно получить
 - Простая аутентификация (Логин-Пароль, SMS с кодом) - Простая ЭП
 - Усиленная аутентификация (ОТР, чтение QR-кода с экрана и отображение на телефоне, генерация кода подтверждения и пр.) - Усиленная ЭП
 - Строгая двухфакторная аутентификация (с использованием криптографии) - УКЭП
- Но это справедливо лишь при работе в доверенной среде (включая смартфон)

Средство аутентификации и ЭП само должно быть сделано как безопасное и для целей обеспечения безопасности (Secure by design)

- Нельзя делать токены для обеспечения безопасности на бытовом микроконтроллере, не имеющем специальных средств защиты от клонирования



JaCarta

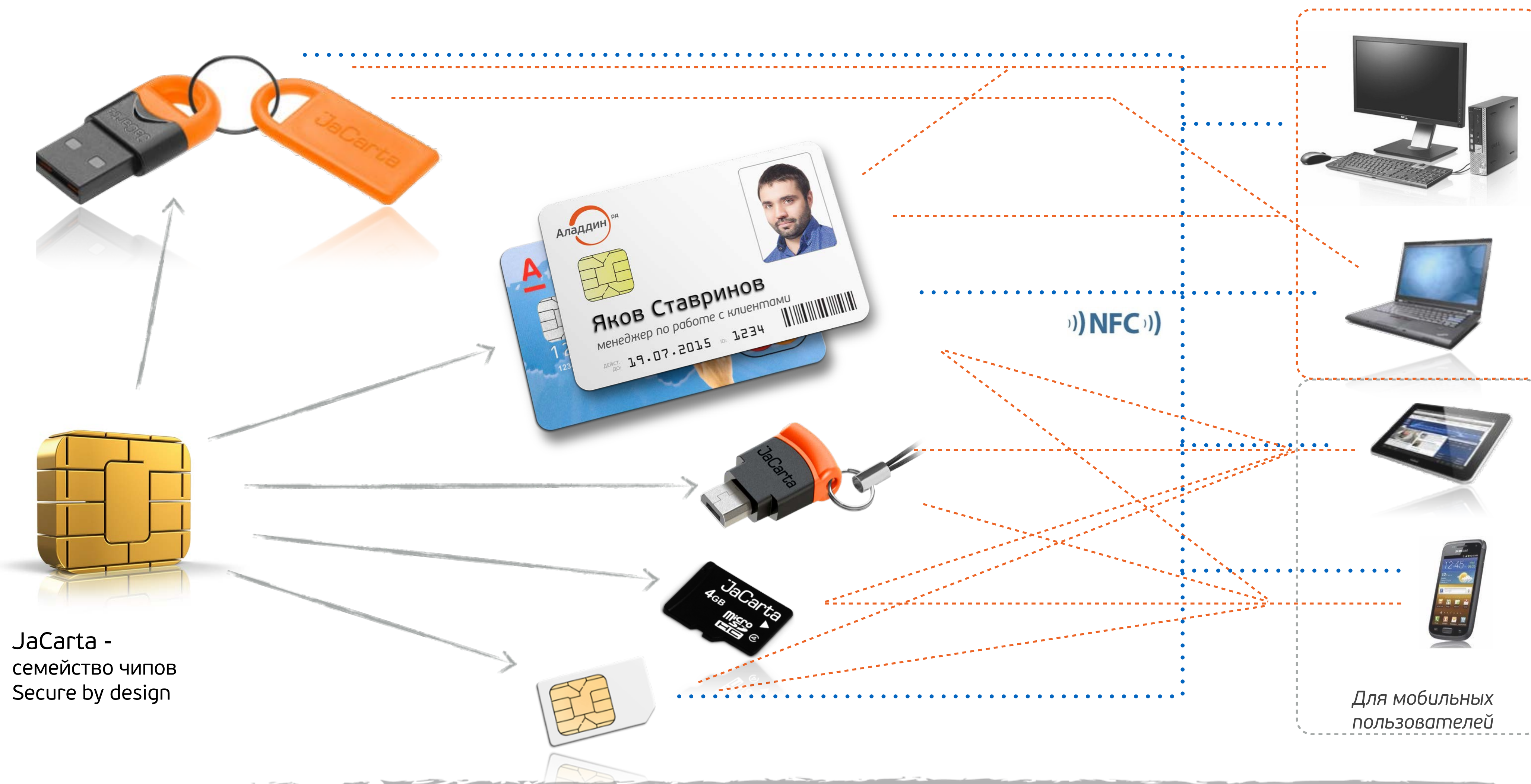
- новая Платформа для обеспечения безопасности

