Система криптографической защиты информации «Шифр-X.509»

Опыт внедрения в банках Украины

Ковтун Владислав
Компания «Сайфер»

Национальный банк Украины

Национальный банк Украины активно строит межбанковскую инфраструктуру открытых ключей:

- Создание Удостоверяющего центра НБУ для регистрации/аккредитации ЦСК Банков
- Разработка организационно - технических нормативных документов, регламентирующих работу ЦСК Банков

Требования НБУ. Постановление №284 от 17.06.2010

«Положення про ЦСК банків України», пункт 2.1:

2.1. Банки та їх клієнти мають право отримувати послуги ЕЦП для банківських операцій та електронного документообігу в банківській системі від:

- власного Центру, … зареєстрованого/акредитованого в Засвідчувальному центрі (ЗЦ);
- Центру іншого банку, зареєстрованого/акредитованого в ЗЦ …
- Центру, що є окремою юридичною особою, який зареєстрований/ акредитований в ЗЦ …

Требования НБУ. Постановление №284 от 17.06.2010

«Положення про центри сертифікації ключів банків України», пункт 2.11:

2.11. Центр має право надавати послуги електронного цифрового підпису після проведення його реєстрації/акредитації в Засвідчувальному центрі в порядку, визначеному нормативно-правовими актами Національного банку України щодо правил реєстрації, засвідчення чинності відкритого ключа та акредитації центрів сертифікації ключів банків у Засвідчувальному центрі.

Письмо НБУ от 25.08.2009

- Национальный банк Украины – меры по формированию инфраструктуры открытых ключей банковской системы Украины (создание Удостоверяющего центра Национального банка Украины (УЦ НБУ) и отработка его взаимодействия с ЦСК банков Украины.

Система криптографической защиты информации

ШИФР-X.509

Назначение системы

Предназначена для:

- управления персональными ключами и сертификатами;
- электронной цифровой подписи;
- шифрования информации;
- строгой аутентификации.

Система криптографической защиты информации «Шифр-X.509»

СООТВЕТСТВИЕ НОРМАТИВНЫМ ТРЕБОВАНИЯМ

Криптографические алгоритмы

- Электронная цифровая подпись –
  ДСТУ 4145-2002
- Шифрование и имитозащита данных –
  ДСТУ ГОСТ 28147:2009
- Выработка хэш-функции данных –
  ГОСТ 34311-95
- Управление ключами шифрования данных (протокол Диффи-Хелмана) –
  ДСТУ ISO/IEC 15946:2006

Соответствие нормативным документам

- Совместному приказу Министерства юстиции Украины и Администрации Госспецсвязи Украины от 20.08.2012 г. №1236/5/453. Требования к форматам, структуре и протоколам, реализуемых в надежных средствах ЭЦП.
- Письму Министерства юстиции Украины от 15.10.2012 г. №12776-026-12-133. Касательно порядка вычисления хеш-значения.

