



Защита банковских транзакций

Андрей Тархов
Руководитель отдела
внедрения и техподдержки
Rainbow Security

О ком пойдет речь



Комплексная сетевая безопасность

Entrust

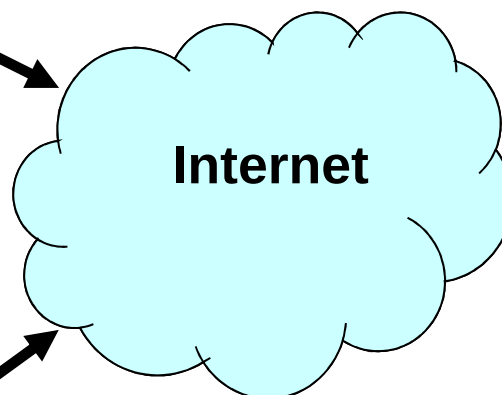
Предотвращение мошеннических операций для online приложений

Actividentity

Аутентификация и управление данными аутентификации



Решения для обеспечения сетевой безопасности компании



Процессинговый центр



WSM



ENTRUST TransactionGuard

Предотвращение мошеннических операций для online приложений

Обнаружение



- Мониторинг всего трафика в реальном времени.
- Анализ на наличие атрибутов в черных списках (база знаний OFIN)
- Анализ расхождения с «нормальным» поведением пользователя
- Комплексная оценка риска для каждой транзакции

Защита



- Автоматическое предотвращение операций с высоким риском
- В сложных случаях аналитик «погружается» в детали предупреждения
- Повторная аутентификация для подтверждения (IdentityGuard, 4TRESS AS)
- Оповещение клиента и выяснение легитимности операции

Адаптация (к новым видам мошеннических операций)



- Постоянное обновление репутационных данных (IP адреса и др.)
- Правила для анализа транзакций поступают из OFIN
- Возможность самостоятельного создания и редактирования правил
- Распределение нагрузки между аналитиками по обработке подозрительных транзакций

4TRESS Authentication Server

4TRESS Authentication Server – это Многоканальная платформа аутентификации, авторизации, управления аутентификаторами и аудита

Реализация:

Программная платформа

Программно-аппаратный комплекс (appliance)

В2С (ритейл):

- CO-OP более 2М пользователей
- SwedBank около 2М пользователей (2007 г.)
- Nordea Bank более 700 000 пользователей
- BNP Paribas 300К пользователей (пилот), всего 5М
- Deutsche Bank более 60 000 пользователей
- First National Bank более 30 000 пользователей

В2В (АБС: ритейл, корпоративные клиенты):

- Zaba Banka 100 000 пользователей
- ABN AMRO более 60 000 пользователей (пилот)
- Allied Irish Bank более 30 000 пользователей
- Caisse des Dépôts более 20 000 пользователей

В2Е (для внутреннего использования)

- | | | |
|-------------------|--------------|-----------------|
| • Crédit Agricole | Commerzbank | Bank of Ireland |
| • SwedBank | Lloyds TSB | PKO BP |
| • Barclays Bank | BSI ABN AMRO | |

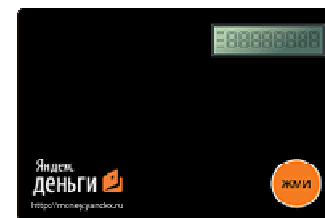
Российская действительность



Бизнес требования

Увеличение доходов / доли рынка

- Привлечение клиентов за счет дополнительных сервисов
- Улучшение репутации / конкурентные преимущества
- Рост известности брэнда (логотип на выпущенных устройствах)



Снижение рисков и стоимости

- Снижение рисков от мошенничества, повреждения репутации.
- Перевод пользователей на не дорогие онлайн-сервисы (каналы)
- Низкая стоимость техподдержки



Требования «регулирующих» организаций

- US/EU: FFIEC, SOX, PCI DSS и т.д.



Гибкий маркетинговый подход

Ориентация на сервисы и сегментацию клиентов

- Различный уровень сервисов с различными уровнями безопасности
- Сегментация основана на уровнях транзакций



