АТ “Інститут інформаційних технологій”
Адміністрація держспецзв’язку
Харківський національний університет радіоелектроніки

Національна інфраструктура відкритих ключів (PKI) як основа формування безпечного середовища бізнесу

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

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**.

Проблемные 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.

Асимметрические криптографические преобразования для ЭЦП

Параметри перетворення / Вид перетворення	Особистий ключ	Відкритий ключ (сертифікат)	Асиметрична пара (ключ)	Загальні параметри	Сертифікати	Складність криптоаналізу
Перетворення в кільці (RSA)	Di	Ei	(Ei, Di)	N = PQ	Ei	Субекспоненційна
Перетворення в полі Галуа F(P) (DSA)	Xi	$Y_i = g^{X_i} (\mathrm{mod}\, P)$	(Xi, Yi)	P, q, g	Yi	Субекспоненційна
Перетворення в групі точок еліптичних кривих E(F(q))	di	Qi= diG(modq)	(di, Qi)	a, b, G, n, f(x)(P), h	Qi	Експоненційна
Перетворення в гіпереліптичних кривих	C_i	$D_2 = c_i D1$	(ci, D2)	f(x), g(x), q, D1, g, J	D_2	Експоненційна
Перетворення зі спарюванням точок еліптичних кривих	$D_i = s\, Q_{iD}$	$Q_{iD} = H1(ID)$	(d_{iD}, Q_{iD})	G1, G2, e, H1, P, H2, H3, F^{2m}, Pp	Q_{iD}	Міжекспоненційна – субекспоненційна

Асимметрические криптографические преобразования для реализации направленного шифрования

Параметри НШ/ Математичний апарат	Особистий ключ НРШ	Відкритий ключ НЗШ (сертифікат)	Асиметрична пара (ключ)	Загальні параметри крипто перетворення	Сертифікати	Складність крипто аналізу
НШ в кільці (RSA)	D_i	E_i	(D_i, E_i)	$N = P\ Q$	E_i	Субекспоненційна
НШ в полі Галуа $F(P)$	X_i	$Y_i = g^{X_i} (\mathrm{mod}\ P)$	(X_i, Y_i)	P, q, g	Y_i	Субекспоненційна
НШ в групі точок еліптичних кривих $E(F(q))$	d_i	$Q_i = d_i G (\mathrm{mod} q)$	(d_i, Q_i)	$a, b, G, n, f(x)(P), h$	Q_i	Експоненційна
НШ в гіпереліптичних кривих	C_i	$D_2 = c_i D_1$	(c_i, D_2)	$f(x), g(x), q, D_1, g, J$	D_2	Експоненційна
НШ зі спарюванням точок еліптичних кривих	$d_{iD} = s\ Q_{iD}$	$Q_{iD} = H_1(ID)$	(d_{iD}, Q_{iD})	$G_1, G_2, e, H_1, P, H_2, H_3, F_2^m, P_p$	Q_{iD}	Експоненційна – субекспоненційна
НШ в кільці зрізаних поліномів (NTRU)	$f = 1 + pF (\mathrm{mod}\ q)$	$h = f^{-1} * g * p (\mathrm{mod} q)$	(f, h)	N, q, p, f, g, df, dg, c		Експоненційна – субекспоненційна

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 форматов представления базовых объектов национальной системы ЭЦП (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.

Технические спецификации форматов представления базовых объектов национальной системы ЭЦП (структура объектных идентификаторов для криптоалгоритмов, которые являются государственными стандартами).

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 отвечает значению, установленному для Украины согласно стандарту ISO 3166 – 804.

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.**

Национальная система ЭЦП

Госспецсвязь Украины

Центральный удостоверяющий орган

Удостоверяющий центр НБУ

ЦСК банков

- 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)

