Система криптографической защиты информации «Шифр-Х.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 24.04.2015

- УЦ НБУ планирует начать регистрацию ЦСК банков и просит предоставить:
  - Информацию о собственном ЦСК
  - Срок готовности к регистрации в УЦ НБУ

Системы криптографической защиты информации

ОБЗОР РЫНКА

Какие алгоритмы используются

Алгоритмы		
ЭЦП	ГОСТ 34.310-95*	ДСТУ 4145-2002**
Хеширование	ГОСТ 34.311-95	ГОСТ 34.311-95
Шифрование	ГОСТ 28147-89	ГОСТ 28147-89
Выработка общего секрета	ДСТУ ISO/IEC 15946-3	ДСТУ ISO/IEC 15946-3

Алгоритмы	
Шифрование	ДСТУ 7624:2014
Хеширование	ДСТУ 7564:2014

* - длина ключа 1024 бит.
** - длина ключа 257 бит.

Назначение системы

Предназначена для:

- Управления личными ключами и сертификатами.
- Формирования электронной цифровой подписи;
- Выработки общего секрета.
- Шифрования информации.
- Строгой взаимной аутентификации.

Управление ключами

- Банковские системы со встроенными клиентскими библиотеками (средств защиты и управления ключами) и параллельно в банке разворачивается ЦСК:
  - ЦСК 2G
  - ЦСК 3G

Банковские системы*

- Автоматизированная банковская система (АБС) или Операционный день банка (ОДБ)
- Клиент-банк (КБ)
- Интернет-банкинг (ИБ)/Web-банкинг
- Денежные переводы (ДП)

* - обязательное применение криптографии

Управление ключами

№	Системы	Банк-Разработчик	Разработчик банковской системы	Разработчик средств защиты
1	Банковская система	+		
	Средства защиты			+
2	Банковская система		+	
	Средства защиты		+	
3	Банковская система		+	
	Средства защиты			+

Основные производители банковских систем

Производитель	АБС	КБ/ИБ/W	ДП	Другие
CS (Харьков)	**+**	**+/+/+**	**+**	**+**
Lime Systems (Донецк-Киев)	+	+/+/+		+
Unity Bars (Киев)	+	+/+/+		+
Bifit (Днепропетровск)	+	+/+/+		
Аргус (Харьков)	+	-/+/+	+	+
Ukr Pay (Киев)		+/+/+		+
Pentagy (Киев)		+/+/+		
Enigma Soft (Харьков)		-/+/-		
R-Style Softlab (Киев)	+	+/+		+
Soft-Review (Киев)	+	+/+		+
Сайфер (Киев)		+/+		
НОКК (Киев)		+/+		

Основные производители средств защиты

- Институт информационных технологий, ИИТ (Харьков)
- Сайфер (Киев)
- НОКК (Киев)
- Автор (Киев)
- Битис (Киев)
- Интер-Метл (Киев)

Основные производители ЦСК*

Производитель	ЦСК 2G	ЦСК 3G	В банках
ИИТ (Харьков)	Щит [Ежик]	ЦСК-1	+
Сайфер (Киев)	Шифр-PKI [Шифр]	Шифр-X.509 [Шифр+]	+
НОКК (Киев)	Вега	Вега (ECC)	+
Автор (Киев)	-	Crypto KDC [CryptoLib]	+
Битис (Киев)	-	ЦСК X.509 [NovaLib]	-
Интер-Метл (Киев)	-	Цезарис	-

* - ЦСК развернуты в банках

Системы криптографической защиты информации

САЙФЕР

Средства управления ключами

- Шифр-PKI (2G)
- Шифр-X.509 (3G)

Интеграция с банковским ПО

ЦСК	АБС	ИБ	ДП	Другие
2G	CS B2, Soft-Review SR-Bank, R-Style UA RS-bank, Credit-Agricole АБС, Lime-Systems Scrooge2	CS iFOBS, Cipher ElPay, Unity Bars КБ, Enigma Soft Style	CS EMOS	CS eFOUR
3G	CS B2*	CS iFOBS, Cipher ElPay, Pentagy, UkrPay Nimbus	CS EMOS	CS eFOUR

* - проходит интеграция

Банки-клиенты (ЦСК 2G)

