АТ “Інститут інформаційних технологій”
Харківський національний університет радіоелектроніки

ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Состояние и проблемы развития инфраструктуры открытых ключей Украины

Потий А.В. , Горбенко Ю.И.,Чичмарь С.В., Тоцкий А.С.,
Погребняк К.А., Оноприенко В.В., Горбенко И.Д.

Адреса: м. Харків, вул. Бакуліна, 12
Тел./факс: (057) 714-22-05
Web-сайт: iit.com.ua
E-mail: iit@iit.kharkov.ua

конференция РусКрипто’2013

http://www.ruscrypto.ru/conference/

Вступление

Украина сделала значительные шаги в направлении создания и совершенствования инфраструктуры открытых ключей. В информационно-телекоммуникационных системах и разнообразных технологиях должны предоставляться услуги по обеспечению безопасности обрабатываемой информации - **целостности**, **аутентичности** (подлинности), **доступности**, **неопровержимости** (наблюдательности), **конфиденциальности** и **надежности** и пр.
В существенной мере качество предоставления указанных услуг определяется **инфраструктурой открытых ключей** (ИОК), которая в Украине получила название **Система ЭЦП**. На международном уровне она является **инфраструктурой открытых ключей**.

Основные задачи в сфере ИОК

ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

1) Стандартизация и унификация криптографических примитивов, криптографических механизмов и протоколов.
2) Согласованное стандартизированное внедрения ИОК в системы электронного документооборота на разных уровнях.
3) Дальнейшее теоретическое обоснование требований и условий предоставления пользователям услуг ИОК с разными уровнями гарантий, и унификации.
4) Усовершенствование и разработка новых методов, механизмов и алгоритмов криптографических преобразований по критериям стойкости и сложности.
5) Прогнозирование развития, стандартизации, унификации и совершенствования ИОК для применения на международном уровне.
6) Практическое создание и внедрение унифицированных программно - технических комплексов ИОК различного предназначения.
7) Утверждение и введение в действие основных технических спецификаций форматов данных и протоколов взаимодействия и др.

Основные требования к ИОК

№	Группы требований	Сущность требований
1	Законодательного и нормативно - правового регулирования взаимоотношений	Регулирование взаимных отношений сторон, которые принимают участие в создании и функционировании ИОК: собственников, разработчиков, поставщиков, пользователей услугами ИОК, контролирующих органов и др.
2	Общесистемного уровня	Обоснование архитектуры ИОК с учетом задач, которые решаются на уровне государств, ведомств, организаций, учреждений и др.
3	Процедурно функциональный уровень	Определение и закрепление основных функциональных требований к системе сертификации, принятие процедур, политик (правил) обработки сертификатов.
4	Функционально - технический уровень	Определение функциональной структуры ЦС, их физической топологии, определение функциональных требований безопасности при предоставлении услуг сертификации.
5	Программно - технический уровень	Выбор и эффективная реализация аппаратных, аппаратно - программных и программных средств, а также оборудования ЦСК, в том числе средств КЗИ.

Нормативная база системы ЭЦП

1. Закон Украины «Об электронной цифровой подписи» от 22.05.2003 г.
2. Закон Украины «Об электронных документах и электронном документообороте» от 22.05.2003 г.
3. Правила усиленной сертификации. Утвержденные приказом ДСТСЗИ СБ Украины №3 от 13.01.2005 г
4. Приказ №141 от 20.07.2007 «Об утверждении Положения о порядке разработки, производства и эксплуатации средств криптографической защиты информации» Администрации Государственной службы специальной связи и защиты информации Украины.
5. Постановление Кабинета Министров Украины от 26.05.2004 г. №680 «Об утверждении Порядка наличия электронного документа (электронных данных) на определенный момент времени».
6. Постановление Кабинета Министров Украины от 13.07.2004 г. №903 «Об утверждении Порядка аккредитации центра сертификации ключей».
7. Постановление Кабинета Министров Украины от 28.10.2004 г. №1451 «Об утверждении Положения о центральном удостоверяющем органе».
8. Постановление Кабинета Министров Украины от 28.10.2004 г. №1452 «Об утверждении Порядка применения электронной цифровой подписи органами государственной власти, органами местного самоуправления, предприятиями, учреждениями и организациями государственной формы собственности».
9. Постановление Кабинета Министров Украины от 28.10.2004 г. №1453 «Об утверждении Типового порядка осуществления электронного документооборота в органах исполнительной власти».
10. Постановление Кабинета Министров Украины от 28.10.2004 г. №1454 «Об утверждении Порядка обязательной передачи документированной информации».