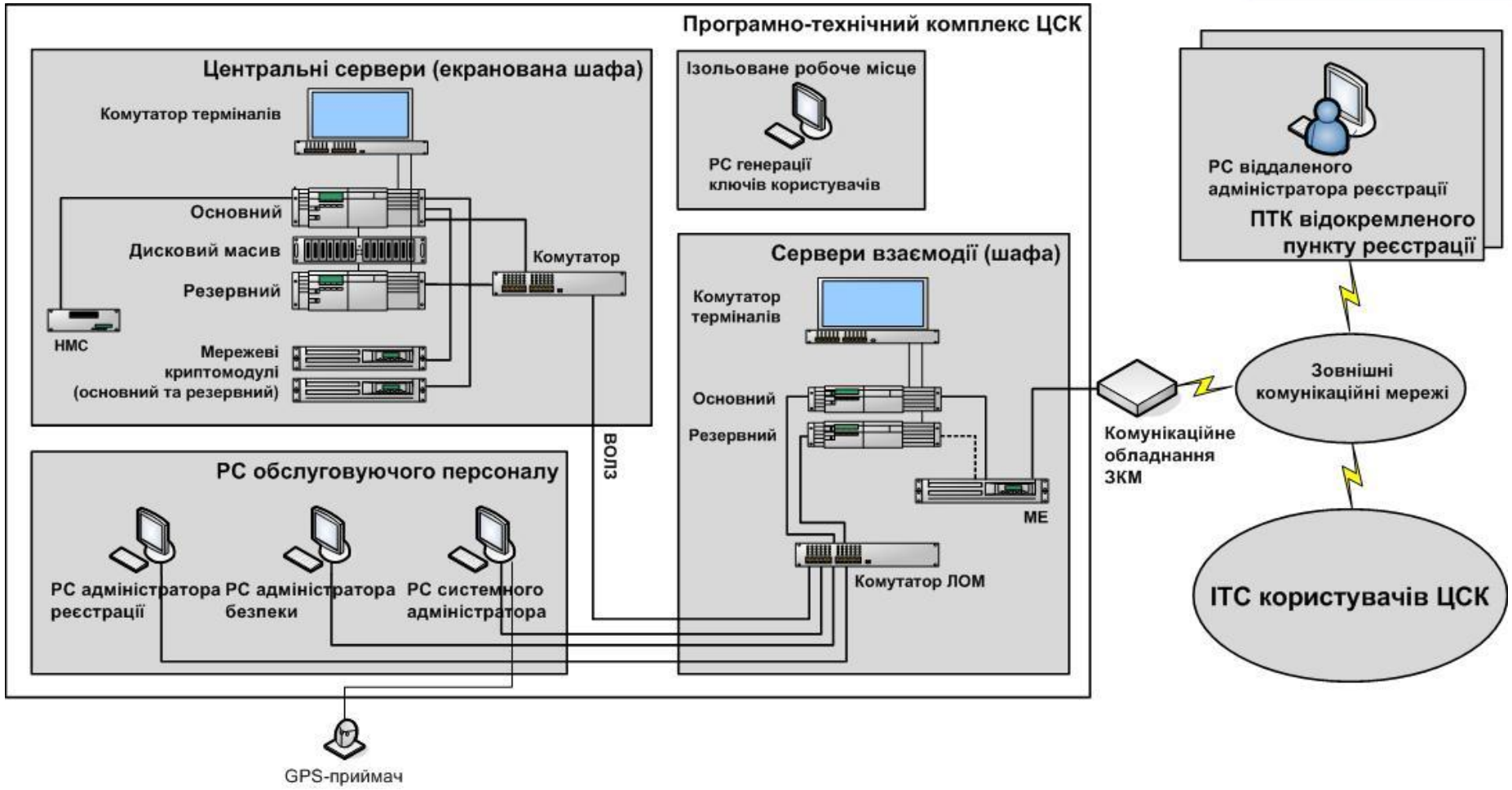
Центр сертификации ключей

