Система криптографической защиты информации «Шифр-X.509»

Применение технологий X.509 для криптографической защиты информации в автоматизированных системах банков

Боровиков А.М
ООО «Сайфер ЛТД»

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 центри сертифікації ключів 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.

СКЗИ «ШИФР-Х.509»

Назначение системы

Система криптографической защиты информации «Шифр-X.509» предназначена для управления персональными ключами и сертификатами электронной цифровой подписи, обмена ключами и шифрования информации, согласно стандарта X.509

Криптографическое ядро

Программное изделие «Шифр+»*
(библиотеки криптографических преобразований Win32, Java)

* Имеется экспертное заключение ДСТСЗИ Украины

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 ТРЕБОВАНИЯМ

Стандарты и документы

№	Обозначение	Название	Краткая характеристика
1	ДСТУ ISO/IEC 9594-8:2006	Информационные технологии - Взаимодействие открытых систем – Каталог. Часть 8.	Основные положения сертификации открытых ключей и атрибутов
2	RFC 2510	PKIX Certificate Management Protocols	Описывает PKIX-протоколы управления сертификатами
3	RFC 2559	Internet X.509 Public Key Infrastructure. Operational Protocols - LDAPv2	Описывает протокол LDAP
4	RFC3161	Time-Stamp Protocol (TSP)	Протокол меток времени
5	RFC2560	Online Certificate Status Protocol - OCSP	Протокол определения статуса сертификата в режиме online
6	PKCS#10	Certification Request Standard	Формат запроса к ЦСК на издание сертификата публичного ключа.
7	PKCS#11	Cryptographic Token Interface	Описывает платформенно-независимое API по работе с криптографическими модулями, такими как HSM

Стандарты и документы

№	Обозначение	Название	Краткая характеристика
8	RFC 2315, RFC 2630 (PKCS#7)	Cryptographic Message Syntax	Описывает форматы криптографических сообщений
9	Совместный приказ ДСТСЗИ СБУ и Государственного департамента по вопросам связи и информатизации Минтранссвязи Украины от 11.09.2006 г. № 99/166		Технические спецификации форматов представления основных базовых объектов инфраструктуры открытых ключей
10	Приказ ДСТСЗИ СБ Украины от 10.05.2006 г. №50		Правила усиленной сертификации

- Ведутся работы по реализации технических спецификаций, указанных в проекте приказа «Об утверждении технических спецификаций форматов представления базовых объектов национальной системы электронной цифровой подписи»

Нормативные документы

- Закон Украины «Об электронной цифровой подписи» от 22 мая 2003 г. № 852-IV.
- Закон Украины «Об электронном документе и электронном документообороте» от 22 мая 2003 г. № 851-IV.
- «О порядке разработки, производства и эксплуатации средств криптографической защиты конфиденциальной информации и открытой информации с использованием электронной цифровой подписи», утвержден приказом ГСССЗИ Украины от 20 июля 2007 г. № 141.
- «Национальная система электронной цифровой подписи. Технические спецификации представления базовых объектов», утвержден совместным приказом ДСТСЗИ СБ Украины и Государственного департамента по вопросам связи и информатизации Министерства транспорта и связи Украины от 11.09.2006 г. № 99/166.
- Проект совместного приказа Министерства юстиции Украины и ГСССЗИ Украины «Об утверждении технических спецификаций форматов представления базовых объектов национальной системы электронной цифровой подписи».

Нормативные документы

- «Правила усиленной сертификации», документ утвержден приказом ДСТСЗИ СБ Украины от 10.05.2006 г. № 50.
- «Инструкция о порядке поставки и использования ключей к средствам криптографической защиты информации, которые реализуют криптографический алгоритм, определенный ГОСТ 28147-89», документ утверждён приказом ГСССЗИ Украины от 12.06.2007 г. №114.
- «Порядок аккредитации центра сертификации ключей», документ утвержден постановлением Кабинета Министров Украины от 13.07.2004 г №903.
- «Порядок применения электронной цифровой подписи органами государственной власти, органами местного самоуправления, предприятиями, учреждениями и организациями государственной формы собственности», документ утвержден постановлением Кабинета Министров Украины от 28.11.2004 г №1452.
- «Положення про центри сертифікації ключів банків України», затвердженого постановою Правління Національного банку України 17.06.2010 №284.
- «Правила реєстрації, засвідчення чинності відкритого ключа та акредитації центрів сертифікації ключів банків України в Засвідчувальному центрі Національного банку України», затверджені постановою Правління Національного банку України 17.06.2010 №284.