УкрСиббанк Кредобанк КБ Дельта Энергобанк Финбанк БМ Банк Астрабанк АктаБанк Банк Восток Банк Форум Укргазпромбанк Банк Богуслав Промэкономбанк Пиреус банк МКБ Банк Порто-Франко Креди Агриколь Банк	ВТБ Банк VS Банк Авант Банк Укринбанк Еврогазбанк Актив-Банк БТА-Банк ОТП Банк Банк Премиум Банк Форвард ЕвроПромБанк Кредит Оптима Банк Национальный кредит ДБ Сбербанка России Банк Украинский капитал Банк Рыночные технологии	Мотор Банк Мелиор Банк Банк Стандарт Юнисон Банк Финанс Банк ФК «Система» ФК «Элайнс» Платинум Банк Банк Пивденный Банк Софийський Интер Кредит Банк Финансовая инициатива Всеукраинский банк развития Городской коммерческий банк

Банки-клиенты (ЦСК 3G)

- Кредобанк
- Всеукраинский банк развития
- Пивденный
- Финансовая инициатива
- Финансбанк
- Форум*
- Терра банк*

* - проходит ликвидация

Система криптографической защиты информации

ШИФР-X.509

Система криптографической защиты информации «Шифр-X.509»

СООТВЕТСТВИЕ НОРМАТИВНЫМ ТРЕБОВАНИЯМ

Криптографические алгоритмы

Алгоритм	Стандарт
ЭЦП	**ДСТУ 4145-2002**
Шифрование и иммитовставка	**ДСТУ ГОСТ 28147:2009**
Хеширование	**ГОСТ 34.311-95**
Выработка общего секрета	**ДСТУ ISO/IEC 15946:2006**

Соответствие нормативным документам

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

Соответствие нормативным документам

- Приказ Администрации Госспецсвязи Украины от 18.12.2012г. №739 «Об утверждении Требований к форматам криптографических сообщений».
- *Совместный приказ Министерства юстиции Украины Администрации Госспецсвязи Украины от 27.12.2013г. №2782/5/689 «Требования к алгоритмам, форматов и интерфейсов, что реализуются средствами шифрования и надежных средств электронной цифровой подписи».