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

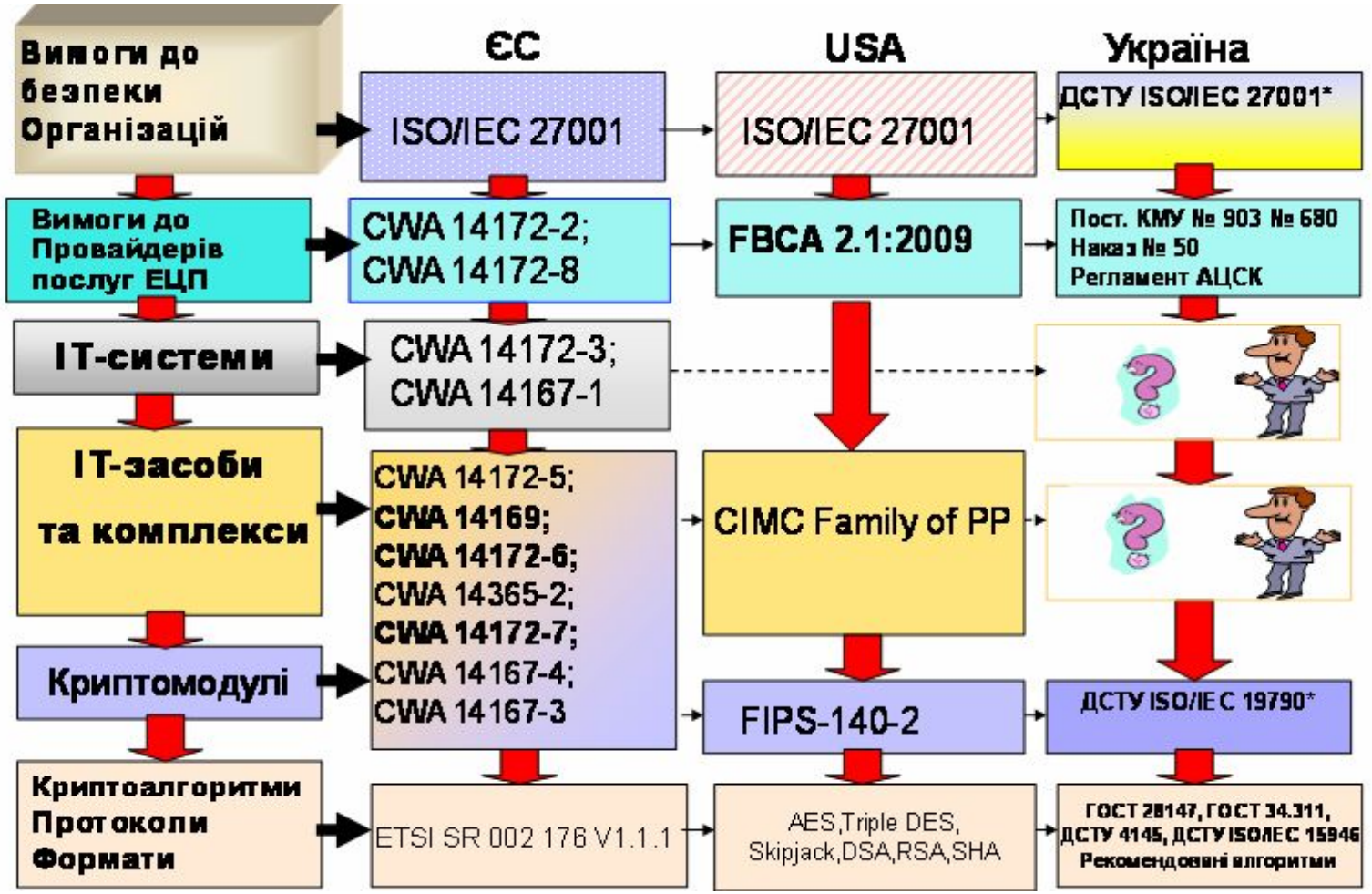
ЦСК обеспечивает:

- 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**)**.**

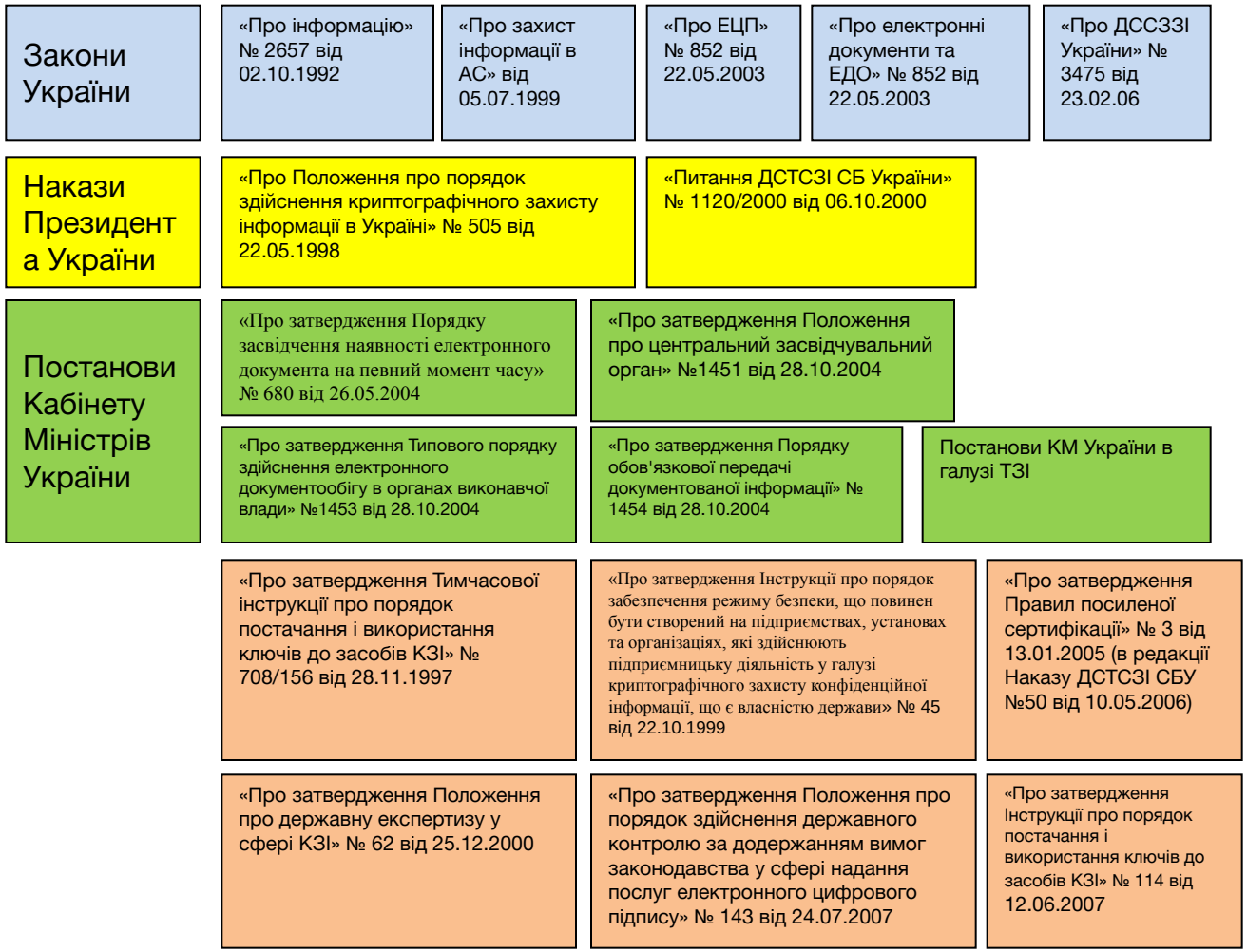
Центр сертификации ключей



Підходи до побудови та забезпечення безпеки PKI-структур



Нормативно-правове забезпечення ЕЦП України



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

- 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

ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

- **Сертификаты** и списки отозванных сертификатов (**COC**) 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

- **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 криптографически е 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.

Аппаратные средства защиты

Электронный ключ “Кристал-1”

Интерфейс: USB

Скорость формирования ЭЦП: 100 мс/ЭЦП

Скорость распределения ключей: 800 мс/распределение

Аппаратно реализует криптографические преобразования.

Применяется в качестве носителя служебных личных ключей администраторов ЦСК.

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

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.

Аппаратные средства защиты

Смарт-карта “Карта-1”

Интерфейс: контактный

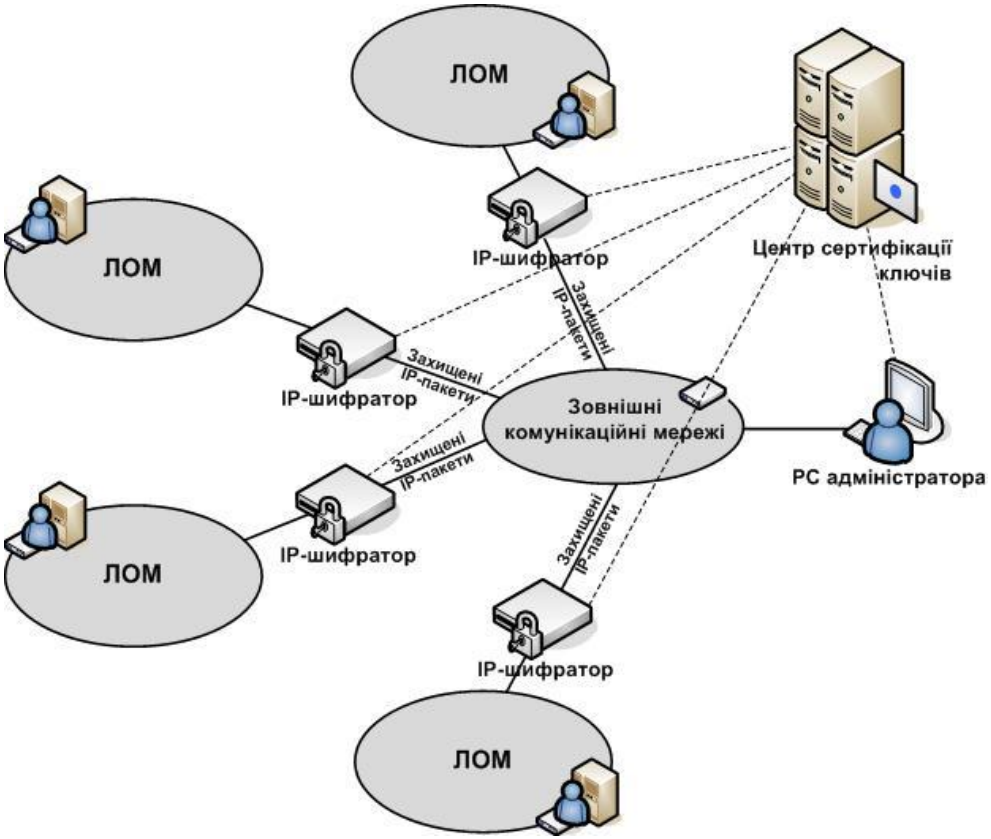
Скорость формирования ЭЦП: 200 мс/ЭЦП

Аппаратно реализует криптографические преобразования.