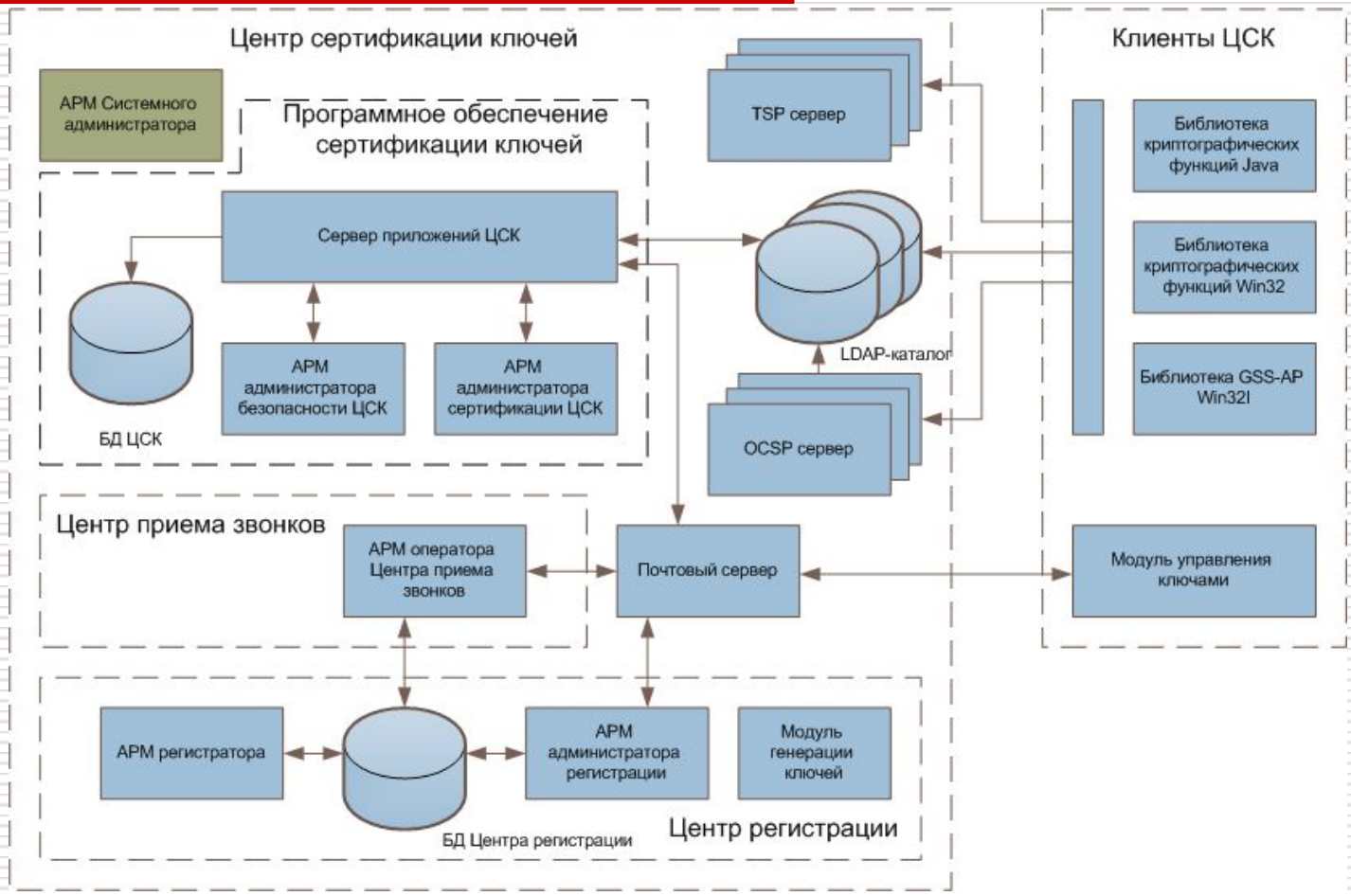
Соответствие нормативным документам

Средства Центра сертификации ключей СКЗИ «Шифр-X.509» полностью удовлетворяет требованиям, которые предъявляются к аккредитованным ЦСК

