# СКЗИ «Шифр-X.509»

# ЦСК и обеспечение непрерывности функционирования информационной системы банка

ООО «Сайфер ЛТД»

к.т.н. Александр Боровиков

# Содержание

- Требования НБУ к ЦСК банков Украины
- СКЗИ «Шифр-X.509»:
  - Соответствие требованиям НБУ
  - Резервирование и восстановление
  - Мониторинг и диагностика
  - Организационно-техническое обеспечение

# ТРЕБОВАНИЯ НБУ
# К ЦСК БАНКОВ УКРАИНЫ

# Основные требования к ЦСК

- Постановление Правления НБУ от **17.06.2010 г. №284 :**

  - Об утверждении нормативно-правовых актов по вопросам функционирования электронной цифровой подписи в банковской системе Украины
  - *Положение о центрах сертификации ключей банков Украины*
  - *Правила регистрации, удостоверения действия ключа и аккредитация ЦСК банков Украины Удостоверяющем центре НБ Украины*

# Требования к ИТС ЦСК

- Положение об обеспечении непрерывного функционирования информационных систем НБУ и банков Украины (постановление Правления НБУ от **17.16.2004 г. №265** с изменениями согласно постановлению от **25.05.2015 г. №337**):

  - *Составной частью обеспечения непрерывной деятельности банков является обеспечение функционирования информационных технологий ... в частности, создание системы резервирования и восстановления функционирования САБ и информационной системы ЦСК банка ...*

# СКЗИ «ШИФР-X.509». СООТВЕТСТВИЕ ТРЕБОВАНИЯМ НБУ

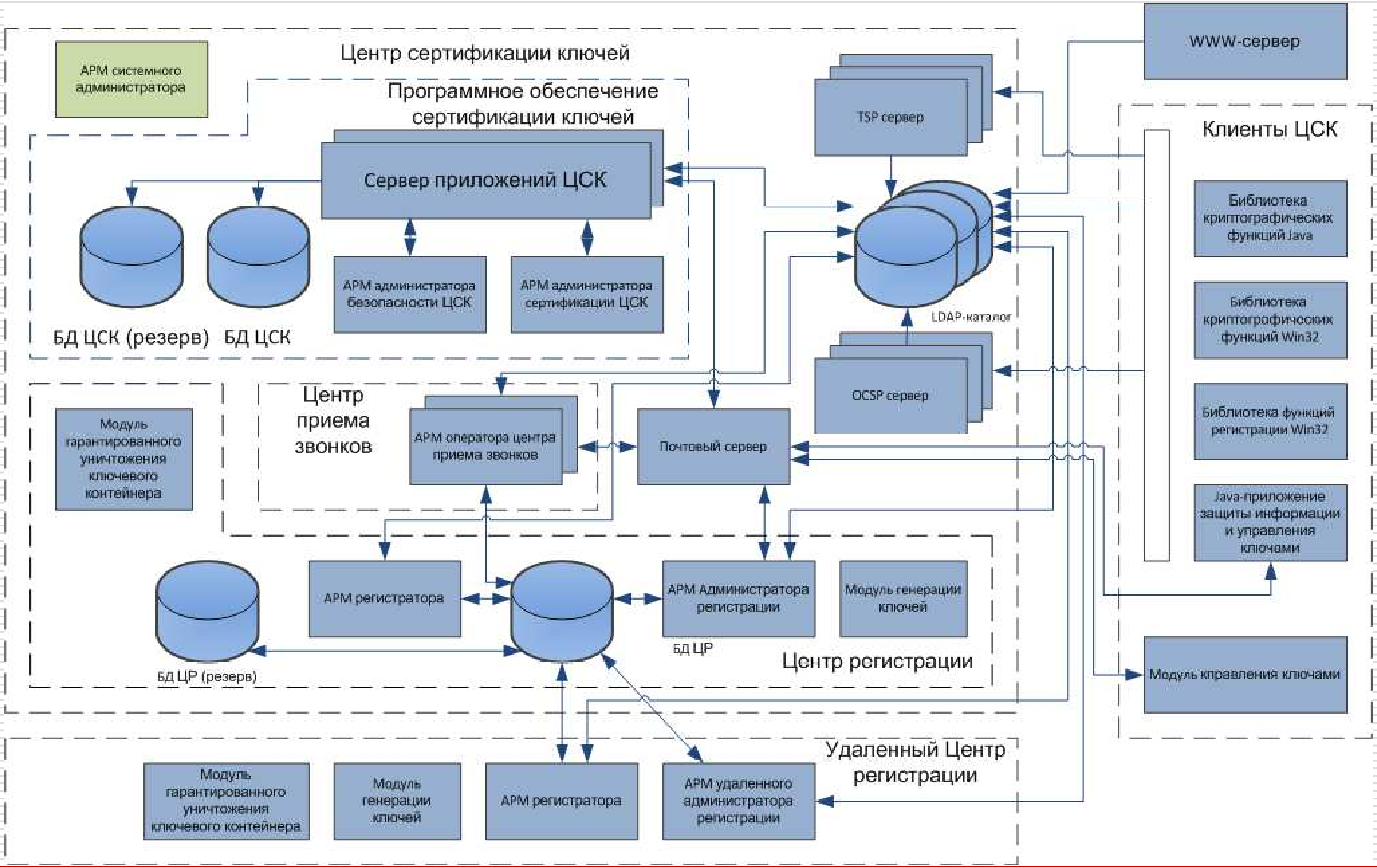
# Назначение

Управление личными ключами и сертификатами, изданными для ЭЦП и шифрования информации, согласно семейству стандартов X.509 и используется для построения центров сертификации ключей.