Национальная система ЭЦП

Госспецсвязь Украины

Центральный удостоверяющий орган

ЦСК банков

- Удостоверяющий центр НБУ
- ЦСК ПАТ "Юникредит банк" ("Укрсоцбанк")
- ЦСК ПАТ "УкрСиббанк"

Аккредитованные ЦСК

- АЦСК ЗАТ "ИОК"
- АЦСК ООО "УСЦ"
- АЦСК ООО "Арт-Мастер"
- АЦСК ГП "УСС"
- ЦСК ООО "Криптомаш"
- АЦСК ЗАО "НИИ ПИТ"
- АЦСК ОАО "НДУ"
- АЦСК Универс. Дата центр
- АЦСК Коммуникационного фондового центра
- АЦСК ООО НПФ "УНИС"
- АЦСК УЖД
- АЦСК ДОГА
- АЦСК ГСЗУ
- АЦСК ГТСУ
- АЦСК ООО УПГ
- АЦСК КБ Приватбанк
- АЦСК Интер-метл
- АЦСК УСС-Цезарис ДП УСС

Зарегистрированные ЦСК

- ЦСК ООО "Арт-Мастер"
- ЦСК ОАО "МФС"
- ЦСК ПАТ "Укрсиббанк"
- ЦСК ФБ "Перспектива"
- ЦСК ООО "УДЦ"

Пользователи услуг ЭЦП (юридические и физические лица)

Технические спецификации и форматы

Технические спецификации интерфейсов средств КЗИ.

Технические форматы представления базовых объектов национальной системы ЭЦП:

- **структура объектных идентификаторов** ;
- **формат контейнера личного ключа;**
- **протокол определения статуса сертификата** ;
- **формат подписанных данных** ;
- **формат усиленного сертификата открытого ключа** ;
- **протокол фиксирования времени.**

Технические спецификации интерфейсов средств КЗИ

Технические спецификации интерфейсов средств криптографической защиты информации, которые реализуют алгоритмы ДСТУ ГОСТ 28147:2009, ГОСТ 34.311-95, ДСТУ 4145-2002 согласно PKCS#11, определяют требования к реализации интерфейсов средств криптографической защиты информации, которые реализуют криптографические алгоритмы согласно стандартов ДСТУ ГОСТ 28147:2009, ГОСТ 34.311-95, ДСТУ 4145-2002 в соответствии с международными рекомендациями PKCS#11.

Определение единых интерфейсов средств криптографической защиты информации имеет целью определение технических условий по обеспечению совместимости средств криптографической защиты информации разных разработчиков.

Технические спецификации интерфейсов средств КЗИ

Технические спецификации основаны на;

1. Международных рекомендациях
   - Public Key Cryptography Standard #11 v2.30: Cryptographic Token Interface Standard,
2. Национальных стандартах Украины:
   - ДСТУ 4145-2002 “Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння”;
   - ДСТУ ГОСТ 28147:2009 “Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования”,
3. Межгосударственных стандартах:
   - ГОСТ 34.311-95 “Информационная технология. Криптографическая защита информации. Функция хеширования”,
4. Нормативно-правовых актах:
   - Національна система електронного цифрового підпису. Технічні специфікації форматів представлення базових об’єктів (Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, Державного департаменту з питань зв’язку та інформатизації Міністерства транспорту та зв’язку України № 99/166 від 11.09.2006);
   - Технічні специфікації форматів криптографічних повідомлень. Захищені дані (Наказ Адміністрації Державної служби спеціального зв’язку та захисту інформації України №112 від 14.05.2010, зі змінами згідно Наказу Адміністрації Державної служби спеціального зв’язку та захисту інформації України №152 від 15.06.2010);
   - Інструкція про порядок постачання і використання ключів до засобів криптографічного захисту інформації (Наказ Адміністрації Державної служби спеціального зв’язку та захисту інформації України №114 від 12.06.2007).

