ДКПП 72.20.21

УКНД 35.240.01

ЗАРЕЄСТРОВАНО

ПОГОДЖЕНО

Перший заступник Голови
Державної служби спеціального
зв'язку та захисту інформації України

_____ **О.В. Корнейко**
"___" _____ 2014 р.

ЗАТВЕРДЖУЮ

Генеральний директор
ТОВ «Базис»

_____ **А.В. Лясковський**
"___" _____ 2014 р.

Виріб програмний
Криптографічний сервіс-провайдер
«Цезаріс-CSP-JM»

ТЕХНІЧНІ УМОВИ
ТУ У 72.2-31085786-001:2014

(Введено уперше)
Дата надання чинності
"___" _____ 2014 р.
Без обмеження чинності

ПОГОДЖЕНО

Перший заступник головного
державного санітарного лікаря
України
Висновком № _____
від "___" _____ 2014 р.

РОЗРОБЛЕНО

Директор технічний
ТОВ «Базис», к.ф.-м.н.

_____ С.В. Мартиненко
"___" _____ 2014 р.

2014

ЗМІСТ

С.

1. СФЕРА ЗАСТОСУВАННЯ

Ці технічні умови (ТУ) поширюються на виріб програмний Криптографічний сервіс-провайдер «Цезаріс-CSP-JM» (далі за текстом – Криптопровайдер “Цезаріс-CSP-JM”, або скорочено – Криптопровайдер).

Криптопровайдер є програмним засобом, який функціонує у середовищі операційних систем електронно-обчислювальної техніки та є єдиним виробом.

Виріб призначений для використання у складі комплексів оброблення та передавання інформації з метою забезпечення функцій криптографічного захисту інформації. Криптопровайдер призначений для його використання у програмних застосуваннях та сервісах операційних систем як сімейства Windows компанії Microsoft, так і Unix/Linux, Mac OS X систем для забезпечення генерації випадкових послідовностей, обчислення асиметричної пари ключів, обчислення особистих та відкритих (асиметричних) ключів, генерації таємних (симетричних) ключів, інтерфейсу взаємодії з носіями інформації, формування та перевіряння цифрового підпису, формування та перевіряння електронного цифрового підпису, узгодження ключів, управління сертифікатами ключів, зашифрування, розшифрування, обчислення геш-функції, формування позначки (штемпелювання) часу та інше.

Відповідно до вимог Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту конфіденційної інформації та відкритої інформації з використанням електронного цифрового підпису, затвердженого наказом Адміністрації Державної служби спеціального зв’язку та захисту інформації України №°141 від 20.07.2007, зареєстрованого в Міністерстві юстиції України від 30.07.2007 за № 862/14129, Криптопровайдер належить до програмних засобів криптографічного захисту інформації категорій "Ш", "К", "П", виду "Б", підвид Б2, класу "Б1".

Приклад познаки Криптопровайдера при його замовленні, ідентифікації та посиланнях в інших нормативних документах:

«Криптографічний сервіс-провайдер “Цезаріс-CSP-JM”. ТУ У 72.2-31085786-001:2014».

Виробником Криптопровайдеру є ТОВ “Базис”, м. Київ.

Ці ТУ є власністю ТОВ “Базис”, м. Київ і придатні для цілей сертифікації. Ці ТУ встановлюють вимоги до Криптопровайдера, що призначений для використання в Україні, а також для постачання за договором (контрактом) на експорт.

Технічні умови перевіряються регулярно, але не рідше одного разу на п’ять років після надання їм чинності або останнього перевіряння, якщо не виникає потреби перевірити їх раніше у разі приймання нормативно-правових актів, відповідних національних (міждержавних) стандартів та інших нормативних документів, якими регламентовано інші вимоги, ніж ті, що встановлені в технічних умовах.

