Технологии создания доверенной среды аутентификации клиентов и их транзакций

Евгений Чугунов

CISA, CISSP, PCI QSA

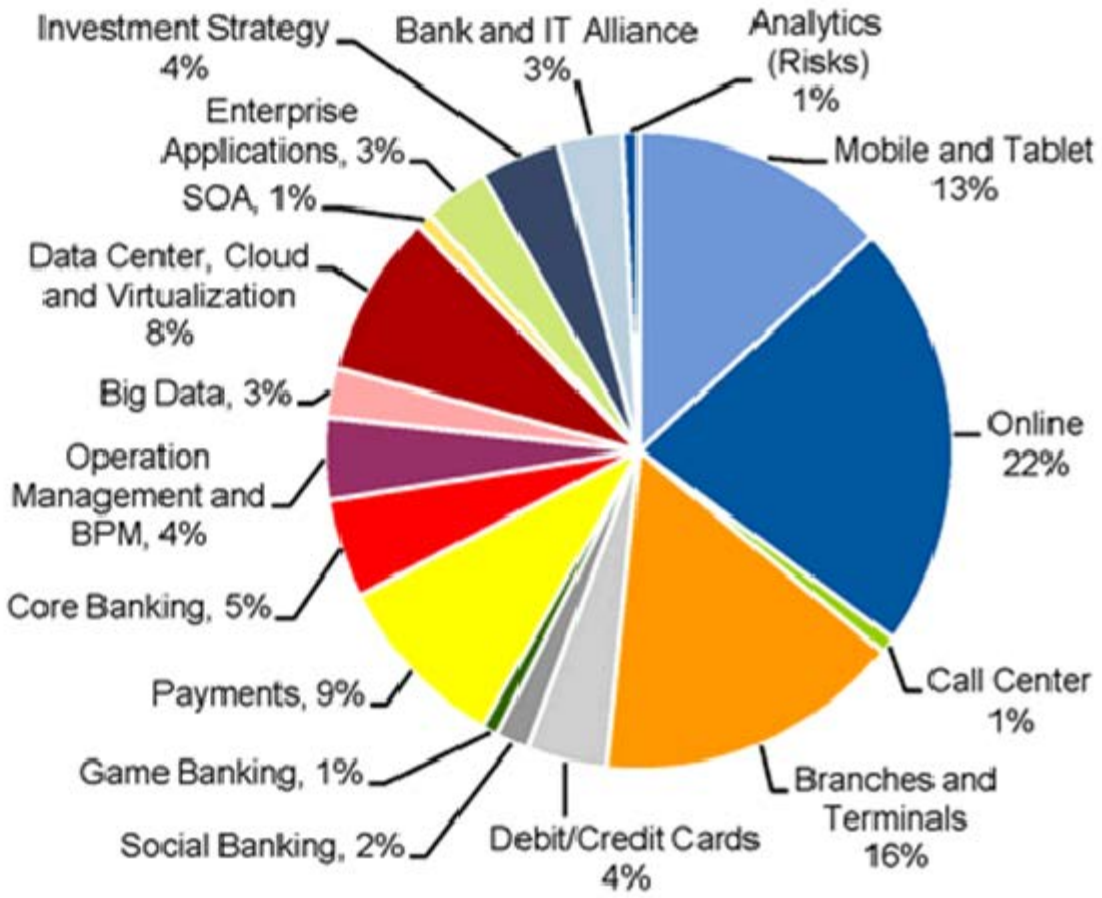
Эксперт
компании КРОК

Москва, 05.02.2013

КЛИЕНТЫ МЕНЬШЕ ХОДЯТ, БАНКИ БОЛЬШЕ ИНВЕСТИРУЮТ В ДИСТАНЦИОННЫЕ СЕРВИСЫ

КРОК

Customer Experience and Channels
Mobile Banking
Online Banking
Call Center
Branches and Terminals
Debit/Credit Cards
Social Banking
Game Banking
Payments
Payments
Core Applications and Architecture
Core Banking
Operation Management and BPM
Big Data
Data Center, Cloud and Virtualization
SOA
Enterprise Applications
IT Strategy
Investment Strategy
Bank and IT Alliance
Risk and Regulation
Analytics (Risks)

