Новые требования ECB и EBA к безопасности интернет-платежей и мобильных платежей

advaPAY events

CANOPUS INNOVATIVE TECHNOLOGIES

Введение:

В свете подготовки PSD 2 и в целях повышения безопасности интернет-платежей Европейское агентство по банковскому надзору (EBA) выпустило документ, содержащий соответствующие инструкции для:

* Платёжных организаций
* Органов по надзору в сфере оказания платёжных услуг -

* **“Final guidelines on the security of internet payments”**

История:

* 2012 г. – консультации по вопросам обеспечения безопасности интернет-платежей, организованные Европейским форумом по безопасности платежей SecuRe Pay;
* 31 января 2013 г. – рекомендации ЕЦБ на основе результатов консультаций, проведенных SecuRe Pay;
* 19 декабря 2014 г. – выход окончательной версии инструкций EBA в качестве правовой основы для реализации рекомендаций ЕЦБ по обеспечению безопасности интернет-платежей;
* 1 августа 2015 г. – дата начала реализации требований к безопасности интернет-платежей в 28 странах-членах ЕС до вступления в силу PSD 2 в 2017 / 2018 гг.

1. Разграничение должностных обязанностей / полномочий в информационных системах:

* Платёжные организации должны обеспечить разграничение полномочий сотрудников при работе в информационных системах, включая среду разработки, тестирования и рабочую систему;
* Для клиентов должны применяться меры усиленной аутентификации (двухфакторная аутентификация):
  * Для доступа клиента к оформлению интернет-платежей и платёжной информации;
  * При авторизации интернет-платежей (переводы, карточные платежи);
  * Для оформления / изменения электронной доверенности для выставления платёжных требований;
  * При выполнении операции на определенную сумму и в адрес определенного получателя

advaPAY events

CANOPUS INNOVATIVE TECHNOLOGIES

2. Повышение защиты серверов посредством оптимальных конфигураций:

* Платёжные организации должны обеспечить необходимую защиту информационных сетей, вебсайтов, серверов и каналов связи от возможных атак;
* Для снижения уязвимости серверов рекомендуется устранить излишнюю функциональную нагрузку;
* Доступ к приложениям, данным и ресурсам должен быть сведен к необходимому минимуму
* Интернет-сайты, предлагающие интернет-платежи, должны иметь расширенные сертификаты, выданные на имя платёжной организации, или обеспечивать аутентификацию иными средствами

3. Использование принципа "минимальных полномочий" в управлении доступом:

Идентификация и контроль доступа должны быть организованы на основе принципа «минимальных полномочий».

Это означает, что каждому пользователю системы должны быть назначены полномочия, достаточные исключительно для исполнения своих должностных обязанностей

4. Ограничение количества попыток входа в ИТ-систему:

Платёжная организации должна иметь возможность ограничить:

* Количество попыток входа в систему;
* Количество попыток аутентификации клиента;
* Срок действия аутентификации клиента

Платёжная организации должна иметь возможность блокировать сеанс работы с системой интернет-платежей по истечении определенного периода бездействия со стороны клиента

advaPAY events

CANOPUS INNOVATIVE TECHNOLOGIES

5. Комплексное шифрование данных:

Любые данные, имеющие отношение к идентификации и аутентификации клиента:

* При входе в систему;
* При оформлении интернет-платежа;
* При выдаче, изменении и отзыве электронной доверенности,

должны быть защищены от кражи, несанкционированного доступа и изменений.

Обмен конфиденциальными данными через Интернет в рамках сеанса связи должен осуществляться в зашифрованном виде с использованием надёжных и признанных средств шифрования данных

Платежная организация должна организовать минимум один защищенный канал связи с клиентом

6. Протоколирование действий:

Платёжные организации должны обеспечить мониторинг доступа к конфиденциальным данным по платежам и критически важным логическим и физическим ресурсам (информационным сетям, системам, базам данных, модулям защиты информации и пр.).