СКЗИ «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 Регистратора
  - Модуль генерации ключей
  - Коммуникационный сервер
- 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
- Аппаратные носители, поддерживающие PKCS#11*
  - Автор USB Token (SLE44C42S, SLE44C160S, SLE66C42P, SLE66C82P, SLE66C161PE)
  - SafeNet USB eToken 5100
  - Giesecke & Devrient StarSign Crypto USB Token, Smart Card

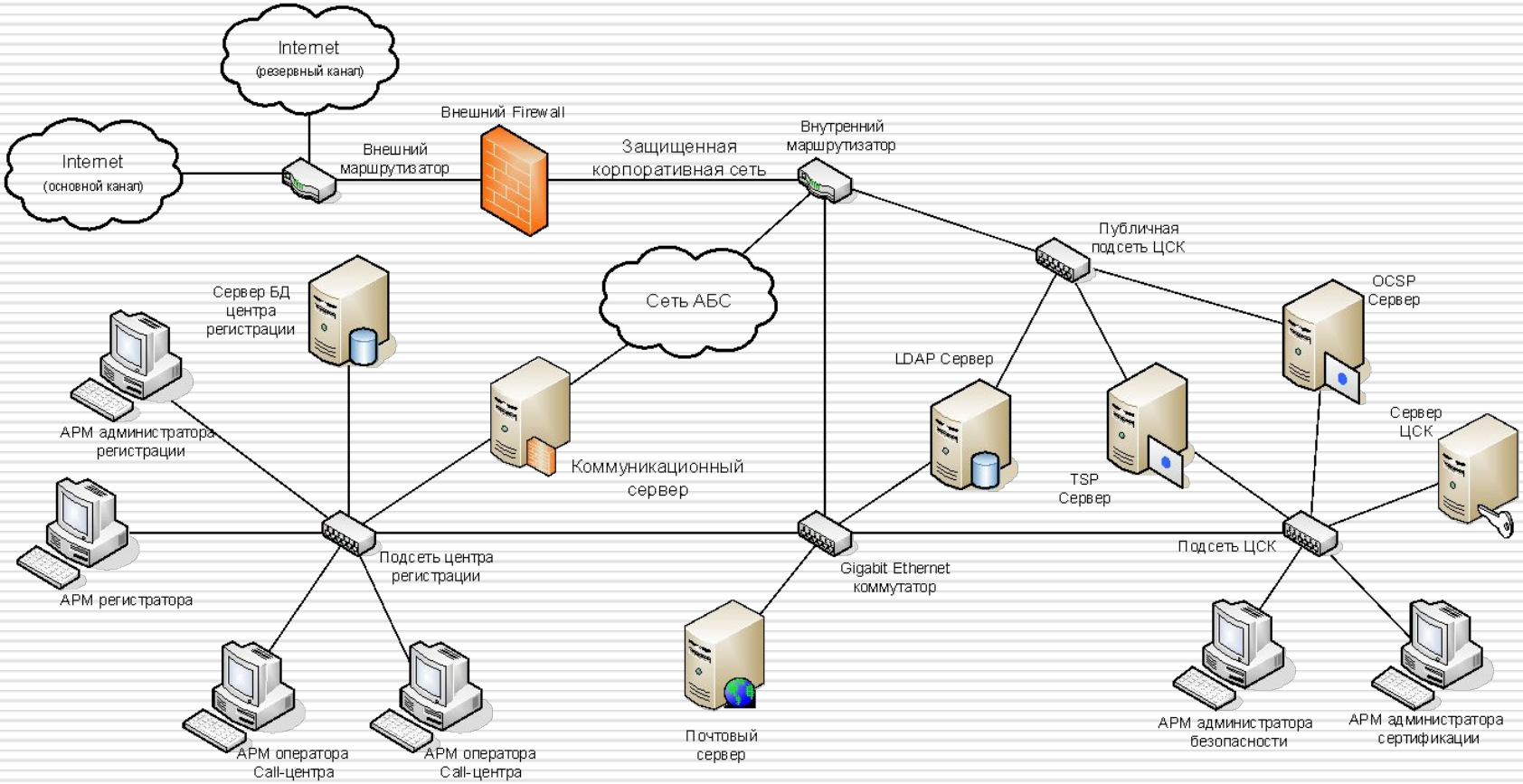
*Пассивный режим

Ключевые носители

- Аппаратные носители, поддерживающие PKCS#11*
  - Автор (SLE44C42S, SLE44C160S, SLE66C42P, SLE66C82P, SLE66C161PE)
  - SafeNet eToken 5100 (к осени 2012 г.)
  - Giesecke & Devrient StarSign Crypto USB Token (к осени 2012 г.)