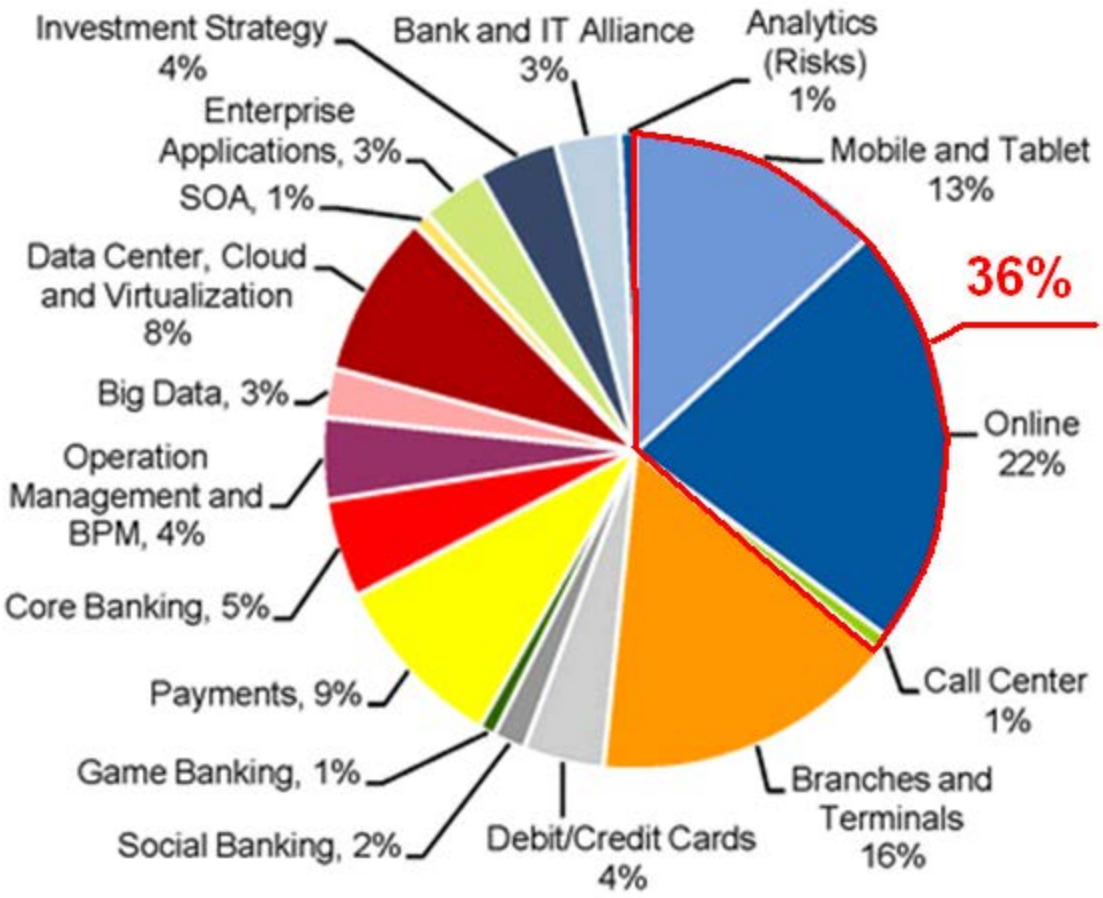


Источник Gartner «Top Japanese Banks: IT Plans and Investments, 2011 and 2012 »

КЛИЕНТЫ МЕНЬШЕ ХОДЯТ, БАНКИ БОЛЬШЕ ИНВЕСТИРУЮТ В ДИСТАНЦИОННЫЕ СЕРВИСЫ

КРОК

Customer Experience and Channels
Mobile Banking
Online Banking
Call Center
Branches and Terminals
Debit/Credit Cards
Social Banking
Game Banking
Payments
Payments
Core Applications and Architecture
Core Banking
Operation Management and BPM
Big Data
Data Center, Cloud and Virtualization
SOA
Enterprise Applications
IT Strategy
Investment Strategy
Bank and IT Alliance
Risk and Regulation
Analytics (Risks)