2. НОРМАТИВНІ ПОСИЛАННЯ

У цих технічних умовах є посилання на такі нормативні документи:

«Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту конфіденційної інформації та відкритої інформації з використанням електронного цифрового підпису», затверджене наказом Адміністрації Держспецзв'язку № 141 від 20.07.2007, зареєстроване в Міністерстві юстиції України від 30.07.2007 за № 862/14129;

ДСТУ 4145-2002 – Інформаційна технологія. Криптографічний захист інформації. Електронний цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння;

ДСТУ ГОСТ 28147:2009 – Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования;

ДСТУ ISO/IEC 8824-2:2009 Інформаційні технології. Нотація абстрактного синтаксису 1 (ASN.1);

ДСТУ ISO/IEC 9594-8:2006 Інформаційні технології. Взаємозв'язок відкритих систем. Каталог. Частина 8. Основні положення щодо сертифікації відкритих ключів та атрибутів (ISO/IEC 9594-8:2001, IDT);

ДСТУ ISO/IEC 10118-1:2003 – Інформаційні технології. Методи захисту. Геш-функції. Частина 1. Загальні положення (ISO 10118-1:2000, IDT);

ДСТУ ISO/IEC 10118-2:2003 – Інформаційні технології. Методи захисту. Геш-функції. Частина 2. Геш-функції з використовуванням n-бітового блокового шифру (ISO 10118-1:2000, IDT);

ДСТУ ISO/IEC 10118-3:2005 - Інформаційні технології. Методи захисту. Геш-функції. Частина 3. Спеціалізовані геш-функції;

ДСТУ ISO/IEC 15946-3:2006 – Інформаційні технології. Методи захисту. Криптографічні методи, що ґрунтуються на еліптичних кривих. Частина 3. Установлення ключів;

ДСТУ ISO/IEC 18033-1:2009 – Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 1. Загальні положення (ISO/IEC 18033-1:2005, IDT) [1];

ДСТУ ETSI TS 102 176-1:2009 – Електронні підписи та інфраструктури (ESI). Алгоритми та параметри безпечних електронних підписів. Частина 1. Геш-функції й асиметричні алгоритми (ETSI TS 102176-1:2007, IDT);

[1] чинний з 01.01.2012 згідно з наказом Держспоживстандарту № 485 від 30.12.2009

ДСТУ ETSI TS 102 176-2:2009 – Електронні підписи та інфраструктури (ESI). Алгоритми та параметри безпечних електронних підписів. Частина 2. Протоколи безпечних каналів та алгоритми засобів створення підписів (ETSI TS 102176-2:2005, IDT);

ДСТУ 2296-93 Система сертифікації УкрСЕПРО. Знак відповідності. Форма, розміри, технічні вимоги та правила застосування;

ДСТУ 3413-96 Система сертифікації УкрСЕПРО. Порядок проведення сертифікації продукції;

ДСТУ Б А.3.2-12:2009 ССБП Системи вентиляційні. Загальні вимоги;

ГОСТ 12.1.004-91 Система стандартов безопасности труда. Пожарная безопасность. Общие требования;

ГОСТ 12.1.005-88 Система стандартов безопасности труда. Общие санитарно-гигиенические требования к воздуху рабочей зоны;

ГОСТ 12.2.032-78 ССБТ. Рабочее место при выполнении работ сидя. Общие эргономические требования;

ГОСТ 15150-69 Машины, приборы и другие технические изделия. Исполнение для разных климатических районов. Категории, условия эксплуатации, хранения и транспортирования в части воздействия;

ГОСТ 34.310-95 – Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе ассиметричного криптографического алгоритма;

ГОСТ 34.311-95 - Информационная технология. Криптографическая функция хеширования;

СНиП 2.04.05-91 Отопление, вентиляция и кондиционирование;

СНиП 2.09.02-85 Производственные здания;

ДБН В.2.5-28-2006 Інженерне обладнання будинків і споруд. Природне і штучне освітлення;

ДСанПіН 3.3.2-007-98 Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин, затверджені МОЗ України;

ДСН 3.3.6.042-99 Санітарні норми мікроклімату виробничих приміщень;

ДСН 3.3.6.096-2002 Державні санітарні норми і правила при роботі з джерелами електромагнітних полів;

ДСН 3.3.6.037-99 Державні санітарні норми виробничого шуму, ультразвуку, інфразвуку.

ДСН 3.3.2.007-98 Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин.

3. ТЕХНІЧНІ ВИМОГИ

3.1. Загальні вимоги

Криптопровайдер “Цезаріс-CSP-JM” повинен відповідати вимогам цих ТУ і комплекту експлуатаційної та програмної документації на програмний виріб відповідно до специфікації «Криптографічний сервіс-провайдер «Цезаріс-CSP-JM». Специфікація. 31085786.1КЦ.019.В1.01.1.».

3.2. Вимоги призначення

3.2.1. Криптопровайдер повинен виготовлятися та постачатися у вигляді пакету ambprovider.jar та допоміжного пакету ambasn.jar через мережу Інтернет з адреси: www.itsway.kiev.ua (далі - ВЕБ-сторінка Виробника)[2].