Технические форматы представления базовых объектов национальной системы ЭЦП

Форматы данных представлены в нотации ASN.1, определенной в международном стандарте ISO/IEC 8824 “Information technology – Open Systems Interconnection – Specification of Abstract Syntax Notation One (ASN.1)”.

Все структуры данных кодируют по правилам DER согласно ISO/IEC 8825-1:2002 “Information technology – ASN.1 Encoding Rules – Part 1: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)”

Структура объектных идентификаторов

Структура объектных идентификаторов для криптоалгоритмов, которые являются государственными стандартами (Object identifier – OID) разработана для обеспечения представления в сертификате криптоалгоритмов, которые являются государственными стандартами, их параметров, а также других данных.

Корень дерева объектных идентификаторов соответствует значению, установленному для Украины согласно стандарту ISO 3166 – 804.

Формат контейнера личного ключа.

Данные технические спецификации определяют требования к представлению контейнера личного ключа ЭЦП в виде DER кодированного блока (дальше – формат контейнера личного ключа), который содержит непосредственно значение личного ключа ЭЦП, а также набор дополнительных данных, необходимых для работы средств ЭЦП, в зашифрованном виде.

Использование контейнера позволяет хранить личные ключи ЭЦП на незащищенных носителях ключевой информации. Определение единого формата контейнера личного ключа имеет целью определение технических условий для обеспечения совместимости средств криптографической защиты информации разных разработчиков.

Формат контейнера личного ключа.

ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

- Спецификация основана на международных стандартах RFC 5208 “Public-Key Cryptography Standards (PKCS) #8: Private-Key Information Syntax Specification Version 1.2” та RFC 2898 “PKCS #5: Password-Based Cryptography Specification Version 2.0”.

- Симметричное шифрование данных контейнера и вычисление имитовставки выполняется в соответствии с криптографическими алгоритмами, определенными в ДСТУ ГОСТ 28147:2009 "Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования". Значение хеш-функции вычисляется по ГОСТ 34.311-95 “Информационная технология. Криптографическая защита информации. Функция хэширования”.

- В контейнерах могут храниться личные ключи криптографических алгоритмов, которые являются национальными стандартами или рекомендованы Администрацией Госспецсвязи.

- В каждом контейнере может содержаться только один личный ключ ЭЦП.

Протокол определения статуса сертификата .

ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

- Технические спецификации определяют процедуру интерактивного определения статуса сертификата и форматы данных.
- Технические спецификации основаны на международном стандарте RFC 2560 “Internet X.509 Public Key Infrastructure Online Certificate Status Protocol – OCSP”.
- Требования Технических спецификаций являются обязательными для программно-технических комплексов аккредитованных центров сертификации ключей, а также для других надежных средств ЭЦП. Правильность реализации протокола и приведенных форматов в средствах ЭЦП должна быть подтверждена сертификатом соответствия или положительным экспертным заключением по результатам государственной экспертизы в сфере криптографической защиты информации.

Формат подписанных данных .

- Технические спецификации определяют требования к представлению ЭЦП в виде DER-кодированного блока, который содержит непосредственно значение ЭЦП как результата криптографических преобразований набора электронных данных, а также набор дополнительных данных, необходимых для проверки электронной цифровой подписи и определения ее действительности.

- Технические спецификации основаны на международных стандартах RFC 3852 “Cryptographic Message Syntax (CMS)”, RFC 5126 “CMS Advanced Electronic Signatures” та ETSI TS 101 733 “Technical Specification. Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)”.