Источник Gartner «Top Japanese Banks: IT Plans and Investments, 2011 and 2012 »

ТРЕНДЫ РАЗВИТИЯ И ФАКТЫ – ДБО ТРЕНД

КРОК

1. Повышение мобильности клиентов

   Отчет Google: Global Business Map

   162% проникновение мобильных телефонов

   25% из них смартфоны

   28% телефонов используются для мобильного интернета

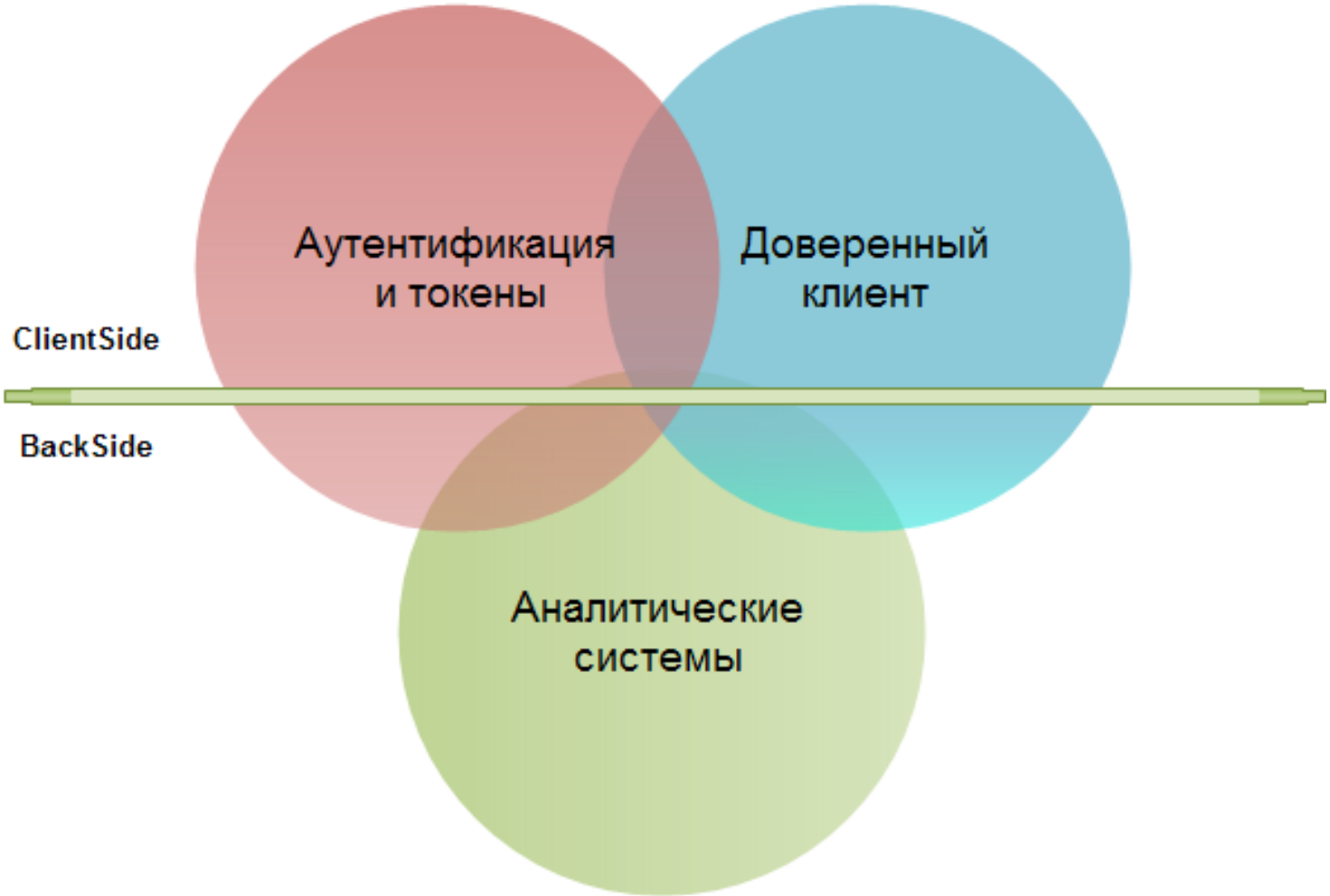
2. Дематериализация каналов связи
   - Экономическая выгода в сравнении с материальным офисом
   - Снижение затрат клиентов, клиент не любит ходить
   - Большая доступность услуг, как следствие ускорение бизнеса
   - Необходимо быть современным
3. Диверсификация продуктов и большая фокусировка на клиенте