3.2.2. Постачання Криптопровайдера повинно здійснюватися цілодобово. За технічних причин допускається припиняти постачання Криптопровайдера на термін, що не перевищує одну добу.

3.2.3. Криптопровайдер повинен забезпечувати виконання таких функцій:

- генерацію випадкових послідовностей, таємних (симетричних) ключів, обчислення асиметричної пари ключів, узгодження ключів, обчислення та перевіряння підпису, асиметричне зашифрування та розшифрування, взаємодію із носіями інформації, експорт та імпорт відкритого/закритого ключа, експорт та імпорт ключової пари та пов’язаного сертифікату, тощо відповідно до методики, погодженої з Адміністрацією Державної служби спеціального зв’язку та захисту інформації України [1];
- формування та обробку об’єктів відповідно до вимог ДСТУ ISO/IEC 9594-8, ДСТУ ISO/IEC 8824-2, ISO/IEC 8825-1[63] та згідно з вимогами національного законодавства для об’єктів національної системи електронного цифрового підпису;
- формування та обробку об’єктів відповідно до вимог Технічного завдання «Криптографічний сервіс-провайдер «Цезаріс-CSP-JM» [2];
- зашифрування та розшифрування даних відповідно до криптографічних алгоритмів, визначених стандартом ДСТУ ГОСТ 28147 у режимах простої заміни (ECB), гамування (CFB), гамування із зворотнім зв’язком (OFB), та вироблення імітовставки (MAC);
- криптографічних алгоритмів симетричного шифрування: DES, TDEA/3DES та AES відповідно до ДСТУ ISO/IEC 18033-1, ISO/IEC 18033-3 [9]; алгоритму RC2 відповідно до RFC 2268 [16], у режимах ECB, CBC, CFB, OFB, CTR, що визначені ISO/IEC 10116 [6];
- обчислення геш-значення відповідно до ГОСТ 34.311;
- криптографічних алгоритмів геш-функцій: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 відповідно до ДСТУ ISO 10118-1, ДСТУ ISO 10118-2, ДСТУ ISO/IEC 10118-3, ДСТУ ETSI TS 102 176-1;

[2] ВЕБ-адреса Виробника може бути змінена, про що Виробник повідомляє споживачів продукції

- формування та перевіряння цифрового підпису відповідно до ДСТУ 4145-2002;
- криптографічних алгоритмів цифрового підпису:
  - алгоритму RSA, визначеного стандартом PKCS #1 v2.1 [50], відповідно до ДСТУ ETSI TS 102 176-1, ДСТУ ETSI TS 102 176-2, RFC 3447 [33];
  - алгоритму DSA відповідно до FIPS PUB 186-3 [62];
  - алгоритму ECDSA відповідно до ANSI X9.62 [64], FIPS PUB 186-3 [62], ДСТУ ETSI TS 102 176-1 та RFC 5639 [46];
  - ECGostR3410 відповідно до ГОСТ Р 34.10-2001 [5] та RFC 5832 [49];
- зашифрування та розшифрування даних за алгоритмом асиметричного шифрування: RSAEncryption відповідно до схеми RSAES-PKCS1-v1_5 та схеми RSAES-OAEP згідно з RFC 3447 [33];
- алгоритмів шифрування, заснованого на паролі, відповідно до схем PBES1 та PBES2 згідно з RFC 2898 [25], PKCS #5 v2.1 [52] та PKCS #12 v1.0 [57];
- захист ключа (wrap/unwrap) відповідно алгоритмів захисту ключа: AESWrap згідно з RFC 3394 [32]; 3DESWrap та RC2Wrap згідно з RFC 2630 [19]; CryptoProKeyWrap та Gost28147KeyWrap згідно з RFC 4357 [37];
- алгоритмів обчислення коду автентифікації повідомлень CMAC згідно з NIST SP 800-38B [58] та HMAC згідно з RFC 2104 [15] та FIPS 198-1 [61];
- криптографічних протоколів узгодження ключів (Діффі-Геллмана) згідно з ДСТУ ISO/IEC 15946-3 та додатково для алгоритмів:
  - ДСТУ 4145 [2];
  - DSA згідно з PKCS #3 [51], RFC 2631 [20], RFC 2459 [17], FIPS PUB 186-3 [62], NIST SP 800-56A [59];
  - ECDSA згідно з RFC 3278:2002 [27], RFC 3370 [31], RFC 5008 [40], RFC 5480 [45];
- криптографічного протоколу транспортування ключів (Діффі-Геллмана) для алгоритму ECGostR3410 згідно з RFC 4490 [38];
- підтримка формування та обробки форматів сертифікатів та списків відкликання з розширеннями відповідно до RFC 5280 [44], RFC 5480 [45], RFC 5758 [48] та PKCS #9 v2.0 [55];
- збереження та використання сертифікатів відкритих ключів, формати яких відповідають вимогам технічних специфікацій форматів представлення базових об’єктів національної системи електронного цифрового підпису, відповідно до вимог стандартів ДСТУ ISO/IEC 9594-8, ДСТУ ISO/IEC 8824-2, ISO/IEC 8825-1[63] та згідно з вимогами національного законодавства для об’єктів національної системи електронного цифрового підпису;
- підтримка алгоритмів синтаксису криптографічних повідомлень з розширеннями відповідно до PKCS #7 [53] та доповнення до PKCS #7 [54]; розширені сервіси безпеки (ESS) відповідно до RFC 5035 [42]; розширені сервіси безпеки для S/MIME відповідно до RFC 2634 [23]; розширений електронний підпис відповідно до ETSI TS 101 733 V1.7.4 (2008-07) [10]; а також розширення відповідно до RFC 5652 [47] та RFC 4491 [39];