Смена парадигмы

- Рынок и потребности изменились - нужна смена парадигмы
 - Было: eToken - один универсальный ключ для всего
 - Стало: JaCarta - оптимальное решение для каждого сегмента, для каждого сценария использования, для разных критериев выбора
- JaCarta
 - Наш собственный российский продукт, технологически уже обогнал eToken на 3-4 года, активно развиваем его
 - Разработан с использованием лучших западных технологий (Java Card), на базе новейших чипов и лучших практик
 - Не просто линейка продуктов, а Платформа, на базе которой строится некая экосистема, включающая:
 - Централизованную систему управления (JMS)
 - Решения для мобильных пользователей, для Web-порталов и облачных сервисов
 - Решения для безопасной работы из недоверенной среды (второй доверенный канал - ЭП на SIM, и Антифрод-терминал)



JaCarta для ДБО



Ключевые особенности



- Сертификат ФСБ России на "Персональное средство ЭП", полностью соответствующее требованиям 63-ФЗ и 796-го Приказа ФСБ России
 - Сделано по новым требованиям ФСБ как функционально законченное безопасное изделие, не требуется "корректность встраивания"
 - ▶ Все другие средства (на сегодня) - для использования в автоматизированных системах без участия человека
 - Это может быть большой проблемной зоной при разборе конфликтных ситуаций у клиента (отложенная проблема)
- Более удобная и надёжная конструкция USB-токена
 - Оптимальный размер (ниже риск сломать, но сложно забыть в компьютере)
 - Металлический разъём заменён на пластиковый - защита от статики в 3 раза выше (до 15 КВ)
- Единый API для встраивания в ДБО для всех форм-факторов, преемственность с eToken
- Новый токен с MicroUSB для планшетов и смартфонов (как более дешёвая альтернатива Secure MicroSD)
- Даём решение для работы с порталными и облачными сервисами
 - При использовании УКЭП пользователю не надо ничего устанавливать на свой компьютер
- Ниже долларовая составляющая
 - ▶ За полгода планируем провести полную миграцию на JaCarta

Платёжные карты с ЭП

Объединение в одной карте двух функций

- Платёжная карта (MasterCard, VISA, ПРО100*)
 - Аладдин получил EMVCo сертификат и статус "Чип-вендор"
 - Сертификация в OpenWay (заканчивается)
- Средство идентификации, строгой двухфакторной аутентификации и УКЭП
 - Полный функциональный аналог USB-токенов JaCarta и eToken ГОСТ
- Что это даёт
 - Удешевление проекта (платёжная карта и карта для ДБО в "одном флаконе")
 - Надёжная идентификация клиента для удалённого обслуживания
 - Снижение нагрузки на доп. офисы
 - Возможность продажи доп. услуг и сервисов
 - Клиент ответственнее относится к своему средству ЭП
 - Возможность использования единой технологии и для юрлиц, и для физлиц
 - Безопасная работа в **недоверенной среде** (при использовании Антифрод-терминала)