РЕАЛЬНЫЕ УГРОЗЫ РЕАЛЬНОГО МИРА

… В УСЛОВИЯХ ОТСУТСТВИЯ ДОВЕРИЯ

ТЕХНОЛОГИИ ЗАЩИТЫ ДБО

КРОК



ЦЕЛЬ ЗАЩИТЫ ДБО

Перехват информации и управления не должны дать злоумышленнику завладеть счетом клиента

ВЫБОР МЕТОДА И СПОСОБА АУТЕНТИФИКАЦИИ

КРОК

1. Использование двухфакторной аутентификации и одноразовых паролей

   Перехват логинов и паролей ничего не даст злоумышленнику в будущем

2. Обеспечение более доверенной среды подтверждения транзакций, чем место совершения транзакции

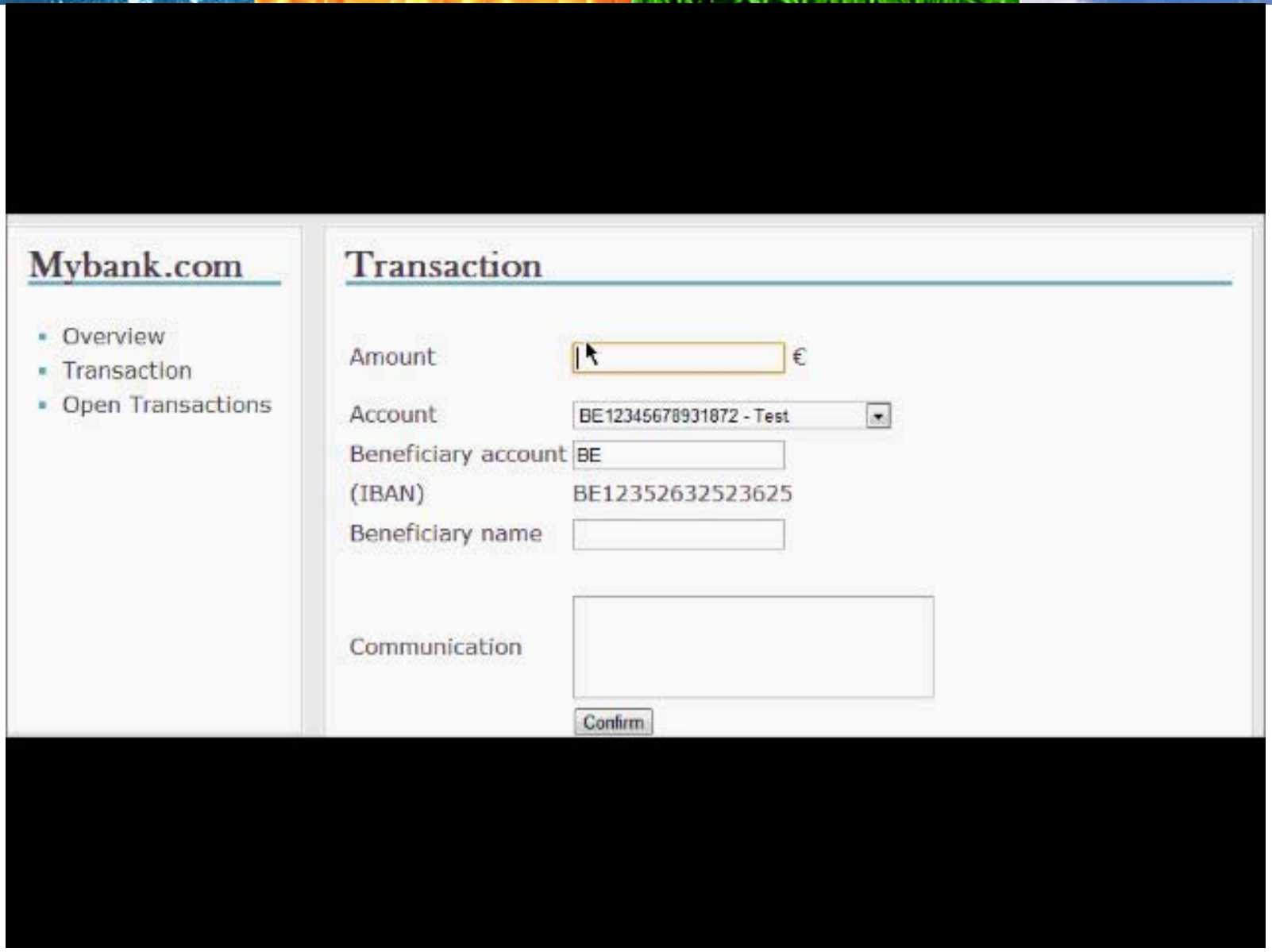
   Злоумышленник не сможет манипулировать параметрами транзакции сейчас

