

# Применение биометрии в системах безопасности

Февраль 2017

Пшеннов Дмитрий

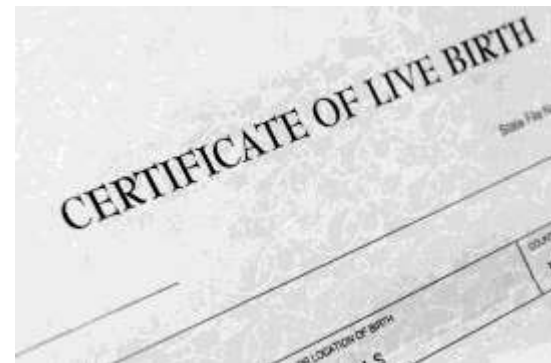
FUJITSU

shaping tomorrow with you

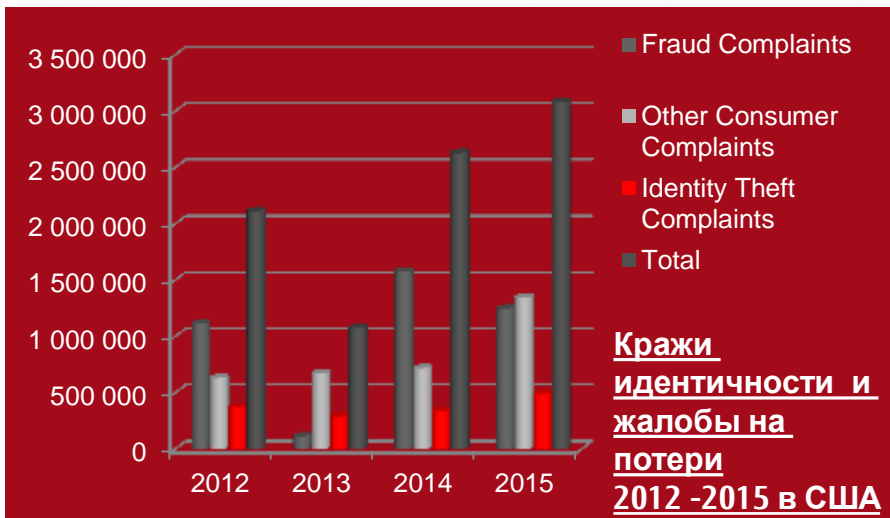
Human Centric Innovation

*Driving Digital Transformation*

- Каждое существо уникально и имеет свою индивидуальную идентичность
  - Все начинается тогда, когда родители дают нам идентичность при рождении
  - Наш первый документ идентичности – свидетельство о рождении if birth
  - Позже мы получаем свой первый паспорт
  - А еще позже идентифицируем себя вклеиванием фотографий в него
  - Но также мы используем другие документы и инструменты в течение жизни:
    - Водительское удостоверение, страховое свидетельство, платежные карты, карты лояльности, имя входа в компьютер, e-mail, экаунты в социальных сетях, банковские счета, экаунты в онлайн магазинах, ИНН и т.д., и т.п.



# Это реальность...



Source: Federal Trade Commission, Consumer Sentinel Network, 2016

- 15 млрд US\$ украдено у 13,1 млн граждан США
- 112 млрд US\$ украдено с помощью краж идентичности за последние 6 лет
- Кражи идентичности выросли более, чем на 47% с 2014



- Так как кредитные карты в США стали более защищенными, воры используют создание и злонамеренное использование новых счетов
- Многие кражи идентичности осуществляются с использованием персональной информации, собранной ворами в Интернете

# Как защитить свою идентичность?

- Паспорта и идентификационные карты, использующие возможности биометрии
- Ежедневное использование компьютеров, планшетов и смартфонов для входа в Интернет, выполнения операций и действий, требующих идентификации
- Мы используем PINы, жетоны, смарткарты, пароли, образы для того, чтобы обезопасить свое имя, представляющее нашу идентичность
- Мы пытаемся обеспечить большую безопасность использованием многофакторности, но...