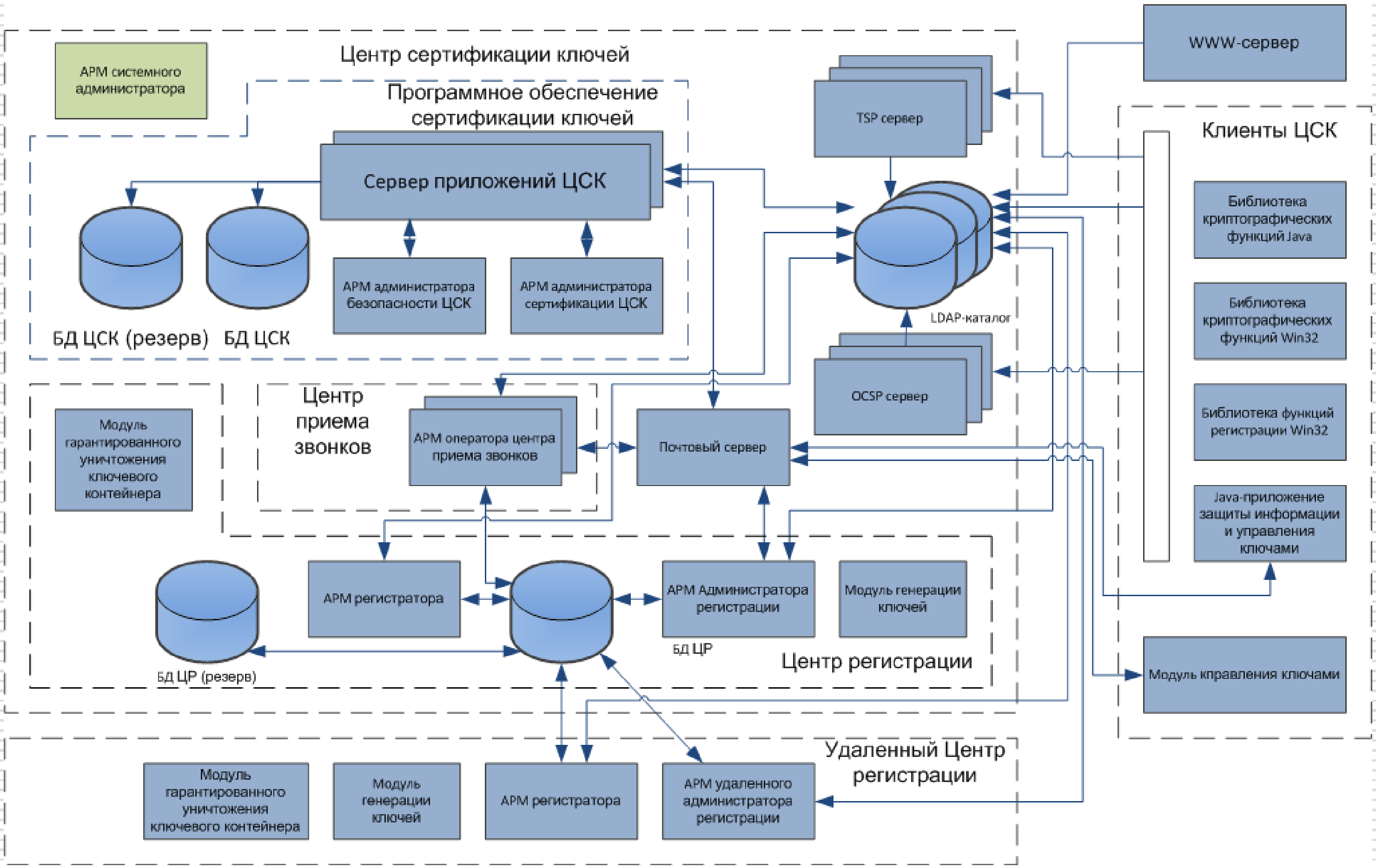
Соответствие нормативным документам

- СКЗИ «Шифр-X.509» имеет позитивное экспертное заключение Администрации Госспецсвязи Украины №05/02/02-5343 от 14.12.2012 г.

Система криптографической защиты информации «Шифр-X.509»

ОСОБЕННОСТИ ПОСТРОЕНИЯ

Архитектура



Состав ЦСК

- Программное обеспечение сертификации
  - АРМ Администратора безопасности ЦСК
  - АРМ Администратора сертификации ЦСК
  - Сервер приложений ЦСК
  - База данных ЦСК

Состав ЦСК

- Службы
  - АРМ Системного администратора
  - LDAP-сервер ЦСК
  - OCSP-сервер
  - TSP-сервер
  - Почтовый сервер

Состав ЦСК

- Центр регистрации
  - АРМ Администратора регистрации
  - АРМ Удаленного администратора регистрации
  - АРМ Регистратора
  - База данных Центра регистрации

Состав ЦСК

- Центр регистрации
  - Модуль генерации ключей
  - Модуль гарантированного удаления ключей
  - Модуль работы с ключевым контейнером
  - Коммуникационный сервер