3. Адаптивная аутентификация

   Что бы не стрелять из пушки по воробьям. Динамический выбор подходящего метода и способа аутентификации в зависимости от выявленных риск факторов

ПРИМЕР: ПОДТВЕРЖДЕНИЕ ТРАНЗАКЦИИ. ВТОРОЙ ФАКТОР + ДОВЕРЕННАЯ СРЕДА

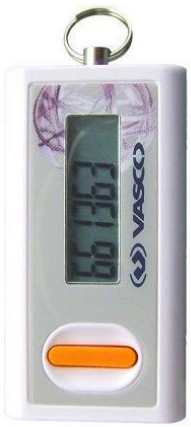
КРОК



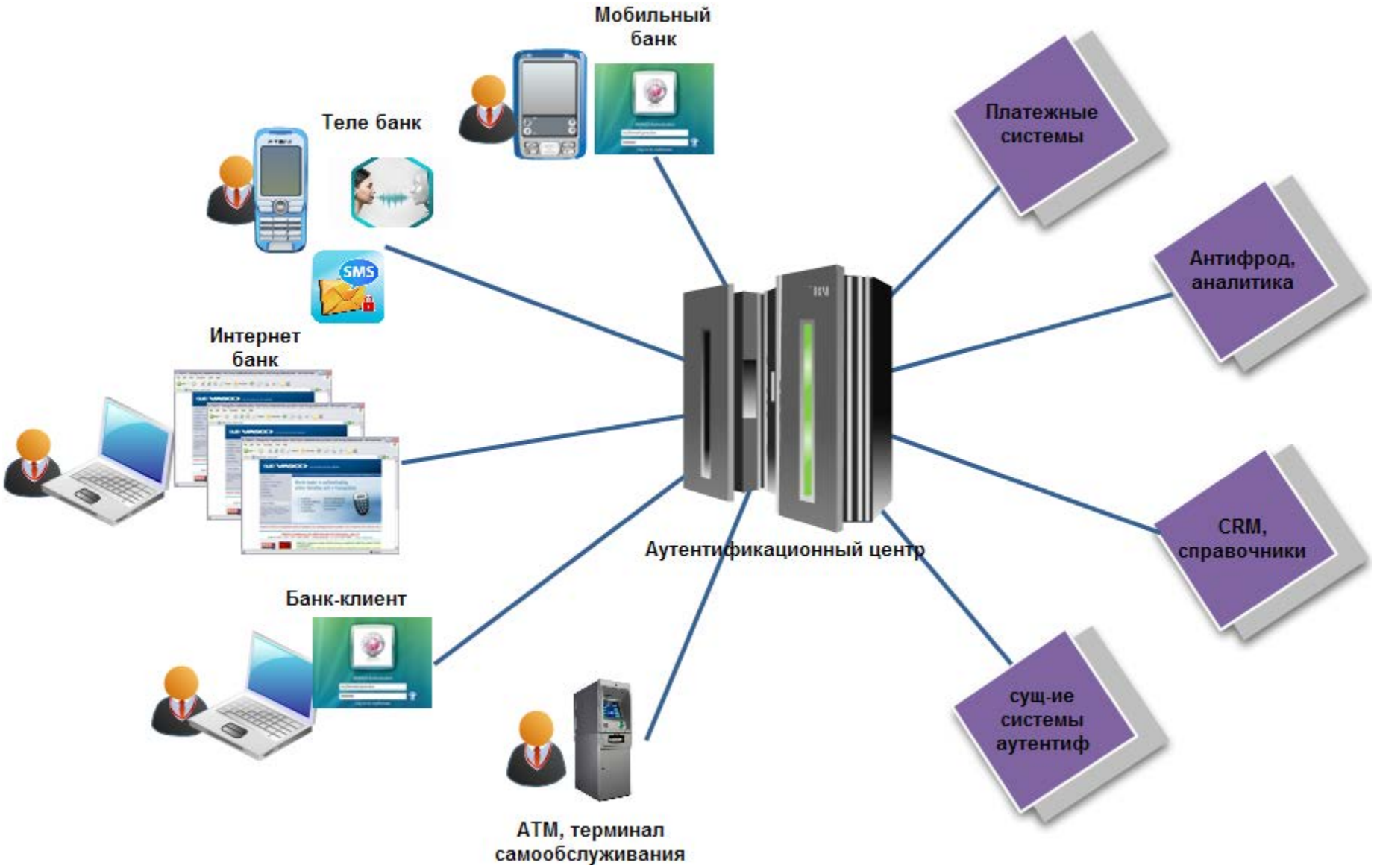
ВИДЫ АБОНЕНТСКИХ УСТРОЙСТВ

Второй фактор аутентификации пользователи могут получить через:

- sms или иной альтернативный канал связи;
- аппаратный/мобильный mac-токен;
- ридер банковских карт (криптокалькулятор)
- TrustScreen



АУТЕТИФИКАЦИОННЫЙ ЦЕНТР ИЗНУТРИ



КРАТКОЕ РЕЗЮМЕ

1. Аутентификационный центр – интеграционный проект
   - Каждый канал требует своих подсистем аутентификации
   - Множество каналов требует управления и координации
   - Необходимо подключение к существующим системам
   - Из коробки не работает
2. Аутентификационный центр – единая платформа для всех приложений
   - Замена и дополнение существующих подсистем аутентификации
   - Быстрое и единообразное добавление новых методов
   - Для последующих систем подсистема аутентификации не требуется