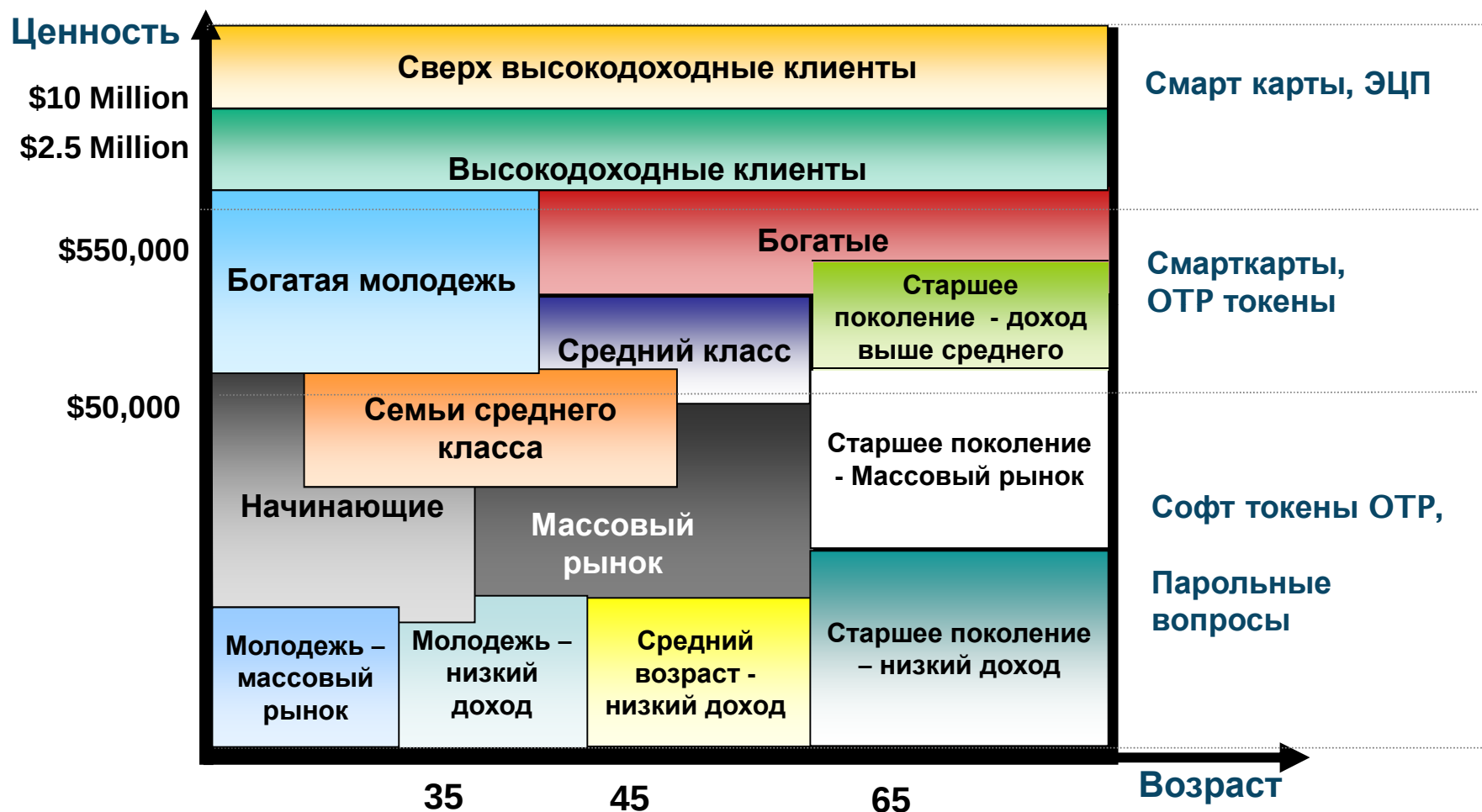
Почем «безопасность» для клиентов

- Бесплатно
- Токены предлагаются в комплекте с банковскими картами
- Ежемесячная или ежегодная плата включается в дополнительные сервисы
- Клиент платит за токены





Сегментация клиентов для определения потребностей ОДИН «РАЗМЕР» ДЛЯ ВСЕХ НЕ ПОДХОДИТ....



Канально-ориентированная структура

Особенности аутентификации в канально-ориентированных системах

Для каждого канала:

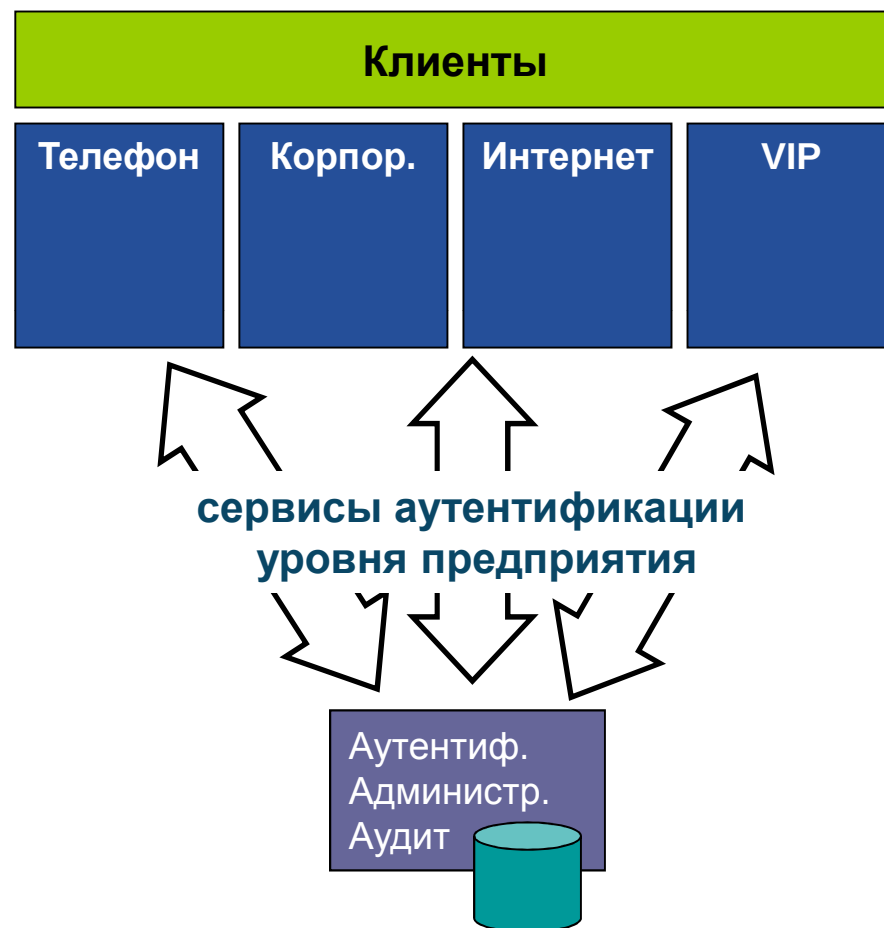
- своя система аутентификации, со своими особенностями
- процессы аутентификации и парольные политики сильно отличаются
- свои особенности управления и поддержки - > \$
- базовая функциональность уникальна для каждого канала
- множество точек компрометации



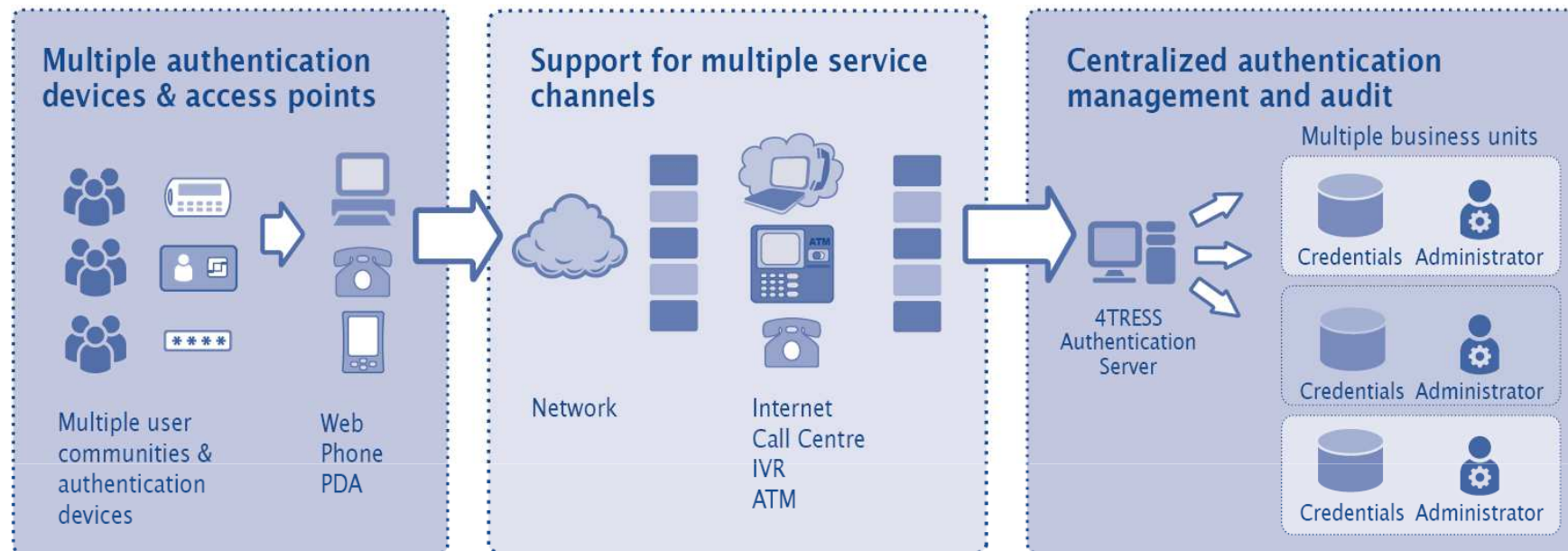
Мультиканальная инфраструктура

Мульти-канальная инфраструктура аутентификации

- Аутентификация клиентов не зависимо от канала
- Единый интегрированный набор сервисов аутентификации, управления и аудита
- Простая и явная модель, усиливающая безопасность за счет уменьшения точек компрометации
- Снижение стоимости управления и поддержки
- Поддержка новых каналов
- Расширение схем аутентификации, не влияя на каналы