Состав ЦСК

- Call-центр (центр приема звонков)
  - АРМ оператора Call-центра

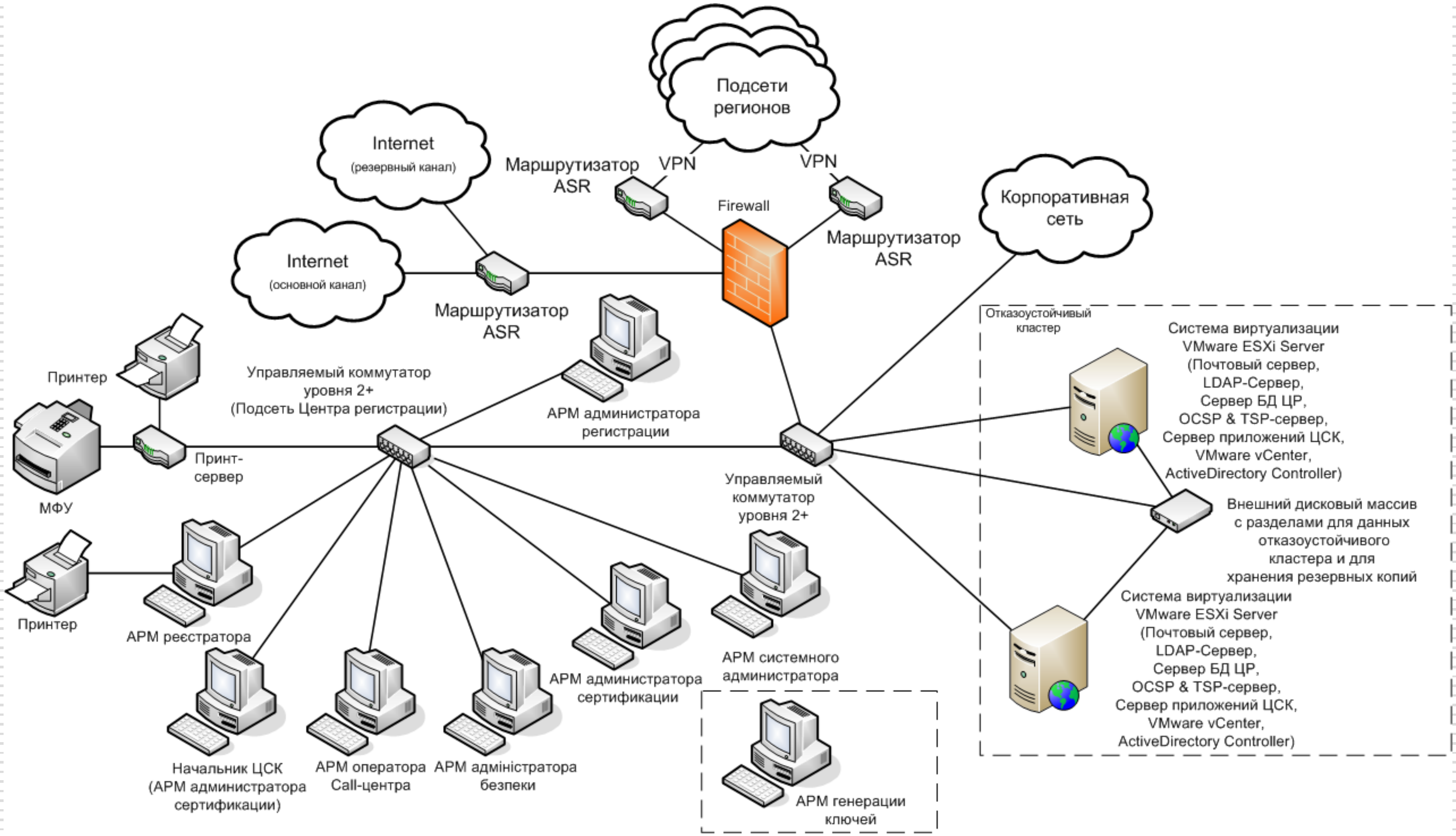
Состав клиентских средств

- Библиотеки криптографических функций
  - Библиотека для Win32 (dll)
  - Библиотека для Java (classes)
  - Библиотека GSS-API для Win32 (dll)
- Модуль управления ключами