- формування та обробку об’єктів криптографічних сховищ ключів:
  - PKCS12 сховище відповідно до стандарту PKCS #12 v1.0 [57] та згідно з вимогами національного законодавства для об’єктів національної системи електронного цифрового підпису;
  - PCSC сховище на смарт-картках та апаратних модулях безпеки (HSM) відповідно до стандарту PKCS #11 [56];
  - Файловий токен - сховище на будь-яких носіях типу диск, дискета, флеш-пам'ять тощо, у форматі об’єктів стандарту PKCS #11 [56] під управлінням операційної системи Windows;
- генераторів псевдо випадкових чисел:
  - DSTURandom відповідно до ДСТУ 4145;
  - Hash_DRBG відповідно до ISO/IEC 18031 [8], NIST SP 800-90 [60], ETSI SR 002 176 V1.1.1 (2003-03) [12].

- формування та обробку об’єктів національної системи електронного цифрового підпису для форматів підписаних даних відповідно до RFC 3851 [35], RFC 3852 [36], RFC 4357 [37], RFC 5126 [43], ETSI TS 101 733 [10], PKCS #7 [53];

- формування та обробку об’єктів національної системи електронного цифрового підпису для протоколу фіксування часу відповідно до ISO/IEC 18014 [7], ETSI TS 101 861 [13], ETSI TS 102 023 [14], RFC 3161 [26], RFC 3628 [34], RFC 3852 [36];

- формування та обробку об’єктів національної системи електронного цифрового підпису для протоколу визначення статусу сертифіката відповідно до RFC 2560 [18], RFC 5019 [41].

3.3. Вимоги до сумісності та працездатності

Криптопровайдер повинен бути сумісним з віртуальною машиною Java (JVM - Java Virtual Machine) версії v.1.6.0_45 (Java™ Platform Standard Edition 6) та вище виробництва корпорації Sun Microsystems® (Oracle) і бути працездатним на цих засобах.

Технічні вимоги до обчислювальної техніки, на якій працюватиме Криптопровайдер, повинні відповідати вимогам, які висуваються до такої техніки операційною системою, під управлінням якої функціонує зазначена віртуальна машина JVM.

3.4. Вимоги до реалізації та складу

Криптопровайдер повинен бути скомпільований у стандартизованому переносимому двійковому форматі (байт-коді), який представлено у вигляді файлів “.class”, зібраних у бібліотеку класів, що упаковані разом у “.jar” файл архіву (Java Archive). Зазначений “.jar” файл є інсталяційним пакетом з повним найменуванням “ambprovider.jar”.

До складу програмного забезпечення Криптопровайдеру (“.jar” файлу) повинні входити базові компоненти (класи “.class”), що вимагаються для Java криптопровайдерів відповідно до архітектури JCA/JCE (Java™ Cryptography Architecture) і забезпечують функціональність відповідно до вимог п. 3.2 цих ТУ, та інші компоненти (класи “.class”), призначені для забезпечення функціонування зазначених базових компонентів.