*Активный режим (к осени 2012 г.)

Топология системы



ВОЗМОЖНОСТИ БИБЛИОТЕК КРИПТОГРАФИЧЕСКИХ ФУНКЦИЙ

Криптографические преобразования

Традиционные функции:

- Постановка и проверка электронной цифровой подписи
- Выработка общего секрета (обмен ключами)
- Зашифровывание и расшифровывание данных

Управление ключами

Смена ключей:

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

Расширенные возможности библиотек криптофункций

On-line контроль статуса сертификата :

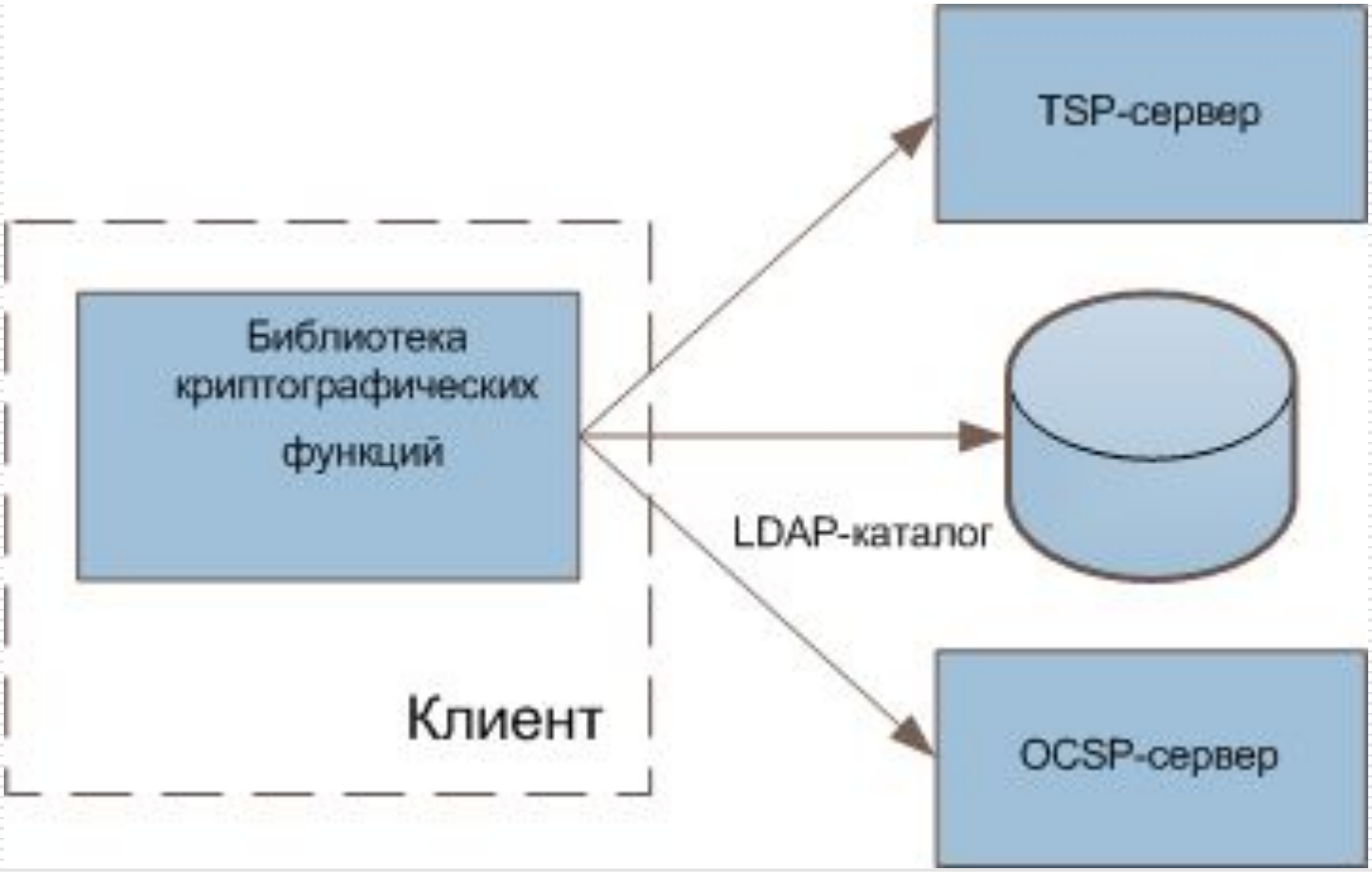
- Формирование запроса о состоянии сертификата на определенное время
- Установление соединения с OCSP-сервером, передача запроса
- Прием ответа от OCSP- сервера, проверка его аутентичности