- ЭЦП вычисляется по криптографическим алгоритмам, определенным в ДСТУ 4145-2002 “Інформаційна технологія. Криптографічний захист інформації. Електронний цифровий підпис, що ґрунтується на еліптичних кривих”. Хеш-функция вычисляется по ГОСТ 34.311-95 “Информационная технология. Криптографическая защита информации. Функция хэширования” (далі – ГОСТ 34.311-95).

- В одном формате ЭЦП возможно использование нескольких криптографических алгоритмов согласно национальным стандартам или которые рекомендованы Администрацией Госспецсвязи.

- Требования Технических спецификаций являются обязательными для программно-технических комплексов аккредитованных центров сертификации ключей, а также для других надежных средств электронной цифровой подписи. Правильность реализации приведенных форматов в средствах ЭЦП должна быть подтверждена сертификатом соответствия или положительным экспертным заключением по результатам государственной экспертизы в сфере криптографической защиты информации. Тип формата ЭЦП выбирается зависимо от требований к хранению подписанных данных.

Формат усиленного сертификата открытого ключа

- Формат усиленного сертификата открытого ключа, основывается на национальном стандарте ДСТУ ISO/IEC 9594-8: 2006 “Інформаційні технології. Взаємозв'язок відкритих систем. Каталог. Частина 8. Основні положення щодо сертифікації відкритих ключів та атрибутів” с учетом требований к содержанию сертификата, определенных в Законе Украины “Про електронний цифровий підпис”.

- Определение формата сертификата не дублирует приведенный стандарт, а лишь описывает особенности содержимого сертификата и форматов его полей. В случае если существуют расхождения с приведенным стандартом, используются положения, которые определены в этих Технических спецификациях.

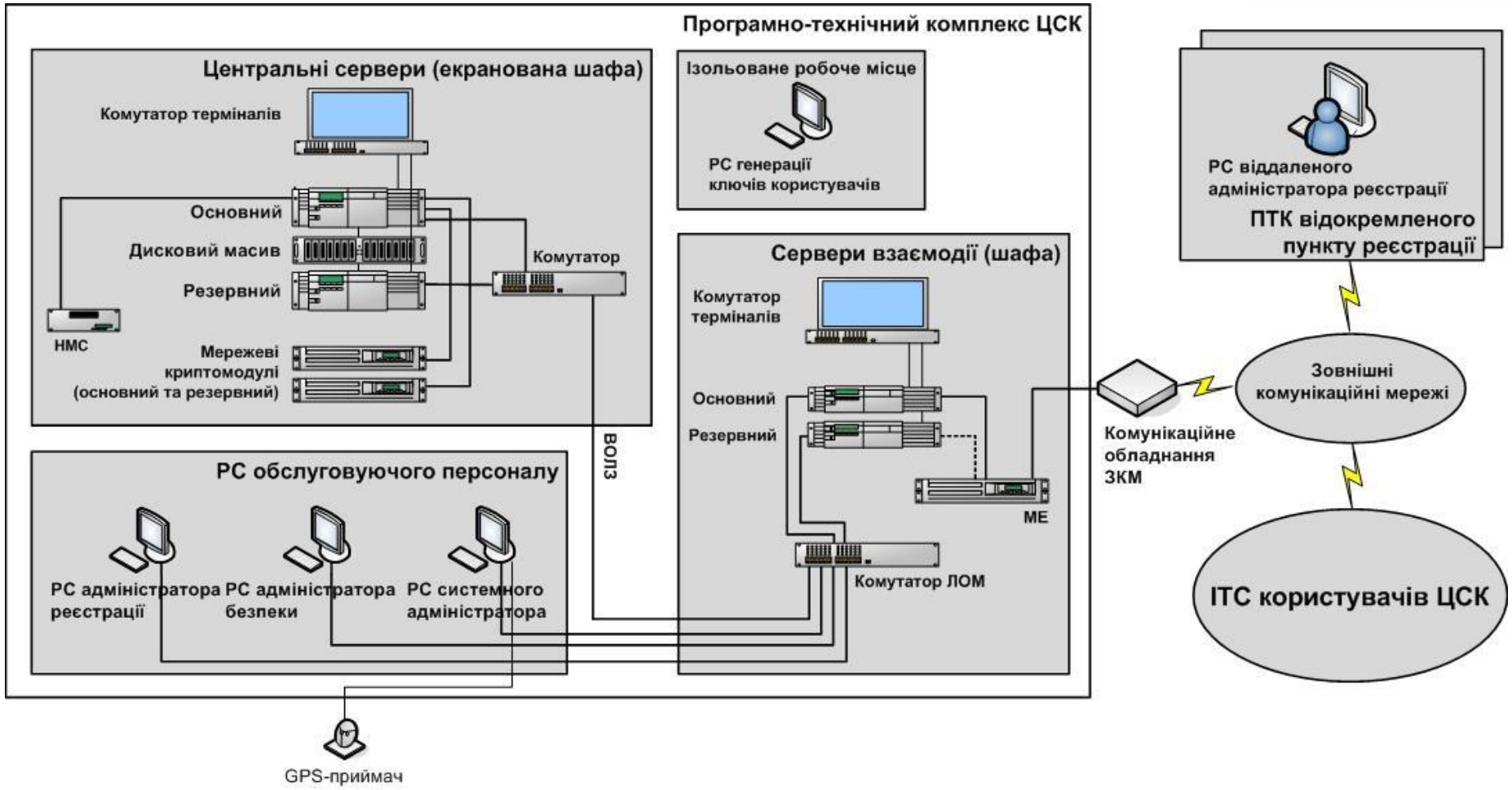
Протокол фиксирования времени.

ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

- Технические спецификации определяют процедуры формирования и проверки метки времени, форматы данных и протоколы взаимодействия субъектов в сфере услуг ЭЦП во время предоставления услуги фиксирования времени.

- Технические спецификации разработаны в соответствии с RFC 3852 “Cryptographic Message Syntax (CMS)”, RFC 3161 “Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)” та ISO/IEC 18014 “Information technology – Security techniques – Time-stamping services”.

Центр сертификации ключей



Центр сертификации ключей

Центр сертификации ключей (ЦСК) предназначен для **обслуживания сертификатов** открытых ключей пользователей и **фиксации времени**.

ЦСК обеспечивает:

- обслуживание сертификатов пользователей, включая:
  - **регистрацию пользователей;**
  - **сертификацию** открытых ключей пользователей;
  - **распространение сертификатов** через информационный ресурс - web-сайт и **LDAP**-каталог, а также по протоколу **CMP;**
  - **управление статусом сертификатов** и **распространение информации про статус** сертификатов через списки отозванных сертификатов на информационном ресурсе и по протоколу **OCSP**;
- фиксация времени (**формирование меток времени**).

Центр сертификации ключей

ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

- Программный комплекс **ЦСК** “ІІТ ЦСК-2” (программные комплексы центрального сервера, сервера взаимодействия, администраторов ЦСК и удаленного администратора регистрации).
- Программный комплекс **пользователя ЦСК** “ІІТ Користувач ЦСК-2” (средства КЗИ – электронной цифровой подписи, шифрования и аутентификации, в т.ч. **библиотеки пользователя ЦСК**).
- Аппаратные **криптомодули** “Гряда-52” та “Гряда-61”.
- Сетевой **криптомодуль** “Гряда-301”.
- **Электронный ключ** “Кристал-1”.
- **Смарт-карта** “Карта-1”.

Криптографические алгоритмы и протоколы

ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

- Шифрование по **ДСТУ ГОСТ 28147:2009**.
- Электронная цифровая подпись (ЭЦП) по **ДСТУ 4145-2002**.
- Хеширование по **ГОСТ 34.311-95**.
- Протокол распределения ключевых данных по **ДСТУ ISO/IEC 15946-3 и** государственным техническим спецификациям.
- Протокол взаимной аутентификации по **ДСТУ ISO/IEC 9798-3**.