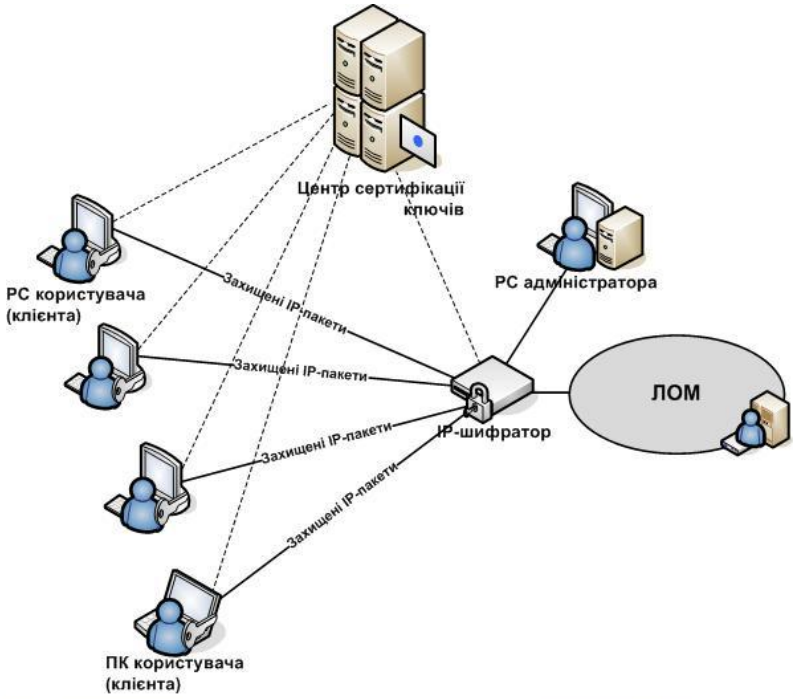
Применяется в качестве носителя личных ключей пользователей АБС/ИБС для реализации криптографических преобразований и защиты личных ключей пользователей.

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

Комплекс захисту інформації у IP-мережах



Забезпечує **шифрування** та **контроль цілісності** потоку **IP-пакетів** між ЛОМ або між клієнтами та ЛОМ. Захист ЛОМ реалізують **IP-шифратори**.



IP-шифратори

IP-шифратор “Канал-**201**”

Інтерфейси: 2 x Ethernet 100/1000 Мбіт (RJ-45)

Швидікість: до 100 Мбіт/с

IP-шифратор “Канал-**301**”

Інтерфейси: 2 x Ethernet 100/1000 Мбіт (RJ-45)

Швидікість: до 250 Мбіт/с

IP-шифратор “Канал-**401**”

Інтерфейси: 2 x Ethernet 100/1000 Мбіт (2 RJ-45 та 2 LC)