Ключевые носители

- Файловый контейнер (*.nctx)
- Аппаратные носители (PKCS#11)
  - Автор USB Token, SmartCard
  - SafeNet USB eToken 5100
  - Giesecke & Devrient StarSign Crypto USB Token, Smart Card
  - Avest-UA
  - Aladdin UA JaCarta USB Token, SmartCard
  - Microcrypt Armorino

Топология системы



Система криптографической защиты информации «Шифр-X.509»

ВОЗМОЖНОСТИ БИБЛИОТЕК КРИПТОГРАФИЧЕСКИХ ФУНКЦИЙ

Традиционные функции

Криптографические преобразования:

- Постановка и проверка ЭЦП
- Выработка общего секрета (обмен ключами)
- Зашифровывание и расшифровывание данных

Расширенные функции

Управление ключами:

- Генерация ключей, запись на носитель, формирование запроса на сертификат
- Установление соединения с LDAP-сервером, получение нового сертификата
- Ввод в действие очередных ключей

Расширенные функции

Интерактивный контроль статуса сертификата :

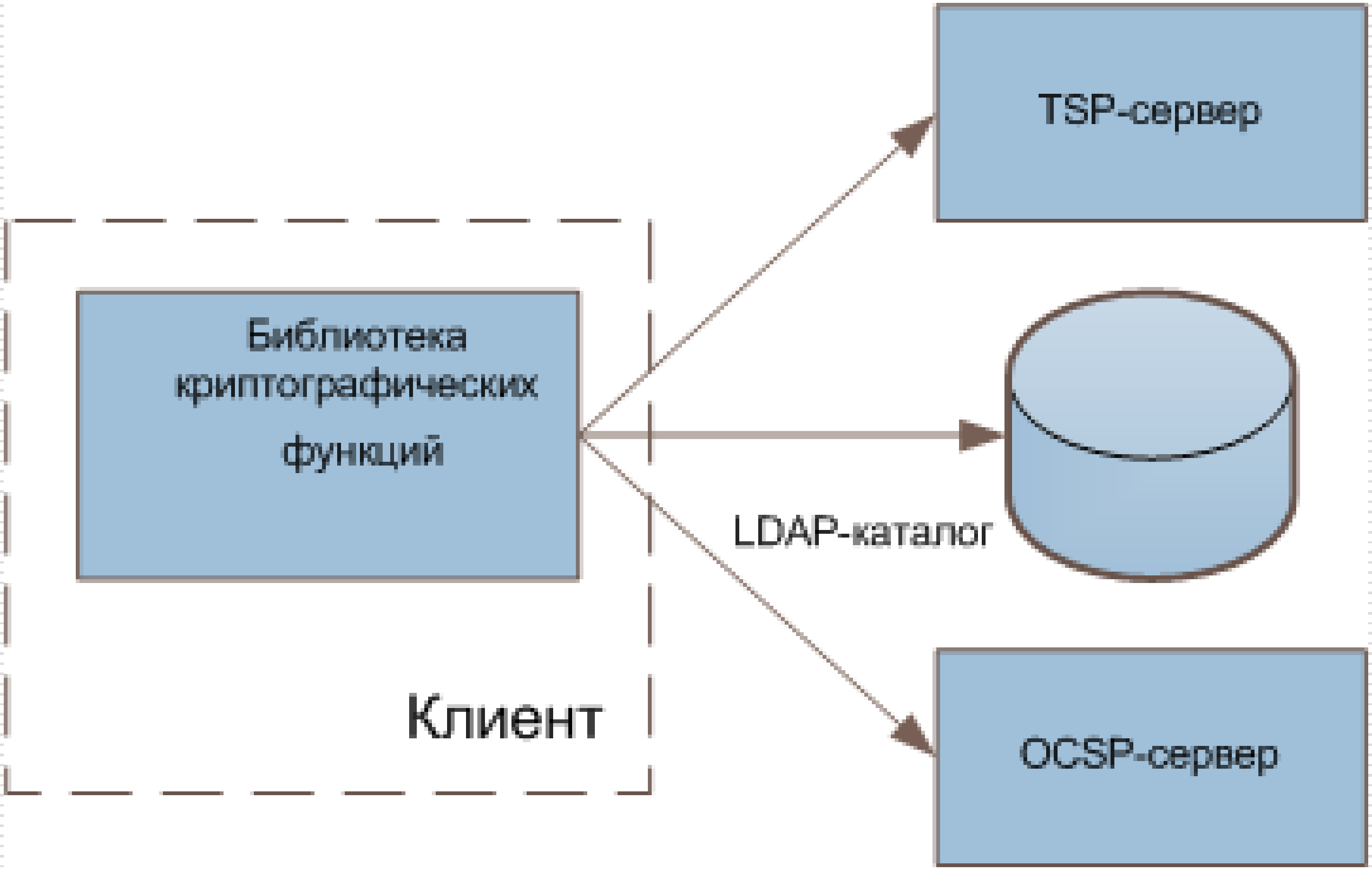
- Формирование запроса о состоянии сертификата на определенное время
- Установление соединения с OCSP-сервером, передача запроса
- Прием ответа от OCSP- сервера, проверка его аутентичности