- Шифрование **TDEA** та **AES** за ISO/IEC 18033-3.
- **ЭЦП RSA** по ISO/IEC 14888-2:2008 и PKCS#1, **DSA** по ISO/IEC 14888-3 и **ECDSA** по ISO/IEC 15946-2.
- Протоколы распределения ключевых данных **DH** по ISO/IEC 11770-3:2008, **ECDH** по ISO/IEC 15946-3.
- Хеширование **SHA** по ISO/IEC 10118-3:2004.

Форматы данных и протоколы взаимодействия

- **Сертификаты** и списки отозванных сертификатов (**СОС**) согласно ISO/IEC 9594-8 и государственным техническим спецификациям.
- Протокол **OCSP** (определения статуса сертификата) согласно RFC 2560 и государственным техническим спецификациям.
- Протокол **TSP** (фиксации времени) согласно RFC 3161 и государственным техническим спецификациям.
- **Подписанные данные** (данные с ЭЦП) согласно ETSI TS 101 733 (CAdES), RFC 5652 и государственным техническим спецификациям.
- **Защищенные данные** (зашифрованные данные) согласно RFC 5652 и государственным техническим спецификациям.
- **Личные ключи** согласно PKCS#8 и PKCS#12.

Носители ключевой информации и криптомодули

ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

- **Электронные диски** (flash-диски).
- **Оптические компакт-диски** (CD/DVD).
- Файловая система (постоянные или съемные диски).
- **Электронные ключи** “Кристал-1”, Технотрейд uaToken, Aladdin eToken, Автор SecureToken та CIC Almaz.
- **Смарт-карты** “Карта-1”, Aladdin, Автор и Криптомаш.
- **Криптомодули** “Гряда-52” и “Гряда-61” и сетевой криптомодуль “Гряда-301”.
- Другие носители и криптомодули с библиотеками поддержки.

Криптомодули (аппаратные средства защиты)

Криптомодуль “Гряда-52”

Интерфейс: PCI-E

Аппаратно реализует криптографические преобразования.

Используется в составе центральных серверов ЦСК или РС администратора сертификации и обеспечивает защиту личного ключа ЦСК.

Личный ключ ЦСК генерируется, хранится и используется только внутри устройства.

Применяется в составе серверов АБС/ИБС для реализации криптографических преобразований и защиты личных ключей серверных частей прикладных систем.

Криптомодули (аппаратные средства защиты)

Криптомодуль “Гряда-61”

Интерфейс: USB

Аппаратно реализует криптографические преобразования.

Применяется в составе РС администратора сертификации и обеспечивает защиту личного ключа ЦСК.

Личный ключ ЦСК генерируется, хранится и применяется только внутри устройства.

Применяется в составе серверов и РС пользователей АБС/ИБС для реализации криптографических преобразований и защиты личных ключей составных частей прикладных систем.

Криптомодули (аппаратные средства защиты)

Сетевой криптомодуль “Гряда-301”

Интерфейсы: 2 x Ethernet 100/1000 Мбит (основной та кластерный)

Быстродействие: 1200 ЭЦП/с, 600 распределений ключей/с

Аппаратно-програмно реализует криптографические преобразования.

Применяется в составе центральных серверов ЦСК и обеспечивает защиту личных ключей серверов ЦСК (CMP, TSP и OCSP).

Личные ключи серверов ЦСК генерируются, хранятся и используются только внутри устройства.

Применяется в составе серверов АБС/ИБС для реализации криптографических преобразований и защиты личных ключей серверных частей прикладных систем.

Апаратні засоби

Електронний ключ “Кристал-1”

Інтерфейс: USB

Швидкість формування ЕЦП: 100 мс/ЕЦП

Швидкість формування спільного секрету: 800 мс/формування

Апаратно реалізує криптографічні перетворення.