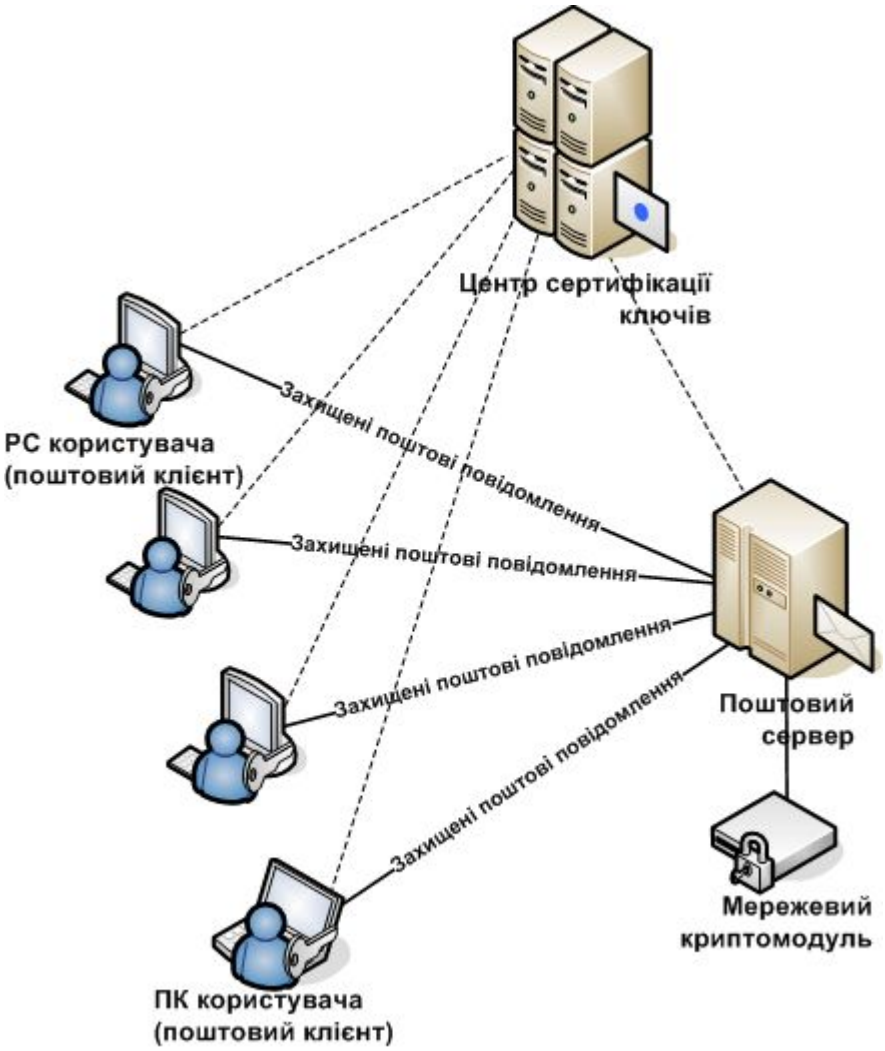
Швидікість: до 350 Мбіт/с

Забезпечують шифрування та контроль цілісності потоку IP-пакетів, що передаються через нього.

Функції:

- **шифрування та контроль цілісності IP-пакетів;**
- **інкапсуляцію IP-пакетів та їх маршрутизацію між мережевими інтерфейсами;**
- **приймання та передачу технологічної (управляючої) інформації;**
- **прийом та введення в дію ключових даних;**
- **встановлення захищених з’єднань з іншими IP-шифраторами.**