Платёжные организации должны иметь возможность вести, хранить и анализировать соответствующие журналы регистрации событий и аудита.

Должно быть обеспечено подробное протоколирование:

* Данных по операционной деятельности и электронным доверенностям;
* Даты и времени по операционным данным;
* Изменений в настройках параметров
* Доступа к операционным данным и электронным доверенностям

Должна быть возможность отследить любое добавление, изменение или удаление данных

advaPAY events

CANOPUS INNOVATIVE TECHNOLOGIES

7. Управление изменениями:

Платёжная организация должна самостоятельно определять:

* Необходимый объем изменений в текущей архитектуре информационной безопасности, технологических решениях и процессах;
* Сроки реализации изменений и их ввода в рабочую эксплуатацию;
* Промежуточные меры по предотвращению / минимизации случаев нарушения режима безопасности, мошеннических действий и перебоев в работе

Любые изменения должны выполняться в строгом соответствии с процедурой внесения изменений, включая:

* Планирование;
* Тестирование;
* Документирование;
* Утверждение

PSD 2 и новые требования безопасности:

Реализация инструкций EBA осуществляется в рамках действующей директивы ЕС об оказании платёжных услуг (PSD) до момента вступления в силу обновленной директивы PSD2 в 2017 / 2018 гг.

В настоящий момент положения PSD2 находятся в стадии окончательного согласования.

Предполагается, что PSD2 будет содержать развитие требований к текущим требованиям ЕЦБ по безопасности интернет-платежей.

Кроме того, в PSD2 ожидают:

* Введение нового субъекта регулирования: PISP - Payment Initiation Service Provider (Служба оформления платежей)
* Интеграцию между такими службами и платёжными организациями в целях единой / сквозной аутентификации клиентов

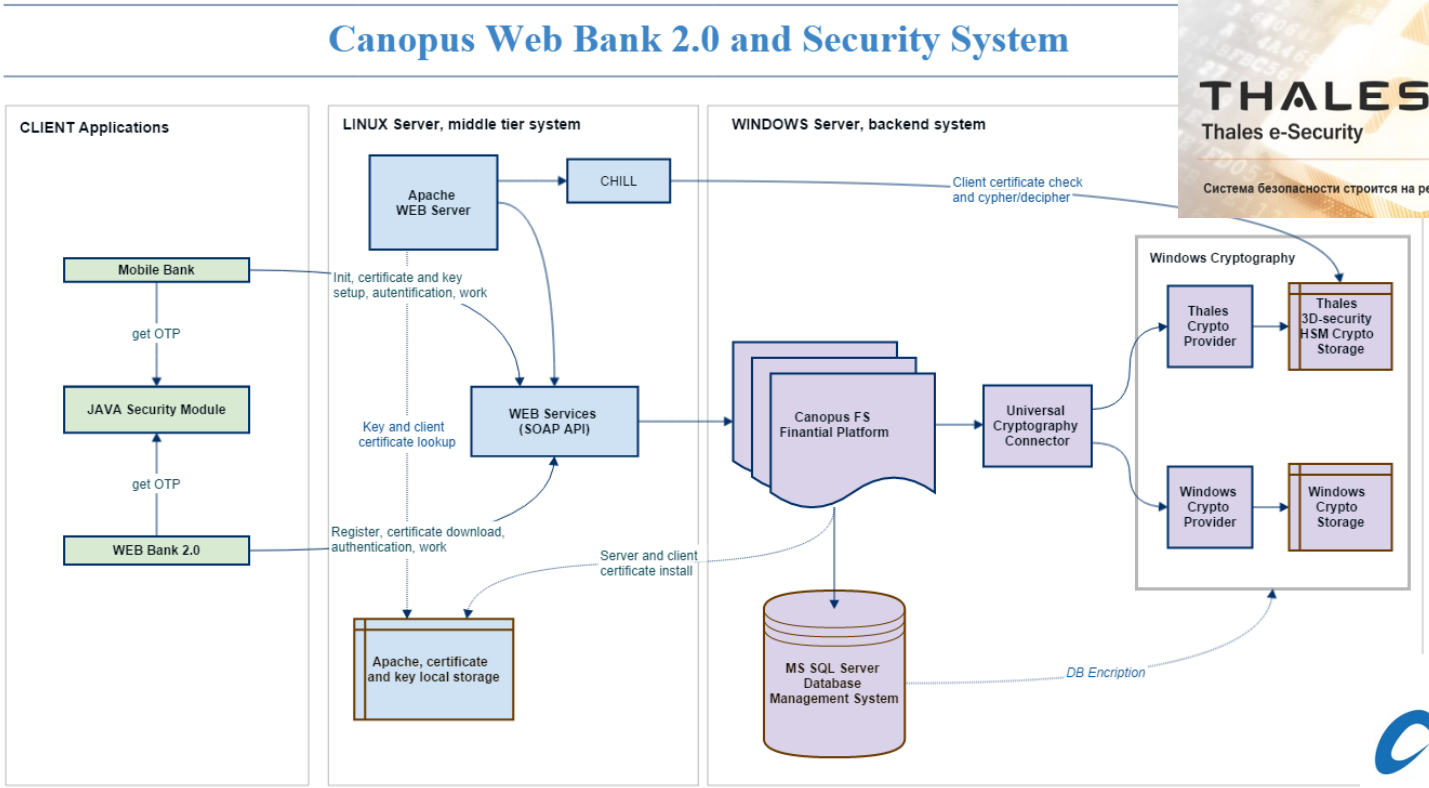
Соответствие наших решений новым требованиям по безопасности EBA