Расширенные функции

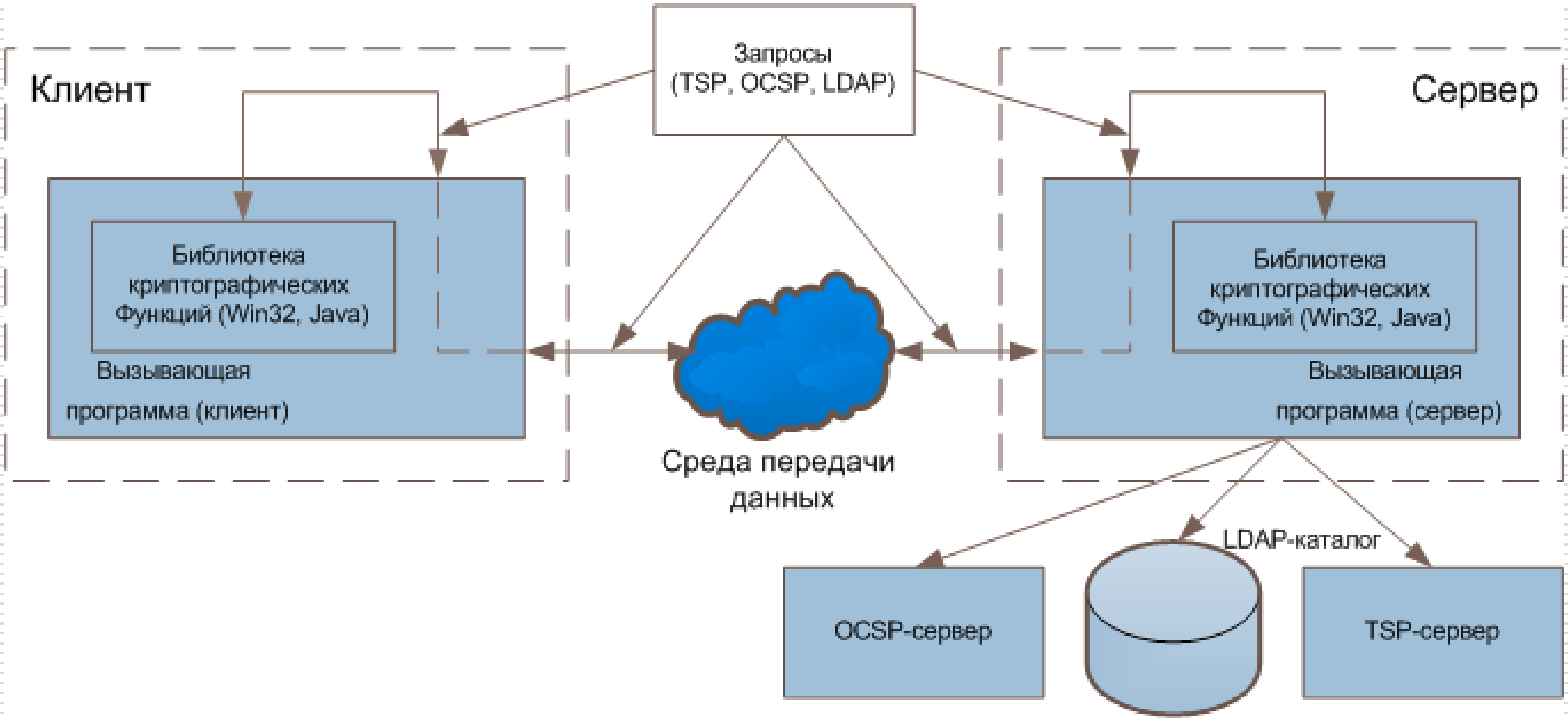
Работа с метками времени:

- Формирование запроса на метку времени для данных
- Установление соединения с TSP-сервером, передача запроса
- Прием метки времени, проверка ее аутентичности

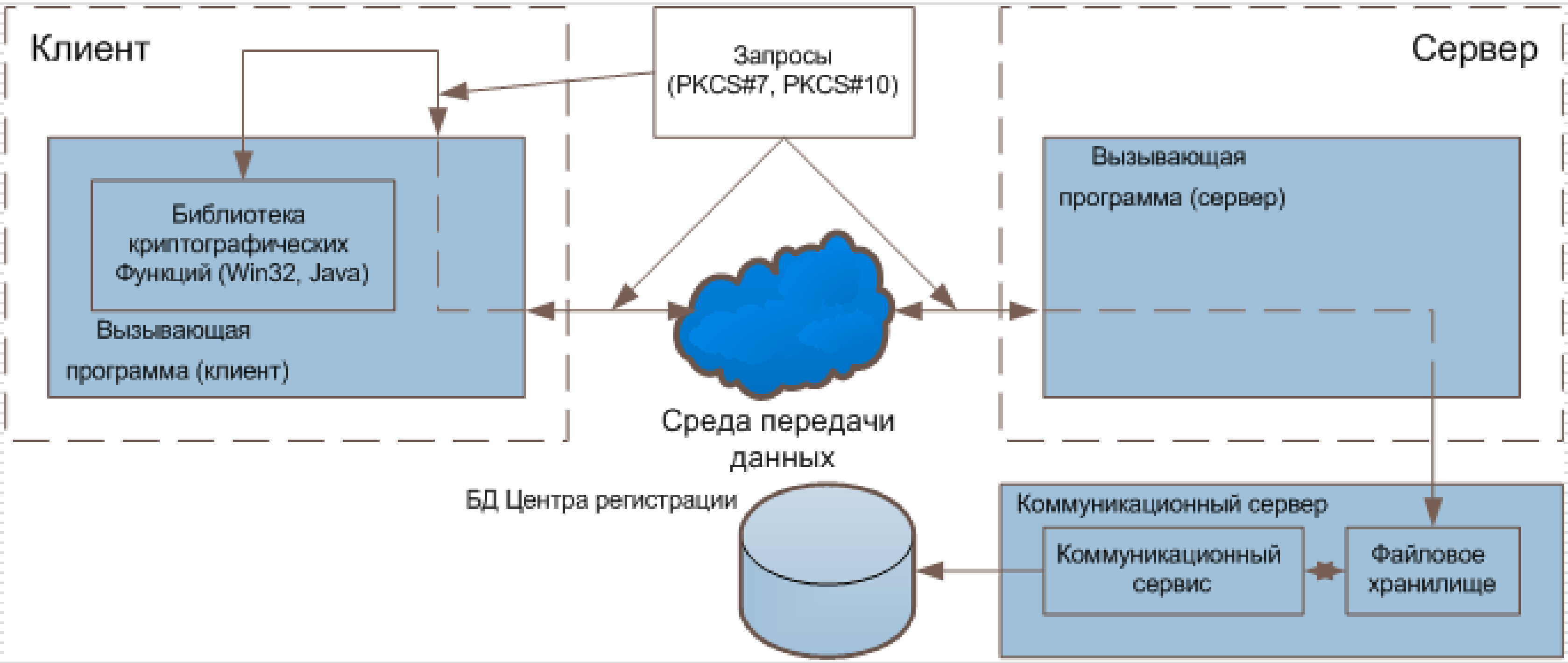
Взаимодействие с ЦСК (1)