Комплекс захисту електронної пошти

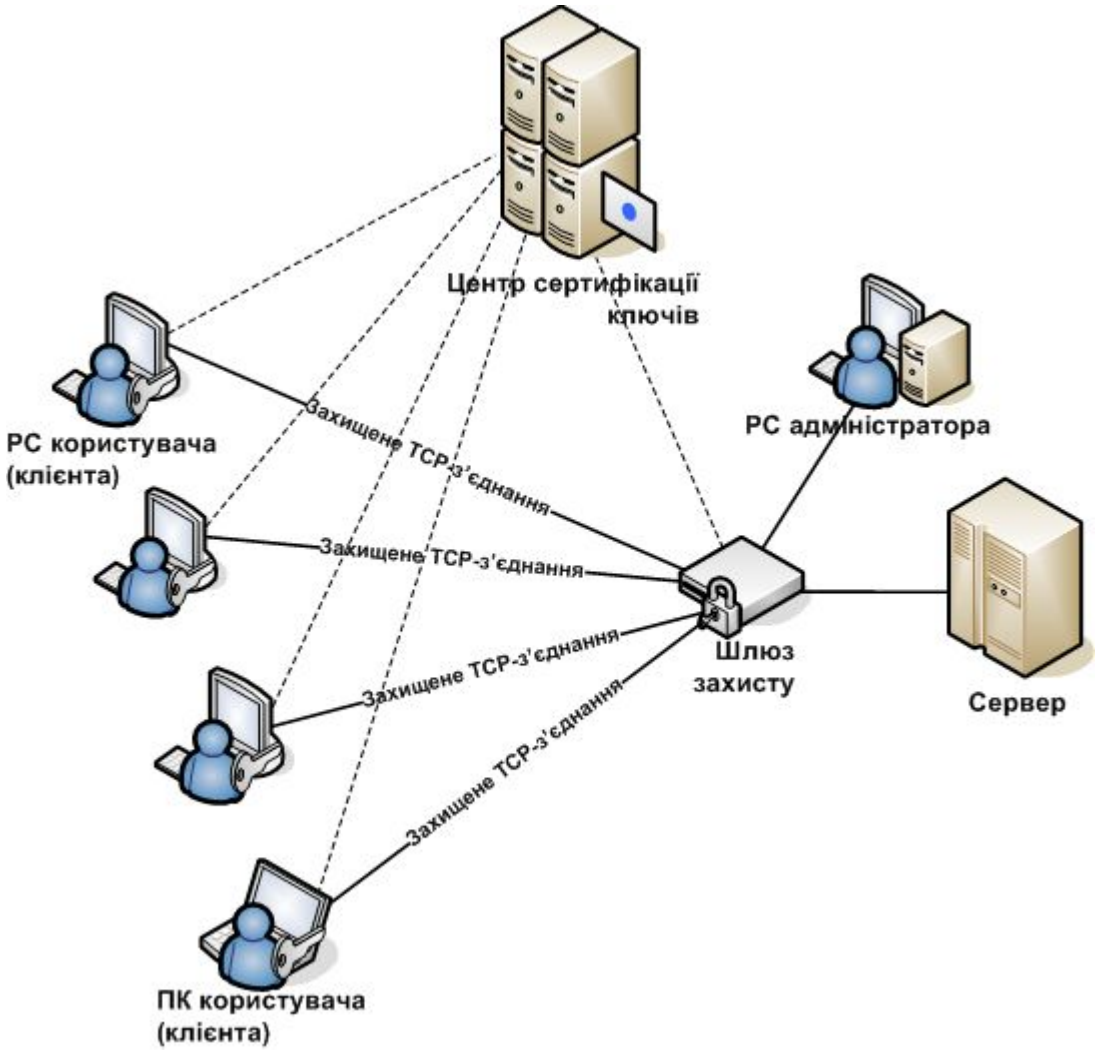


Забезпечує:

- **підпис** повідомлень з використанням **електронного цифрового підпису;**
- **шифрування** повідомлень користувача у поштовому клієнті при передачі та зберіганні.

Інтегровано у **поштові клієнти** Microsoft Outlook, IBM Lotus Notes, Авіаінтур Захід, ФОСС FOSS-Mail.

Комплекс захисту TCP-з’єднань



Забезпечує:

- **автентифікацію** клієнтів та встановлення **захищеного** з’єднання;
- **шифрування** даних з’єднання.

Шлюз захисту

Шлюз захисту
“Бар’єр-301”

Інтерфейси: 2 x Ethernet 1000 Мбіт (RJ-45)

Швидікість: до 250 Мбіт/с

Забезпечує до 100 автентифікацій/с

Забезпечує:

- **автентифікацію клієнтів та встановлення захищеного з’єднання;**
- **шифрування даних з’єднання;**
- **приймання та передачу технологічної (управляючої) інформації;**
- **прийом та введення в дію ключових даних.**