Антифрод-терминал

Смарт-карта клиента



Предназначен

- Для защиты от большинства известных атак на клиентов ДБО, включая:
 - удалённое управление компьютером "жертвы"
 - в том числе с "пробросом" USB-порта, к которому подключен USB-токен или ридер со смарт-картой, на компьютер злоумышленника
 - атаки с подменой подписываемых документов (когда пользователь набирает на клавиатуре и видит на экране одну информацию, а подписывает другую)

Позволяет

- Безопасно и удобно подписывать как одиночные, так и групповые документы, создавать и вести "белые списки", оперативно подтверждать сомнительные операции
- Снять суточные лимиты на проведение операций через интернет-банкинг

Обеспечивает

- Формирование доказательной базы, необходимой при расследовании инцидентов (ст. 9 Закона о НПС)

Реализована

- Новая технология аутентификации терминала и выполняемых транзакций:

SWYX - "Подписываю всё, что выполняю"

Как работает

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 №2077 22.01.2014 Электронный
Дата Вид платежа

ИНН 7719165935	КПП 771601001	Сумма	238,000.00	
ЗАО "Аладдин Р.Д."		Сч. №	407.02.810.4.0002.1087822	
Платательщик		БИК	044525787	
ОАО "Уралсиб"		Сч. №	301.01.810.1.0000.0000787	
Банк плательщика		БИК	044525225	
ОАО БАНК "ВОЗРОЖДЕНИЕ"		Сч. №	301.01.810.5.0000.0008933	
Банк получателя		Сч. №	407.02.810.5.0000.0008933	
ИНН 7710140679	КПП 775000856	Сч. №		
ООО "Мажторг"		Вид оп.	01	Срок плат.
		Наз оп.		Очер. плат.
		Код		Рез. поле
3				
За оборудование				
Назначение платежа				





Спасибо

Будь собой в электронном мире!

Контакты:

Сергей Груздев

www.aladdin-rd.ru

+7 (495) 223-0001

s.gruzdev@aladdin-rd.ru



Будь собой в электронном мире!

Данный документ, включая подбор и расположение иллюстраций и материалов в нём, является объектом авторских прав и охраняется в соответствии с законодательством Российской Федерации.

Обладателем исключительных авторских и имущественных прав является ЗАО "Аладдин Р.Д.". Использование материалов из данного документа любым способом без письменного разрешения правообладателя запрещено и может повлечь ответственность, предусмотренную законодательством РФ.

Информация, приведённая в данном документе, предназначена исключительно для ознакомления и не является исчерпывающей.

Состав продуктов, компонент, их функции, характеристики, версии, внешний вид, доступность и пр. могут быть изменены компанией "Аладдин Р.Д." без предварительного уведомления.

Все указанные данные о характеристиках продуктов основаны на международных или российских стандартах и результатах тестирования, полученных в независимых тестовых или сертификационных лабораториях, либо на принятых в компании методиках.

В данном документе компания "Аладдин Р.Д." не предоставляет никаких ни явных, ни подразумеваемых гарантий.

Владельцем товарных знаков Аладдин, Aladdin, JaCarta, логотипов и правообладателем исключительных прав на их дизайн и использование, патентов на соответствующие продукты является ЗАО "Аладдин Р.Д.".

Названия других технологий, продуктов и компаний, упоминающиеся в данном документе, могут являться товарными знаками своих законных владельцев.

Сведения, приведённые в данном документе, актуальны на дату его публикации.

При перепечатке и использовании данных материалов либо любой их части ссылки на "Аладдин Р.Д." обязательны.

© 1995-2015, ЗАО "Аладдин Р.Д." Все права защищены.

Лицензии ФСТЭК России № 0037, № 0054, № 2874

Лицензии ФСБ России № 12632Н, № 24530

Сертификат соответствия системы управления качеством СМК ГОСТ Р ИСО 9001-2011

№ РОСС RU.ИС72.К00079 от 29.07.14



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

Приведённая информация актуальна по состоянию на 1 февраля 2015 г.