   - Снижение стоимости внедрения последующих систем
3. Это сервис – внутренний или внешний

ТИПИЧНЫЙ ПРОЕКТ 2FA/FRAUD MONITORING

КРОК

Подход КРОК

Этап	Результат
Обследование	Отчет с деталями работы инфраструктуры и подключаемых систем
Проектирование	Спецификация интерфейсов, форматов, логистика средств защиты
Развертывание	Работающий ландшафт аутентификационного центра
Модификация подключаемых систем	Новые версии систем ДБО, работающие через аутентификационный центр
Пилотный запуск	Новая версия с исправленными ошибками и недочетами
Реальный запуск	Полностью работоспособная система, обеспечивающая новый уровень защиты
Сопровождение	Стабильность работы

КАРТА УСЛУГ КРОК

КРОК

Защита системы дистанционного банковского обслуживания (ДБО)

Контроль и мониторинг работы пользователей в АБС

Борьба с мошенничеством (внедрение систем класса anti-fraud)

Соответствие требованиям (Compliance Management)

http://www.croc.ru/security/

СПАСИБО ЗА ВНИМАНИЕ!

Евгений Чугунов

CISA, CISSP, PCI QSA

Эксперт
компании КРОК

111033, Москва, ул. Волочаевская, д.5, корп.1
+7 495 974 2274 (6415), +7 495 974 2277 (факс)
echugunov@croc.ru
www.croc.ru