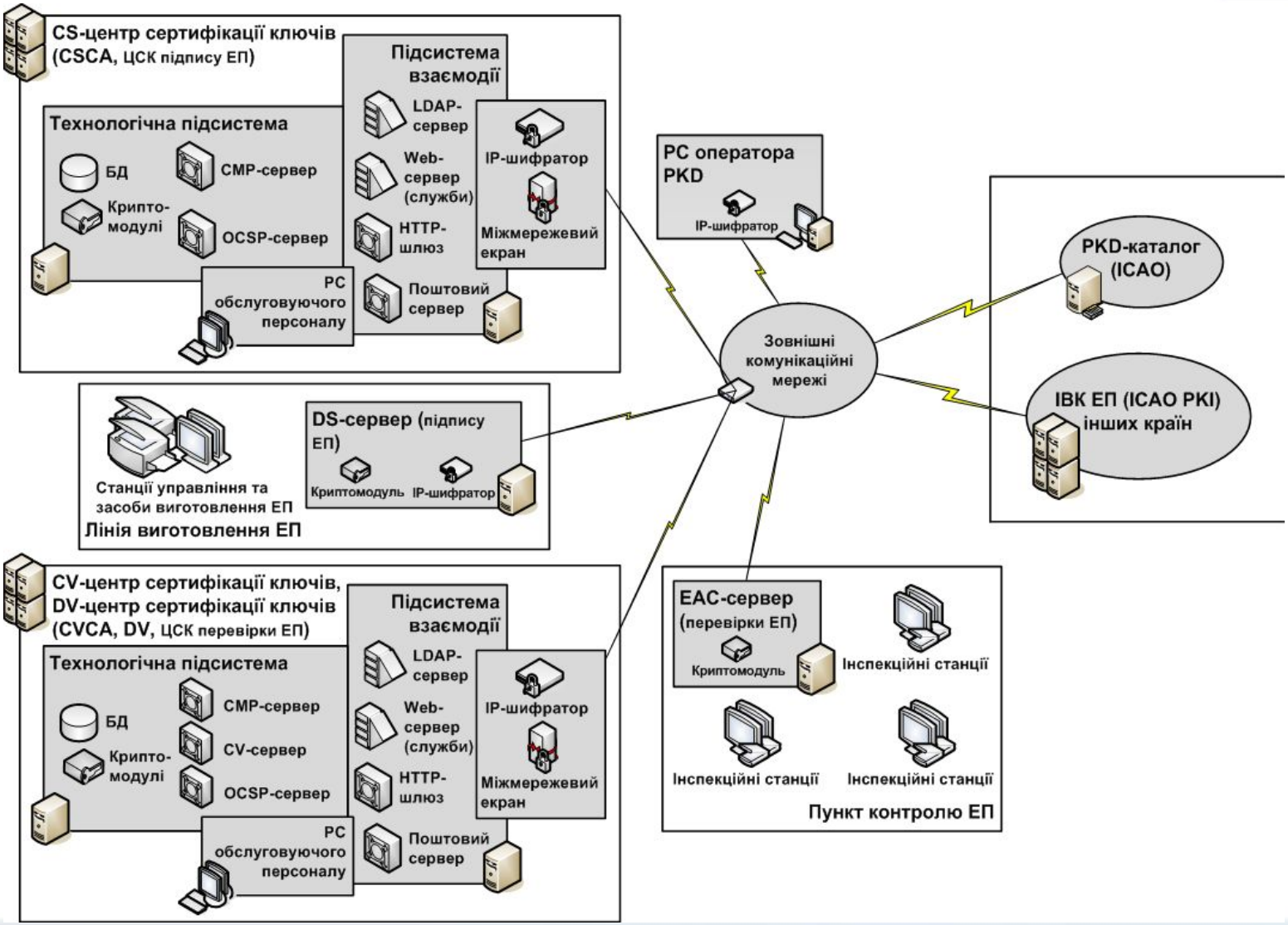
ИОК паспортной системы

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.

Состав ИОК для паспортной системы

- Компонента CSCA (ПТК CS-центра сертификации ключей – ЦСК подписи МЗПД);
- Компонента DS (DS-сервер, программные средства для станций изготовления МЗПД);
- Компонента CIL (рабочая станция оператора PKD);
- Компонента DV (ПТК DV-центра сертификации ключей);
- Компонента CVCA (ПТК CV-центра сертификации ключей);
- Компонента Сервер-концентратор EAC (EAC-сервер);
- Компонента Модуль обслуживания IS (Средства для инспекционных станций).

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**

Автоматизированные и интегрированные банковские системы (АБС/ИБС)

Центр сертификации ключей

Основные направления развития и усовершенствование ИОК

Перспективная система шифрования на основе NTRU

Параметр	Коротке пояснення параметру
N	Розмір усіченого кільця многочленів R. Елементи кільця представлені у вигляді поліномів ступеня N – 1(не секретний)
q	Великий модуль по якому приводиться кожний коефіцієнт многочлена у кільці R (не секретний)
p	Малий модуль по якому приводиться кожний многочлен (не секретний)
f	Многочлен, який є секретним ключем
g	Многочлен, який використовується для генерації публічного ключа h з f (секретний але відкидається після першого використання)
h	Публічний ключ, теж многочлен
r	Випадковий «забілюючий» многочлен (секретний але відкидається після першого використання)
df	f має df коефіцієнти еквівалентні 1 та df-1 коефіцієнти еквівалентні - 1
dg	g має dg коефіцієнти еквівалентні 1 та dg коефіцієнти еквівалентні - 1
dr	r має dr коефіцієнти еквівалентні 1 та dr коефіцієнти еквівалентні - 1

Основное преимущество, в том числе и относительно криптосистем на эллиптических кривых, есть возможность увеличения скорости на 2–3 порядка

NTRU

- NTRU – Nth Degree Truncated Polynomial Ring Units. Все операции производятся в кольце усеченных многочленов (R=Z[X]/(X^N-1));
- NTRU — первая криптосистема с открытым ключом, основанная не на задачах факторизации или дискретного логарифмирования;
- Криптографическая стойкость NTRU основана на сложности задачи нахождения короткого вектора в заданной решётке.
- Включен в IEEE 1363.1 «Lattice-based public-key cryptography» (2008);
- Модифицированная версия является основой стандарта ANSI X9.98-2010 «Lattice-Based Polynomial Public Key Establishment Algorithm for the Financial Services Industry».

NTRU

ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Все алгоритмы были реализованы на языке C, тестовый стенд имел частоту процессора 2 ГГц.

Уровень стойкости, бит	Операций/с		
	NTRU	ECC	RSA
112	10638	951	156
128	9901	650	12
192	6849	285	8
256	5000	116	1

1. При сопоставимых уровнях стойкости примерно в **300/100 раз быстрее** ECDH (зашифр./расшифр. соответственно);
2. Выполняет операцию расшифрования **в 125 раз быстрее**, чем RSA.
3. Осуществляет генерацию ключей более, чем **в 300 раз быстрее** по сравнению с RSA.

NTRU. Результаты исследования способности ассиметричных алгоритмов к распараллеливанию

- Распараллеленная с помощью технологии CUDA реализация NTRU **до 20 раз быстрее**, чем реализация ECC-NIST-224.
- Выигрыш от распараллеливания RSA фактически отсутствует: его реализация на CUDA **в 230 раз медленнее** аналогичной реализации NTRU.