Апаратна реалізація забезпечує захищеність процесу виконання криптографічних перетворень та унеможливлює доступ до особистих ключів з боку зовнішнього апаратного-програмно середовища.

Аппаратные средства защиты

Смарт-карта “Карта-1”

Интерфейс: контактный

Скорость формирования ЭЦП: 200 мс/ЭЦП

Аппаратно реализует криптографические преобразования.

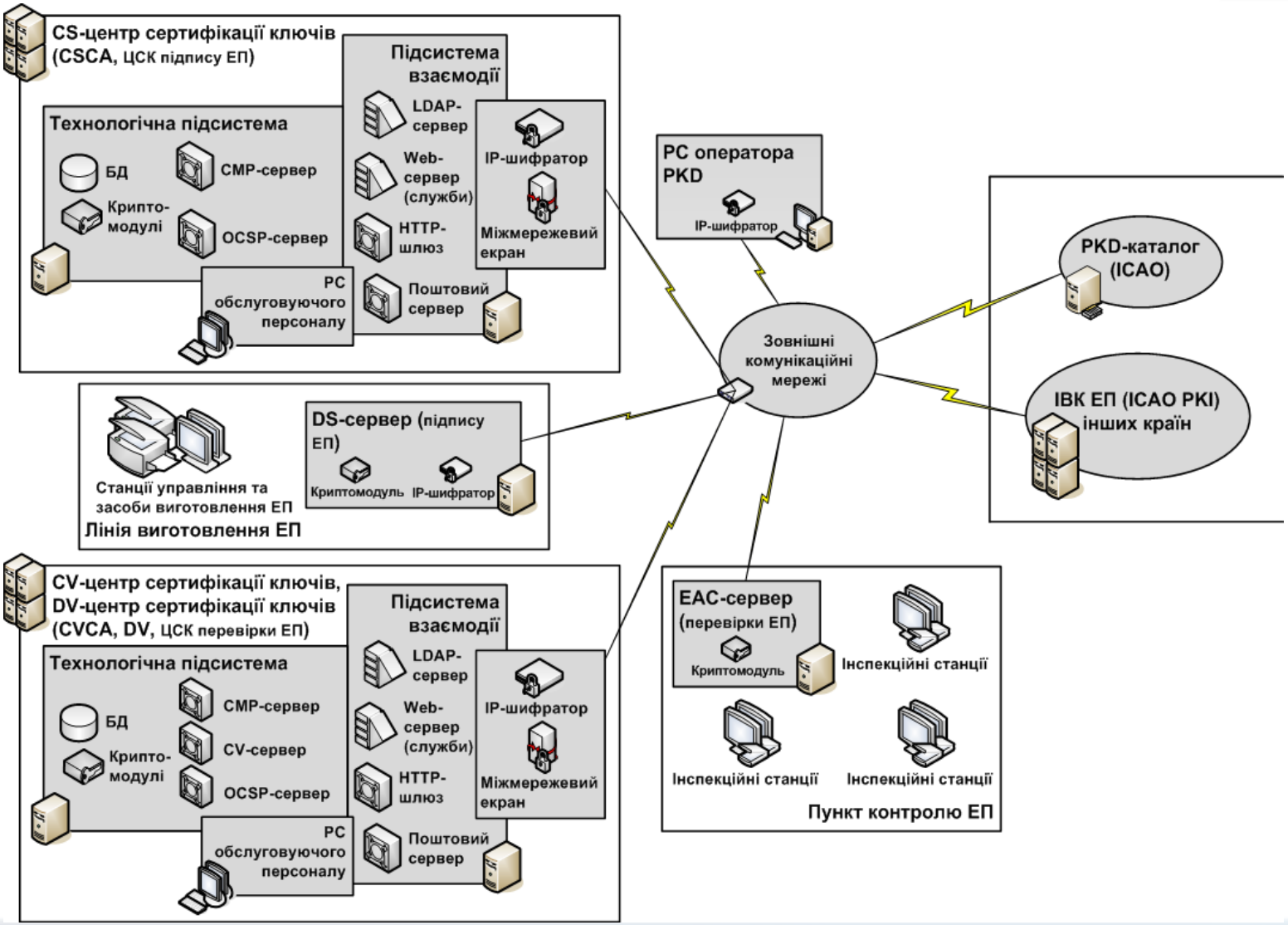
Применяется в качестве носителя личных ключей пользователей АБС/ИБС для реализации криптографических преобразований и защиты личных ключей пользователей.