Расширенные возможности библиотек криптофункций

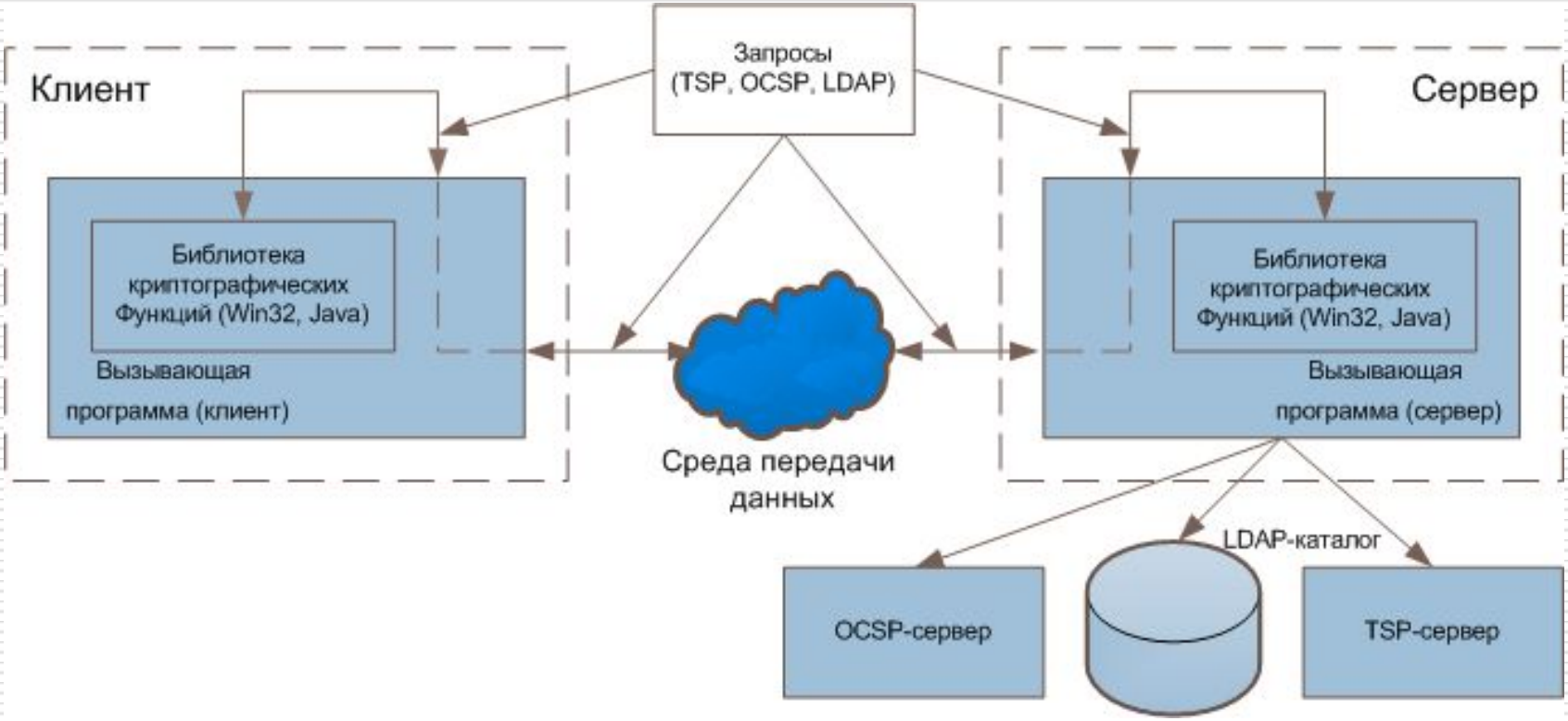
Работа с метками времени:

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

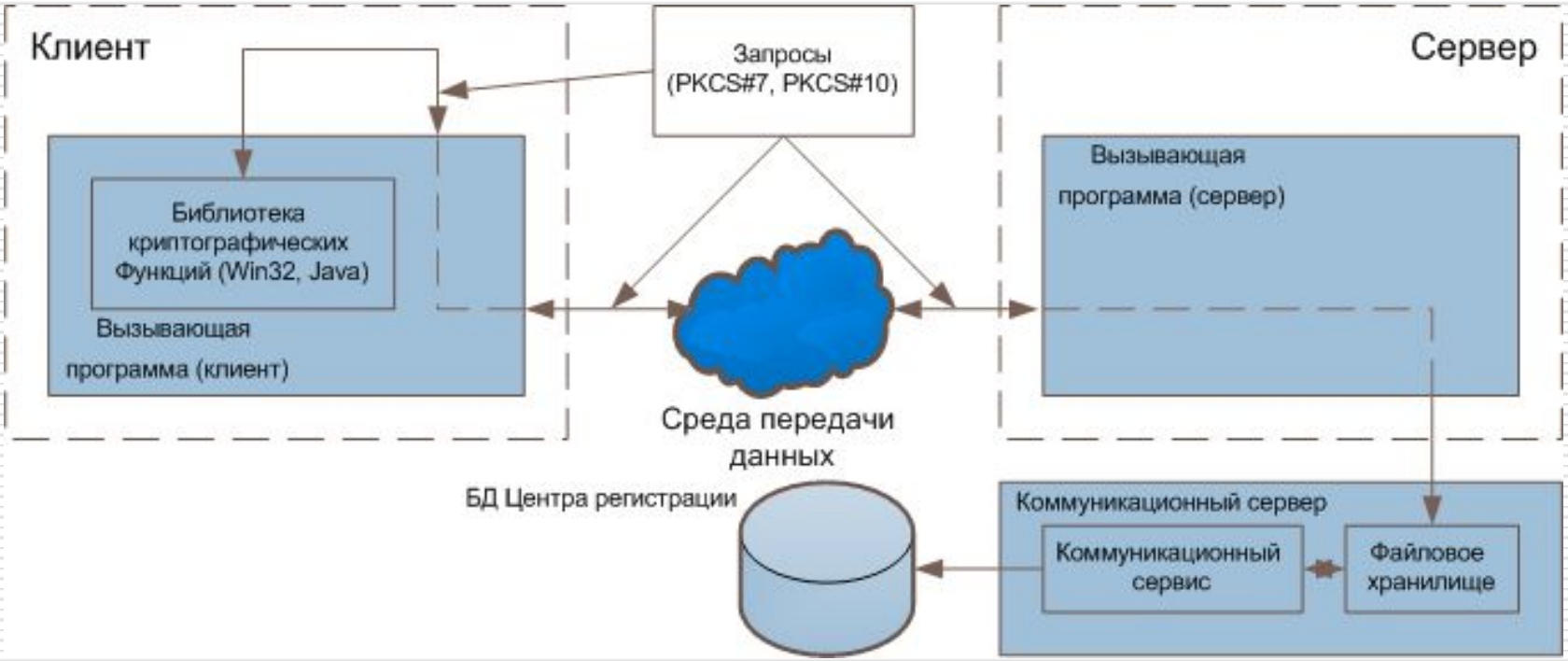
Взаимодействие с ЦСК (1)