# Необходимость в биометрической аутентификации



- Ничего не потеряется
- Ничего не будет передано незаконно
- Ничего не будет забыто «дома»
- Ничего не будет украдено
- Никаких компромиссов в идентификации – никаких злоупотреблений
- Быстрая обработка
- Быстрый ROI – низкое TCO
- Обеспечение мультифакторности
- Минимизация стоимости поддержки



# Необходимо создавать надежный IAM с использованием биометрии

**Identity Access Management – это не продукт, это РЕШЕНИЕ**



**IAM начинается с идентификации, но после этого включает пути взаимодействия с доступными ресурсами**

- **Бизнес:**
  - Определение процессов IAM: права доступа, уровни защиты, защищаемые зоны, создание метадиректориев
- **Технологии:**
  - Создание интерфейса различных приложений и платформ для взаимодействия
- **Управление доступом:**
  - Определение ролей / групп доступа
  - Определение процесса аутентификации
  - Определение управления идентификацией
  - Определение внешнего управления доступом

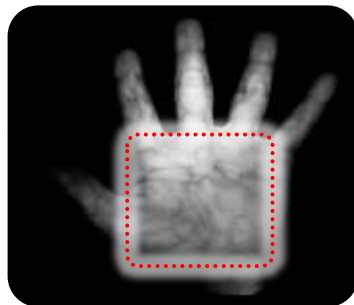
## 1 Безопасность

- Вены расположены глубоко под кожей
- Уникальный рисунок
- Не меняется на протяжении всей жизни
- Необходимость движения крови для работы технологии



## 2 Точность

- Биометрический шаблон формируется по 5 миллионам контрольных точек
- Вены в ладони проще обнаружить, чем капилляры в пальцах
- Нет чувствительности к окружающей обстановке



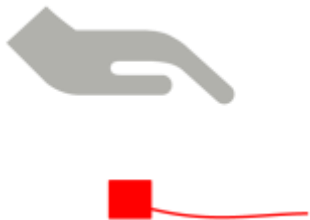
## 3 Применяемость

- Гигиеничность
- Интуитивное использование
- «Ключ» спрятан под кожей

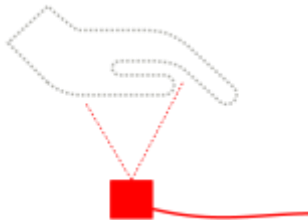




Позиционирование  
руки над сенсором



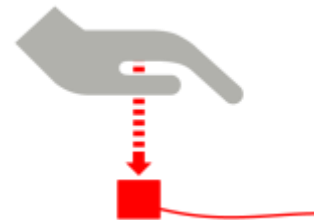
Фокусировка и  
детекция пульсаций



Сканирование



Запись рисунка вен



Сохранение  
биометрического  
шаблона



Преобразование в  
биометрический шаблон,  
формирование индивидуального  
ключа, шифрование

h3 9d j1 9f 0q o2 09 s0 1011010010101000



Передача на ПК

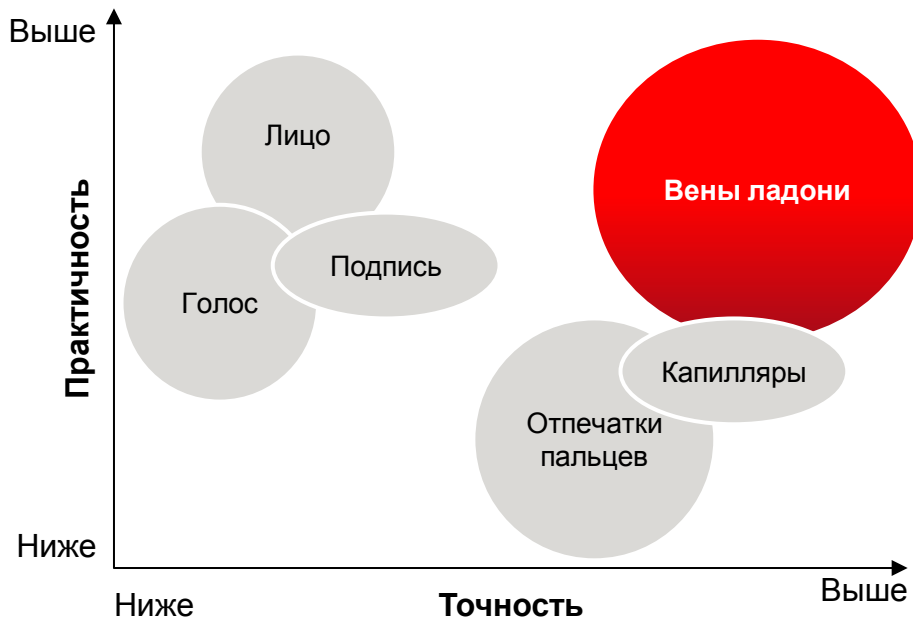


101011010010101000

Шифрование



# Точность Fujitsu PalmSecure



Метод	FAR* (%) =	FRR** (%) =
Распознавание лица	~ 1.3	~ 2.6
Распознавание голоса	~ 0.01	~ 0.3
Отпечатки пальцев	~ 0.001	~ 0.1
Капилляры в пальцах	~ 0.0001	~ 0.01
<b>Вены ладони</b>	<b>&lt; 0.00008</b>	~ 0.01