Допоміжні компоненти Криптопровайдера, які не призначені для криптографічних перетворень, а відповідають за оброблення ASN.1 нотації [3,4], представлені у “.jar” файлі з найменуванням “ambasn.jar”.

3.5. Вимоги надійності та безпеки експлуатації

Робота Криптопровайдера не повинна викликати спотворення інформації, збоїв та блокування роботи операційної системи та віртуальної машини Java JVM.

Криптопровайдер повинен бути стійким до відмов та відновлювати свою роботу після збоїв. Для повідомлення про результати роботи Криптопровайдер повинен надавати прикладній програмі коди завершення операцій.

Захист Криптопровайдера щодо несанкціонованих дій (захист від *порушника першого рівня*) повинен забезпечуватися організаційними засобами та контролем цілісності.

Контроль цілісності при обміні, у тому числі завантаження через Інтертнет, забезпечується накладанням цифрового підпису розробника з використанням сертифікату, виданого довіреним центром сертифікації ключів для підпису коду (Code Signing).

Контроль цілісності при експлуатації забезпечується накладанням електронного цифрового підпису розробника на сертифікаті, виданим компанією Oracle для підпису коду (Code Signing).

Контроль цілісності при експлуатації шляхом перевірки цифрового підпису забезпечується:

- при кожній ініціалізації провайдера автоматично перевіряється двигуном (engine) JCE, який входить до J2SE, та відмовляється завантажувати JCE провайдера, який не підписано відповідним кодом підпису чи цілісність провайдера порушена;
- автоматично під час ініціалізації (старту) Криптопровайдером шляхом виконання само-тестування вбудованим статичним методом AMBProvider.selfIntegrityChecking();
- будь-якою прикладною програмою, яка використовує Криптопровайдер через виклик статичного методу AMBProvider.selfIntegrityChecking();
- вручну окремою «jarsigner» утилітою, яка входить до складу JRE/JDK.

Контроль цілісності Криптопровайдера та забезпечення безпеки експлуатації повинні бути викладені у документі «Криптографічний сервіс-провайдер «Цезаріс-CSP-JM». Інструкція із забезпечення безпеки експлуатації. 31085786.1КЦ.019.I4.01.1».

3.6. Комплектність

До комплекту постачання повинно входити:

- Інсталяційний пакет “ambprovider.jar” Криптопровайдера, який містить програмні компоненти криптографічних перетворень відповідно до п. 3.2 цих ТУ;

- Інсталяційний пакет “ambasn.jar” Криптопровайдера, який містить програмні компоненти оброблення ASN.1 нотації;

- Специфікація «Криптографічний сервіс-провайдер «Цезаріс-CSP-JM». Специфікація», 31085786.1КЦ.019.В1.01.1, відповідно до ГОСТ 19.202, у вигляді PDF файлу (register.pdf);

- Інструкція з інсталяції та ініціалізації «Криптографічний сервіс-провайдер «Цезаріс-CSP-JM». Інструкція з інсталяції та ініціалізації. 31085786.1КЦ.019.I1.01.1» у вигляді PDF файлу (install.pdf);

- Інструкція із забезпечення безпеки експлуатації «Криптографічний сервіс-провайдер «Цезаріс-CSP-JM». Інструкція із забезпечення безпеки експлуатації. 31085786.1КЦ.019.I4.01.1».

- Керівництво програміста «Криптографічний сервіс-провайдер «Цезаріс-CSP-JM». Керівництво програміста. 31085786.1КЦ.019.I3.01.1», відповідно до ГОСТ 19.505, у вигляді документації, згенерованої згідно із стандартом документування Javadoc (стандарт для документування класів Java).

Інструкція з інсталяції та ініціалізації, специфікація, керівництво програміста, інструкція із забезпечення безпеки експлуатації Криптопровайдера, можуть бути доступні для перегляду на Інтернет сторінці Виробника.

Для програмних засобів та комплексів, де застосовується Криптопровайдер, додатково (якщо вимагається) повинна бути розроблена (під час створення цих програмних засобів та комплексів):

- Інструкція щодо порядку генерації ключових даних і поводження (обліку, зберігання, знищення) з ключовими документами.