* - с изменениями

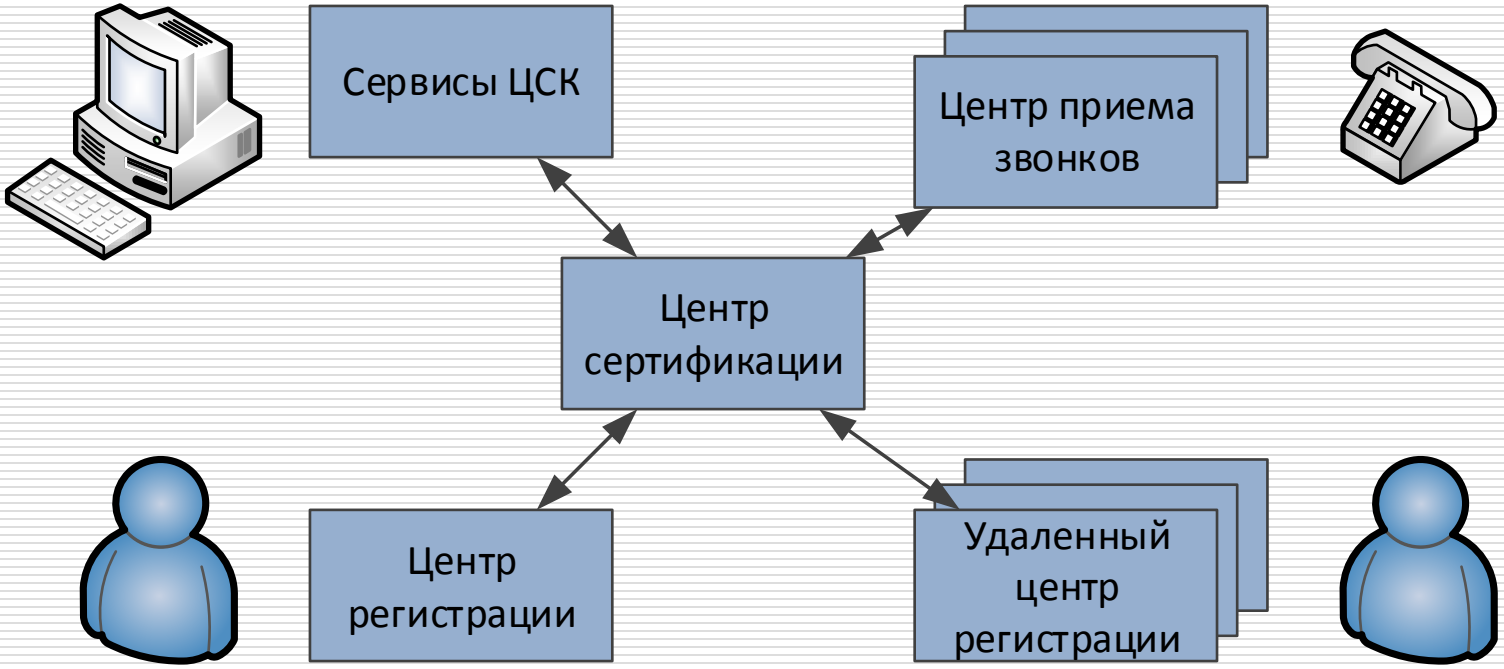
Соответствие нормативным документам

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

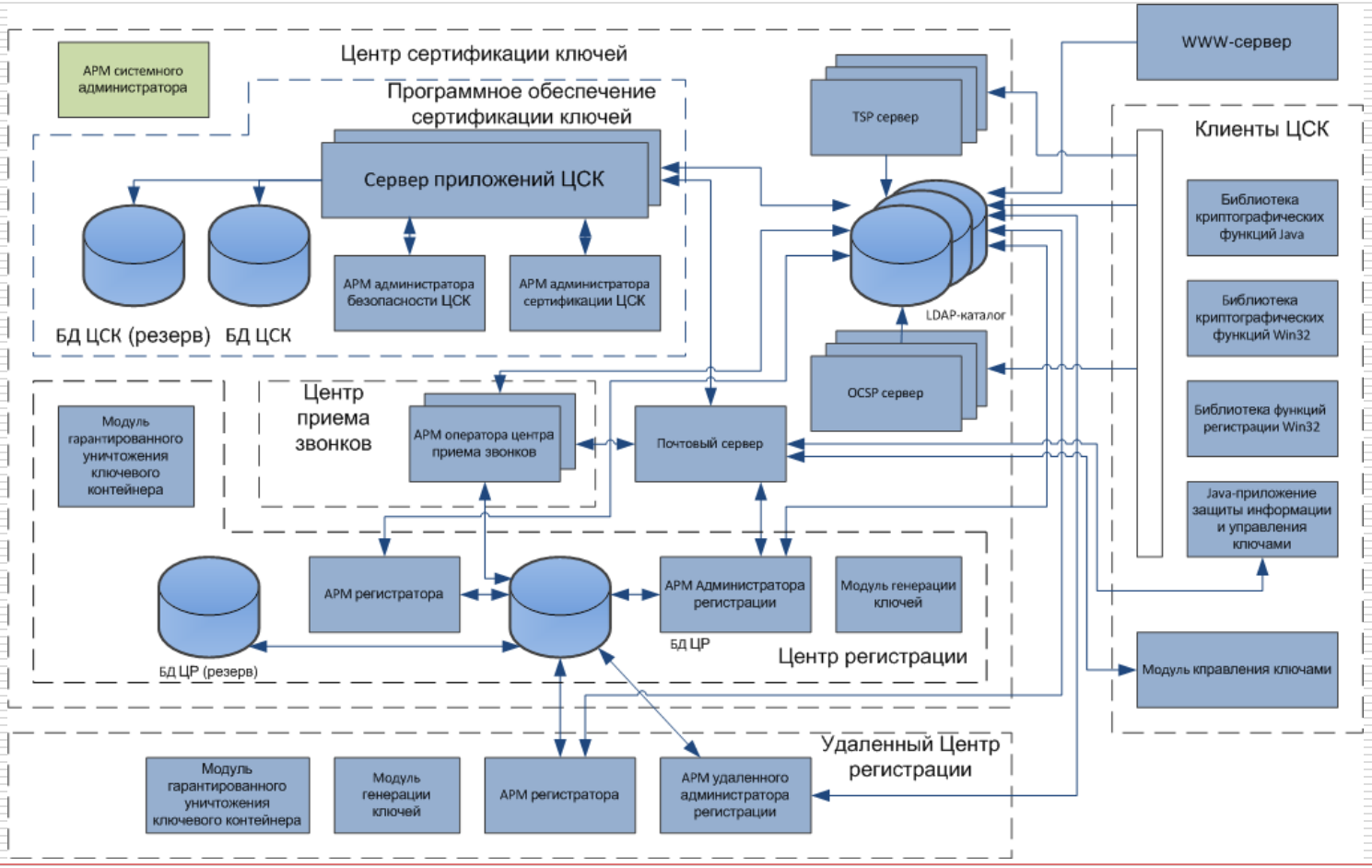
Система криптографической защиты информации «Шифр-X.509»

ОСОБЕННОСТИ ПОСТРОЕНИЯ

Архитектура



Архитектура



Состав ЦСК

- Центр сертификации
  - АРМ Администратора безопасности ЦСК
  - АРМ Администратора сертификации ЦСК
  - АРМ отчетности ЦСК
  - Сервер приложений ЦСК
  - База данных ЦСК