Взаимодействие с ЦСК (2)



Расширенные возможности библиотек криптофункций



Система криптографической защиты информации «Шифр-X.509»

ВЫГОДЫ ОТ ВНЕДРЕНИЯ

Перспективное решение

- Универсальная и гибкая, позволяет обеспечивать криптографическую защиту в любых АБС и системах удаленного обслуживания клиентов
- Поддерживает стандарт ЭЦП ДСТУ 4145-2002, который является базовым в Украине
- Реализует в полном объеме требования семейства стандартов X.509
- Современная, ориентирована на эксплуатацию в течение продолжительного времени
- Обеспечивает создание ЦСК, который может быть зарегистрирован/аккредитован в Удостоверяющем центре НБУ

Достинства

- Единая система управления ключами и сертификатами для АБС и систем ДБО
- Современная, ориентирована на удаленное обслуживание пользователей в интерактивном режиме
- Повышает надежность и безопасность обслуживания удаленных пользователей и клиентов, посредством сервисов работающих в интерактивном режиме (OCSP, TSP, LDAP)

Достинства

- Упростить порядок регистрации (выдачи ключей) клиентам и работникам банка: клиент посетит отделение 2 раза, вместо 3-х
- Упростить порядок смены ключей клиентов и работников банка: смена происходит на рабочем месте клиента, без необходимости посещения банка
- Повысить защиту и надежность хранения ключевой информации: работа с защищенными носителями ключевой информации (ключ хранится внутри защищенного устройства)

Интеграция

- **eFOUR** – система фронтофисного обслуживания, разработчик компания CS (**завершена**)
- **iFOBS** – Интернет-банкинг, разработчик компания CS (**завершена**)
- **B2** – автоматизированная банковская система, разработчик компания CS (**в процессе**)
- **Nimbus** – Интернет-банкинг, разработчик компания УкрПей (**завершена**)
- **IB Pentagy** (физ. лица) - Интернет-банкинг, разработчик компания Пентеджи (**завершена**).

Интеграция

- **Winbank** - Интернет-банкинг, Пиреус Банк (**разработана технология интеграции**).
- **FlexiCRM** – CRM-система (управление взаимоотношениями с клиентами), разработчик компания Microcrypt (**завершена**).
- **Ensemble** – универсальная платформа для построения web-приложений, разработчик компания Intersystems (**завершена**).

Внедрения

- Банки
  - ПАО Кредобанк (eFOUR, iFOBS)
  - ПАО Банк Форум (IB Pentagy)
  - ПАО Терра Банк (Nimbus)
  - ПАО Пиреус Банк (Winbank)
- Органы государственной власти
  - Генеральная прокуратура Украины (Единый реестр досудебных расследований)

Спасибо за внимание

Компания «Сайфер»

г. Киев ул. Нагорная д.25-27

Тел.: (044) 484-46-12

(044) 484-46-17

E-mail: vk@cipher.kiev.ua

WWW: cipher.kiev.ua