# Использование

- Корпоративный ЦСК
- Публичный ЦСК
  - Зарегистрированный ЦСК
  - Аккредитованный ЦСК

# Архитектура ЦСК



# Архитектура ЦСК

- Гибкая модульная архитектура
- Компоненты могут работать как в интерактивном, так и автономном режиме
- Одновременная работа нескольких экземпляров ЦСК в одном и более ЦОД
- Гарантированная доставка и обработка запросов
- Журналирование действий пользователей и событий компонентов
- Централизованная система резервного копирования с инструментами восстановления из резервных копий

# Архитектура ЦСК

- Развитая СУБД с контролем целостности данных и эффективным разграничением доступа
- Хранение данных в БД с возможностью контроля целостности и авторства через ЭЦП
- Возможность «ручного» ввода информации о фактически выполненных операциях, произошедших до инцидента
- Наличие web-сайта ЦСК с возможность публикации информации о режиме работы ЦСК

# Надежность

- С ростом нагрузки возможно горизонтальное масштабированием сервисов (LDAP, OCSP, TSP)
- Непрерывность функционирования обеспечивается резервированием сервисов

# Надежность

Непрерывность достигается:

- Мониторингом и диагностикой сервисов посредством АРМ системного администратора
- Резервированием данных посредством централизованной системы резервного копирования

# Производительность

- Эффективное управление 3 млн. и более сертификатов
- Издание 50 тыс. сертификатов в автоматическом режиме в сутки*
- OCSP – 3 тыс. запросов/с**
- TSP – 3 тыс. запросов/с**
- LDAP – 96 тыс. запросов/с**

*- Intel Xeon E3-1245 **- 2xIntel Xeon E5-2640

# СКЗИ «ШИФР-Х.509». РЕЗЕРВИРОВАНИЕ И ВОССТАНОВЛЕНИЕ

# Резервирование и восстановление

- Поддерживается работы в двух и более ЦОД
- Горизонтальное масштабирование компонентов
- Наличие централизованного хранилища эталонных дистрибутивов всех используемых приложений и ОС
- Возможность работы с несколькими подсетями
- Наличие централизованной системы резервного копирования данных ЦСК, инструментов репликации и синхронизации данных для СУБД и LDAP

# Резервирование и восстановление

- Обеспечивается целостность и конфиденциальность резервных копий посредством использования механизмов ЭЦП и шифрования
- Компонентами ЦСК обеспечивается возможность импорта и экспорта данных на носители

# Резервирование и восстановление

- Recovery Time Objective (RTO) - время, на протяжении которого следует восстановить работу ЦСК.
- Recovery Point Objective (RPO) – период времени, за который данные могут быть утрачены в случае аварии ЦСК.

# Резервирование и восстановление

| | 1 x ЦОД без дбл | 1 x ЦОД с дбл | 2 x ЦОД без дбл | 2 x ЦОД с дбл |
|---|---|---|---|---|
| RTO | 30 мин | 10 мин | 10 мин | 10 мин |
| RPO | Т мин | 0 с | 0 с | 0 с |

(1) – время восстановления БД, настроек из резервной копии, без учета времени восстановления ОС
(2) – время переключения на дублирующие сервера
(3) – время переключения на сервера резервного ЦОД
(4) – время переключения на резервный ЦОД или дублирующие сервера

* - Предполагается наличие централизованной системы резервного копирования данных ЦСК, период выполнения резервных копий – Т мин

# СКЗИ «ШИФР-X.509». МОНИТОРИНГ И ДИАГНОСТИКА

# Мониторинг и диагностика

- АРМ системного администратора ЦСК
  - Централизованный мониторинг и диагностика работоспособности компонентов ЦСК
  - Работа в режиме 24x7
  - Визуализация и оповещение о событиях и инцидентах

# АРМ системного администратора ЦСК

- Windows приложение
- Аутентификация и обеспечение целостности журналов на основе ЭЦП
- Журналы
  - Локальная БД Firebird Embedded
  - Более 20 млн. записей в сутки*
  - Работа с журналами более 5 Гб*
  - Ротация и архивация по времени
  - Работа с архивами журналов и их визуализация
- Мониторинг и диагностика всех сервисов и серверов ЦСК (более 500 серверов одновременно)*

*- Intel Core i3

# АРМ системного администратора ЦСК

- Поддержка компонентов ЦСК:
  - OCSP, TSP, LDAP
  - Сервер приложений ЦСК
  - Точное время (NTP)
  - Почтовый сервер (SMTP/POP3/IMAP)
  - Web-сервер (HTTP/HTTPS)
  - СУБД Firebird + БД Firebird v2.5+
  - СУБД Oracle + БД Oracle 11g
  - ОС: Windows/Linux/QNX/Unix (SNMP)

# СКЗИ «ШИФР-X.509». ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

# Организационно-техническое обеспечение

- Большой опыт и наработки по созданию и внедрению административно-распорядительской документации.
  - Приказы
  - Должностные инструкции
  - Регламент ЦСК
  - Технический проект ИТС ЦСК
  - План обеспечения непрерывной деятельности

# Вопросы?

Спасибо за внимание!

# ООО «САЙФЕР ЛТД»

Александр Боровиков

email: alex.borovikov@cipher.kiev.ua
www: http://www.cipher.kiev.ua