\*FAR (False Acceptance Rate) — процентный порог, определяющий вероятность того, что один человек может быть принят за другого (коэффициент ложного доступа)

\*\*FRR (False Rejection Rate) — вероятность того, что человек может быть не распознан системой



**Fujitsu PalmSecure – один из самых точных методов аутентификации.**

# Сравнение методов биометрии

	Вены ладони	Отпечаток пальца	Радужная оболочка глаза
Точность аутентификации	Отлично	Хорошо	Хорошо
Количество ошибок	Очень мало	Много	Средне
Скорость аутентификации	Очень быстро	Медленно	Быстро
Уязвимость к подлогу	Очень низкая	Высокая	Высокая
Прочность сенсора	Очень хорошая	Удовлетворительная	Очень хорошая
Чувствительность к внешним факторам	Очень низкая	Очень высокая	Очень высокая



OEM сенсор



PC login



Сенсор USB Guide Kit



Подставка под руку



USB stick



Сенсор USB Guide Kit



PalmSecure ID Access

## Workplace Protect

- Аутентификация Microsoft Windows® с помощью PalmSecure
- Автоматический лог-ин в Microsoft Windows®
- Поддержка Windows 7, Windows 8, Windows 10
- Предустанавливается на клиентские системы

## Workplace Protect Manager

Workplace Protect Manager : решение для администраторов

Централизованное управление:

- Стандартная аутентификация PalmSecure, SmartCard, ...
- Предзагрузочная аутентификация на уровне БИОС
- Централизованное безопасное хранилище логинов и паролей

S26361-F2727-L770 Workplace Manager - Client License



## ПО bioLock

Управление и мониторинг приложений SAP, в т.ч. с требованием повторной аутентификации

Единственное биометрическое приложение SAP – сертифицировано SAP!

Настраивается на экран в целом и на поля

- Данные не пересылаются!
- Высочайший уровень безопасности SAP!
- Powered by Realtime US

## Безопасное использование приложений SAP

- Защита от краж
- Управление данными
- Контроль авторизации финансовых транзакций
- Контроль входа и мониторинг транзакций SAP
- Индивидуальная защита процессов, например:
  - Финансовые транзакции
  - Персональные данные
  - Список покупателей



# Пример использования в России

## ■ Встроенные PalmSecure

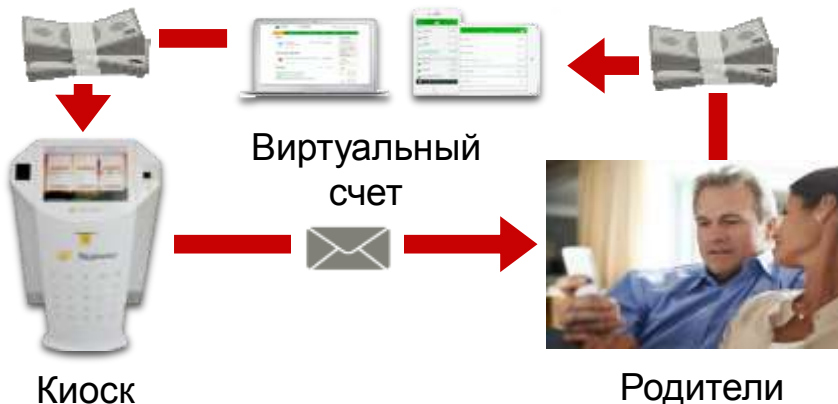
1-я фаза: установка в 100 школах / >60,000 учеников

## ■ Сервис – безналичные платежи

Оплата еды в столовой/кафетерии

## ■ Преимущества

- Бесконтактные безналичные платежи
- Короткие очереди и повышенная безопасность
- Родители знают, что ребенок ел на обед





## **Дмитрий Пшеннов**

Менеджер по развитию бизнеса решений для ритейла и безопасности  
в России, Fujitsu Россия и СНГ

E-mail: [Dmitry.Pshennov@ts.fujitsu.com](mailto:Dmitry.Pshennov@ts.fujitsu.com)

Телефон: +7 985 3645395

The logo features a red infinity symbol positioned above the word "FUJITSU". The word "FUJITSU" is rendered in a bold, red, serif typeface. The infinity symbol is a simple, continuous loop.

shaping tomorrow with you