Взаимодействие с ЦСК (2)



Расширенные возможности библиотек криптофункций



Производительность

Формирование ЭЦП

- Разбор параметров сертификата
- Проверка значений параметров (например полномочий)
- Проверка статуса
- Вычисление образа документа
- Вычисление подписи
- Формирование метки-времени

Проверка ЭЦП

- Загрузка сертификата из хранилища (LDAP, локально, БД)
- Разбор параметров сертификата
- Проверка значений параметров (например полномочий)
- Проверка цепочки сертификатов (статус, полномочия, …)
- Проверка статуса сертификата
- Вычисление образа документа
- Проверка подписи
- Проверка метки времени

Производительность

Операции	Условия тестирования			
	Intel Core i7 2600 3,8 ГГц Windows 7 x64, **8 потоков**	Intel Core2 Duo E6400 (с 2,13 ГГц до 3 ГГц) Windows XP SP3 x86, **2 потока**	Intel Core i3 M350 2,3 ГГц Windows 7 x64, **4 потока**	Intel Core2 Duo T7200 Windows XP SP3 x86, **2 потока**
С проверками				
Подпись на поток, шт/с (мс)	96 (10,4)	105 (9,5)	61 (16,4)	73 (13,7)
Проверка на поток, шт/с (мс)	100 (10,0)	109 (9,1)	61 (16,4)	73 (13,7)
Подписей на CPU, шт/с	768	210	245	146
Проверок на CPU, шт/с	793	218	245	146
Без проверок				
Подпись на поток, шт. (мс)	192 (5,1)	208 (4,7)	121 (8,3)	142 (7,0)
Проверка на поток, шт. (мс)	100 (10,0)	109 (9,3)	62 (16,1)	73 (13,7)
Подпись на CPU, шт/с	1594	416	482	284
Проверка на CPU, шт/с	794	218	244	146

Носители. Критерии оценки

- Стоимость
- Качество изделия
- Качество программного обеспечения
- Наличие качественной поддержки и ее стоимость
- Работа в различных средах (Microsoft Terminal Server, Citrix XenApp Server)

Поставка носителей

ООО «Сайфер ЛТД» является дистрибьютором защищенных носителей (поддерживающие PKCS#11) :

- **Автор** USB Token, Smart Card, Card Reader
- **SafeNet** USB eToken 5100
- **Giesecke & Devrient** StarSign Crypto USB Token, Smart Card, Card Reader

Поставка ПО к носителям

Управление защищенными носителями на клиентском рабочем месте

- **Автор** – драйвера, интерфейсные клиентские библиотеки (Drivers, Libraries)
- **SafeNet** – Secure Authentication Client (полноценный комплекс управления - PKI Client, Drivers, Libraries)
- **Giesecke & Devrient** (A.E.T. Flexible Security) **-** SafeSign Identity Client (полноценный комплекс управления - PKI Client, Drivers, Libraries)

* Предоставляется бесплатно, вместе с носителями

ВЫГОДЫ ОТ ВНЕДРЕНИЯ

Перспективное решение

- Универсальная и гибкая, позволяет обеспечивать криптографическую защиту во всех автоматизированных системах банка, включая любые системы удаленного обслуживания клиентов
- Поддерживает стандарт ЭЦП ДСТУ 4145-2002, который является базовым в Украине
- Реализует в полном объеме требования 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 всех банковских систем
- Современная, ориентирована на удаленное обслуживание пользователей в режиме on-line (большинство перспективных банковских сервисов ориентированы на работу в режиме on-line)
- Повышает надежность и безопасность обслуживания удаленных пользователей и клиентов, посредством сервисов работающих в режиме on-line (OCSP, TSP, LDAP)

Спасибо за внимание

ООО «Сайфер ЛТД»

Г. Киев ул Нагорная д.25-27

Тел.: (044) 484 46 12

(044) 484 46 17

E-mail:sales@cipher.kiev.ua

http://www.cipher.kiev.ua