4TRESS AS - кратко о возможностях



- Аутентификация клиентов в различных точках доступа/ сервисных каналах
- Поддержка широкого перечня методов и схем аутентификации
- Управление учетными данными пользователей
- Управление жизненным циклом устройств (выпуск, отзыв, синхронизация)
- Авторизация ценных транзакций
- Защищенный от вмешательства журнал аудита
- Полное разделение данных в зависимости от различных направлений бизнеса
- Защищенность, высокая масштабируемость, «гибкая» архитектура.

4TRESS AS - необходимые методы

По материалам исследований Gartner Group

Что требуется банкам ?

Обязательна поддержка OTP (EMV CAP и/или Oath)	✓
Закрытые алгоритмы – обязательное требование	✓
PKI Аутентификация	✓
Возможность подключения механизмов аутентификации сторонних производителей	✓

Структура сервера



Аутентификация (OTP- генераторы)

- OATH
 - Время
 - Событие
- Проприетарные
 - Событие
 - **Время и событие**
- Запрос-ответ
- Подпись транзакций (MAC)



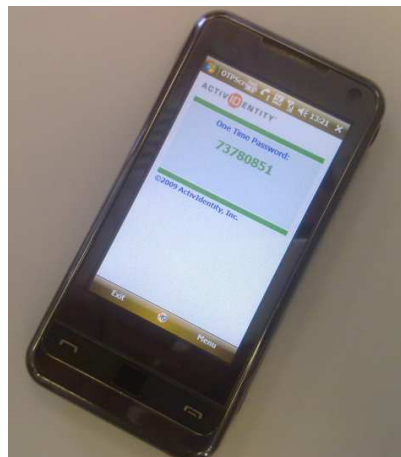
Выбор подходящего метода аутентификации – верный способ сохранения и увеличения числа клиентов и прекрасная возможность защитить репутацию компании

- EMV (первое в мире решение, сертифицированное MasterCard)
- PKI



Аутентификация

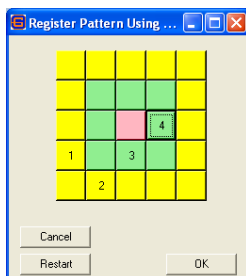
- OTP через SMS
- Mobile
 - Java
 - Microsoft Mobile
 - iPhone
 - Blackberry
- Web
- PC



- Пароли
- Секретные вопросы

Новые методы аутентификации

Расширяемость - схемы, методы, устройства



Gridsure

- Пользователь вводит учетную информацию путем выбора ячеек в таблице, исходя из пользовательских правил и шаблонов



Устройства сторонних производителей

- Поддержка проприет. алгоритмов других вендоров



Yubico

- не дорогие подключаемые устройства



Matrix Cards

- Пользователь вводит код из матрицы значений



Out of Band

- голосовая внеканальная аутентификация

Управление ПДА и устройствами



- Загрузка устройств и «привязка» к пользователям
- Включение/выключение ПДА
- Статистика использования
- Синхронизация генераторов и разблокировка PIN
- Отзыв и перевыпуск устройств
- Канально-ориентированные правила
- Защищенная отсылка PIN и паролей
- Система формирования запросов

**Управление различными типами ПДА и устройств,
полностью контролируя их жизненный цикл**

Авторизация и прочие тонкости

- Связанные методы
- Автоматический выбор метода по правилу (сумма, лимит)
- По каналу
- Управление сессиями
- Интеграция с системами управления риска
- Обслуживание как внешних, так и внутренних клиентов



- Защищенный аудит
- Управление с помощью готовых порталов и интеграция с внешними системами
- Кратчайшее время внедрения при использовании программно-аппаратного комплекса

Вопросы?



СПАСИБО ЗА ВНИМАНИЕ

129343, МОСКВА, ПРОЕЗД СЕРЕБРЯКОВА,
Д. 14, СТР. 10, БИЗНЕС-ЦЕНТР "SILVERSTONE"
+7 (495) 66 323 66

WWW.RAINBOW.MSK.RU
SECURITY@RAINBOW.MSK.RU