Состав ЦСК

- Сервисы ЦСК
  - АРМ Системного администратора
  - LDAP-сервер ЦСК
  - OCSP-сервер
  - TSP-сервер
  - Почтовый сервер
  - Система резервного копирования
  - Служба репликации и синхронизации

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

- Центр приема звонков
  - АРМ оператора ЦПЗ

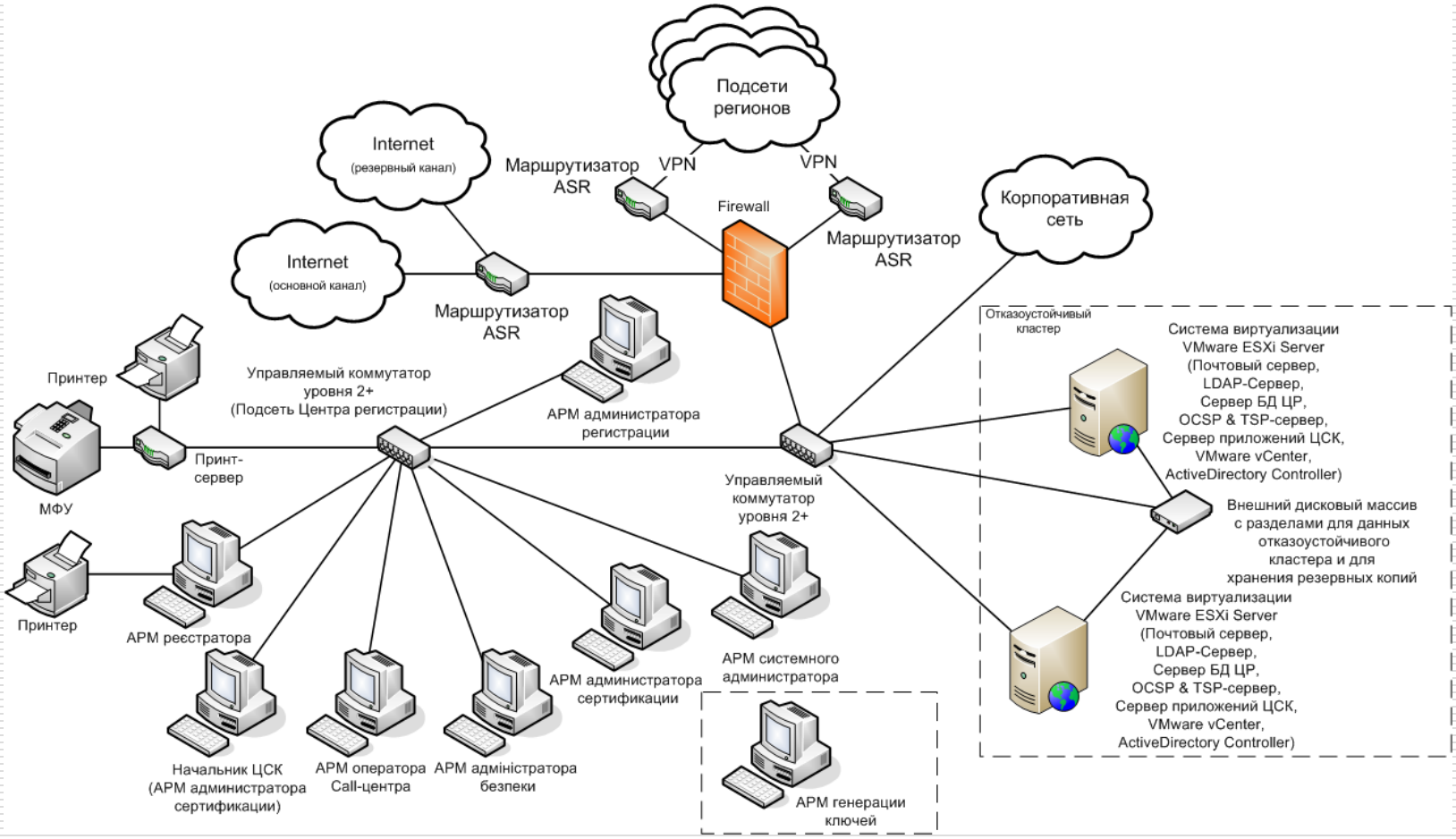
Состав клиентских средств

- 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)
- Файловый контейнер (*.pfx |*.p12)
- Аппаратные носители (PKCS#11)
  - Автор USB Token, SmartCard
  - SafeNet USB eToken 5100
  - Gi & De StarSign Crypto USB Token, Smart Card
  - Avest-UA AvestKey
  - Aladdin UA JaCarta USB Token, SmartCard
  - Microcrypt Armorino

Топология системы



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)

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