* Мы провели внутренний аудит на соответствие наших IT-решений (CANOPUS WebBank, EpaySuite и др.) новым требованиям по безопасности платежей EBA;
* Было выявлено, что наши решения практически полностью соответствуют данным требованиям;
* В настоящее время мы готовимся к проведению внешнего аудита.

advaPAY events

CANOPUS INNOVATIVE TECHNOLOGIES

Схема решения безопасности CANOPUS WebBank/EpaySuite:



1. WEB and mobile application
2. Amazing user experience
3. Integrated security
4. Secure HTTPs access to middle tier
5. OTP client module

1. Separation of business and client logic
2. Client application access via WEB services
3. Secure HTTP access via SSL/TLS
4. Apache security system including HSM intergation
5. Support for failover cluster

1. Setup and execution of business processes
2. Accounting and finantial transaction processing
3. Integrated security system including key and certificate creation Polifactor client transaction authentification
4. Failover cluster or mirroring of database system
5. Complete finantial transaction history
6. Complete user activity log

advaPAY events

CANOPUS INNOVATIVE TECHNOLOGIES

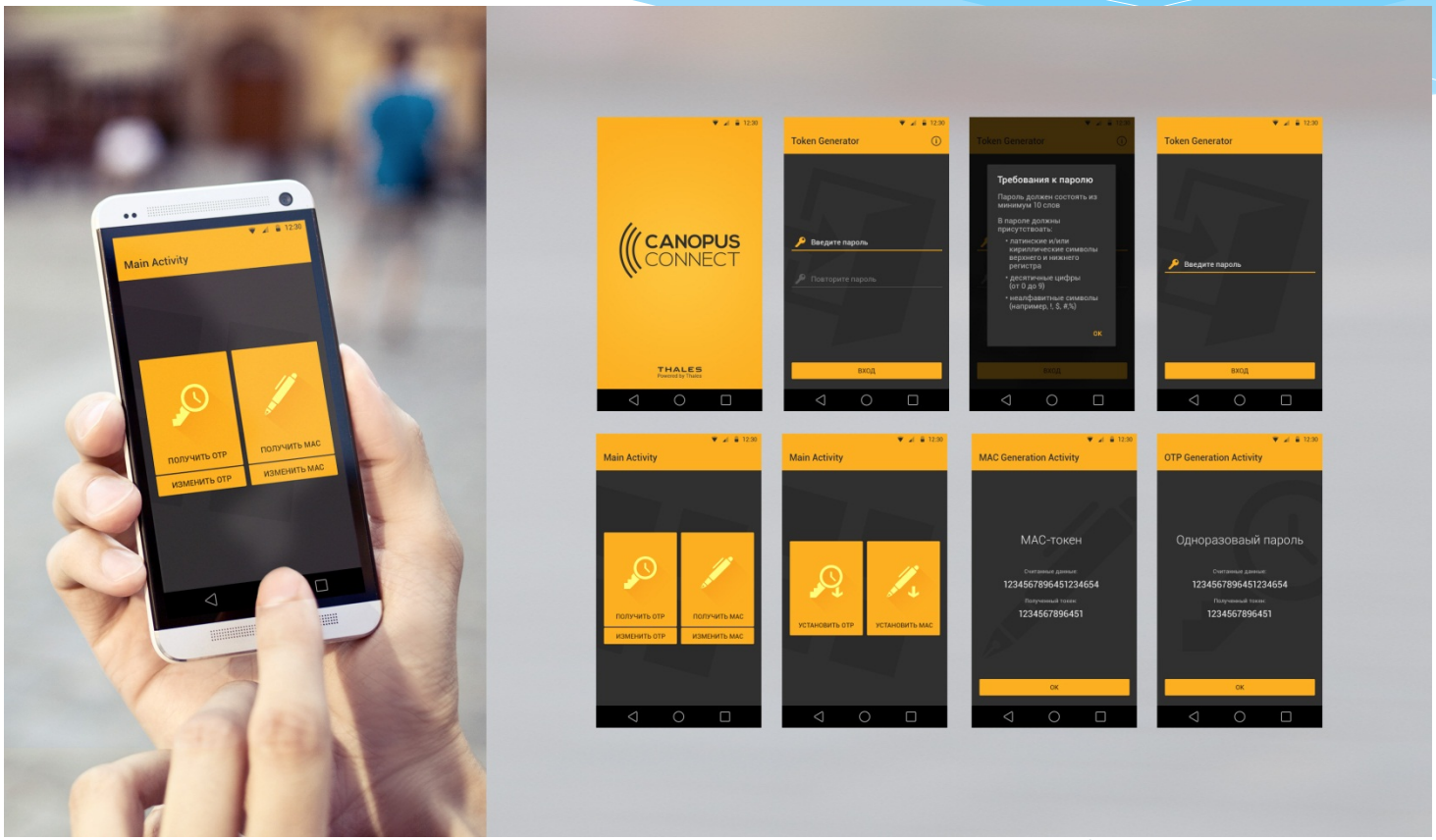
Параметризованная аутентификация:

* В документе EBA содержится рекомендация о связи между процедурой аутентификации и параметрами транзакции: суммой платежа, получателем платежа и др.
* Исходя из данного требования нами был разработан алгоритм расчета MAC-Кодов для аутентификации транзакций, который лег в основу специального приложения для смартфонов – MAC-генератора:
* http://canopus.ru/canopus-mac-token/

advaPAY events

CANOPUS INNOVATIVE TECHNOLOGIES

MAC-генератор



advaPAY events

CANOPUS INNOVATIVE TECHNOLOGIES

Контакты:

* CANOPUS Innovative Technologies,
* Москва, ул. Ярославская д. 8 к. 6.
* +7 495 9563468
* CEO
* Максим Иванченко
* Mob. +7 985 7617998
* ceo@canopus.ru
* Epaysuite.com Advapay.eu Canopus.ru

advaPAY events

CANOPUS INNOVATIVE TECHNOLOGIES