Аппаратная реализация обеспечивает защищенность процесса выполнения криптографических преобразований и делает невозможным доступ к личным ключам со стороны внешней аппаратно-програмной среды.

ИОК паспортной системы

Непосредственно ИОК Украины создается, как составная часть системы изготовления и применения биометрических паспортов в соответствии с техническими требованиями ICAO.
Ее основой является программно - технический комплекс.
Комплекс и его составные части должны соответствовать техническим требованиям ICAO и правилам усиленной сертификации. Он также должен обеспечить реализацию регламентных процедур и механизмов функционирования ИОК относительно обслуживания сертификатов открытых ключей; предоставление средств КЗИ для использования в составных частях инфраструктуры при изготовлении и проверки биометрических паспортов.

Функциональная схема ИОК для биометрического паспорта



Основные характеристики ПТК для паспортной системы

- число одновременных подключений к серверам взаимодействия CS-ЦСК и CV / DV-ЦСК - LDAP-каталога и web-страницы - не менее 1 000;
- время обработки ЦСК запросов на формирование, блокирование, обновления и отмены сертификатов - не более 1 с (не менее 20 запросов / с);
- время обработки ЦСК запросов на определение статуса сертификата - не более 1 с (не менее 100 запросов / с);
- время формирования ЭЦП при подписи данных паспорта не более 0.05 с (не менее 20 запросов / с);
- количество одновременных подключений к серверам взаимодействия CS-ЦСК и CV / DV-ЦСК - LDAP-каталога и web-страницы) не менее 1 000;
- время обработки ЦСК запросов на формирование, блокирование, обновления и отмены сертификатов- не более 1 с (не менее 20 запросов / с);
- время обработки ЦСК запросов на определение статуса сертификата не более 1 с (не менее 100 запросов / с);
- время формирования ЭЦП при подписи данных паспорта не более 0.05 с (не менее 20 запросов / с).

Основные характеристики ПТК для паспортной системы

Для определения степени выполнения и функциональных требований были использованы, в соответствии со стандартом ISO / IEC 15408 (Common Criteria for Information Technology Security Evaluation), критерии оценки электронных проездных документов.

Применение стандарта ISO / IEC 15408 позволяет обеспечить условия, в которых процесс описания, разработки и проверки продукта будет произведен с выполнением необходимых требований.

Сущность и применение ИОК в АБС

Центр сертификации ключей

Обеспечивает обслуживание сертификатов и фиксирование времени

Средства криптографической защиты информации (КЗИ)

Обеспечивают **целостность и неопровержимость** авторства электронных данных и документов с использованием механизмов э**лектронной цифровой подписи** (ЭЦП), а также **аутентификацию** и **конфиденциальность и целостность** данных путем **шифрования** и вычисления **криптографических контрольных сумм**

Автоматизированные и интегрированные банковские системы (АБС/ИБС)

Центр сертификации ключей

Сервери ЦСК

БД, CMP-, TSP- та OCSP-сервери

Центральні сервери (кластер)

Дисковий масив

НМС

Мережні криптомодулі (кластер)

Комутатор

Міжмережний екран/IPS

Сервери взаємодії (кластер)

Web-сервер, LDAP-сервер, поштовий сервер, шлюз захисту

АБС/ІБС

Сервери та користувачі прикладних систем із засобами КЗІ

Віддалені адміністратори реєстрації

Криптомодулі

РС адміністратора безпеки

РС адміністратора сертифікації

РС адміністратора реєстрації

Робочі місця адміністраторів ЦСК