3.7. Маркування

Криптопровайдер постачається користувачу через мережу Інтернет з електронної адреси, зазначеної у комплектності (див п.3.6 цих ТУ). В окремому розділі, присвяченому Криптопровайдеру, за вказаною електронною адресою повинна бути розміщена така інформація (українською та англійською мовами):

- повна назва виробу українською мовою та позначення цих ТУ: «Виріб програмний. Криптографічний сервіс-провайдер “Цезаріс-CSP-JM”, ТУ У 30.0-31085786-001:2014»;
- назва виробу англійською мовою: “Software. Cryptographic Service Provider “CESARIS-JM”;
- назва країни та підприємства виробника;
- версія виробу програмного;
- дата вироблення (день, місяць, рік);
- відомості щодо державної експертизи у сфері криптографічного захисту інформації;
- знак відповідності згідно з ДСТУ 2296 (при сертифікації).

4. ВИМОГИ БЕЗПЕКИ, ОХОРОНИ ДОВКІЛЛЯ, УТИЛІЗУВАННЯ

4.1. За ступенем впливу на життя і здоров’я споживачів і на навколишнє середовище Криптопровайдер є безпечним виробом.

4.2. Параметри виробничого процесу

4.2.1. Вимоги до виробничих приміщень відповідно до СНиП 2.09.02, до пожежної безпеки та вибухонебезпечності відповідно до ГОСТ 12.1.004.

4.2.2. Параметри опалення, вентиляційних та систем кондиціювання повинні відповідати вимогам СНиП 2.04.05 та ДСТУ Б А.3.2-12.

4.2.3. Повітря робочої зони повинне відповідати вимогам ГОСТ 12.1.005.

4.2.4. Параметри мікроклімату приміщень повинні відповідати вимогам ДСН 3.3.6.042.

4.2.5. Освітлення повинне відповідати ДБН В.2.5-28.

4.2.6. Організація робочих місць та режими праці повинні відповідати вимогам ДСН 3.3.2.007, ДСН 3.3.6.096, ДСН 3.3.6.037, ГОСТ 12.2.032.

5. ПРАВИЛА ПРИЙМАННЯ

5.1. Приймання Криптопровайдера здійснює підприємство виробник (постачальник) та споживач у відповідності до цих ТУ.

5.2. Криптопровайдер підлягає приймально-здавальним, кваліфікаційним, періодичним та типовим випробуванням та експертним дослідженням в рамках державної експертизи в сфері криптографічного захисту інформації.

5.3. Криптопровайдер не підлягає випробуванням на надійність. Відмови обчислювальної техніки, на якій використовується Криптопровайдер, не залежать від використання Криптопровайдеру та можуть бути спричинені дефектом цієї техніки або її старіння, зносом або зламом.

5.4. Приймально-здавальні випробування

5.4.1. Склад і послідовність приймально-здавальних випробувань повинні відповідати наведеним у таблиці 1.

Таблиця 1 - Склад і послідовність приймально-здавальних випробувань

Найменування випробувань (перевірок)	Номери пунктів		Вид випробувань	
	Технічних вимог	методів випробувань	Приймально-здавальні	Періодичні
1 Відповідність документації	3.1	6.2.1	+	+
2 Перевірка умов постачання	3.2.1, 3.2.2	6.2.2	+	+
3 Перевірка функціональних вимог	3.2.3	6.2.3	+	+
4 Перевірка вимог щодо сумісності	3.3	6.2.4	+	+
5 Перевірка вимог до реалізації та складу програмного забезпечення	3.4	6.2.3	+	+
6 Перевірка вимог надійності та безпеки експлуатації	3.5	6.2.7	+	+
7 Перевірка комплектності	3.6	6.2.2	+	+
8 Перевірка маркування	3.7	6.2.2	+	+
9 Перевірка комплексу за ступенем безпечності для споживачів і довкілля	4.1	6.2.5	–	–

Кінець Таблиці 1

Найменування випробувань (перевірок)	Номери пунктів		Вид випробувань	
	Технічних вимог	методів випробувань	Приймально-здавальні	Періодичні
10 Вимоги до безпеки процесу виробництва*	4.2	6.2.5, 6.2.6	–	–

Примітка: "+" – випробування проводяться, "–" – випробування не проводяться, "" – випробування проводяться при постановці на виробництво та, в подальшому, за вимогою відповідних органів держнагляду.*

5.4.2. Приймально-здавальним випробуванням підлягає кожний зразок Криптопровайдера.

5.4.3. Прийнятим вважається зразок Криптопровайдера, який витримав приймально-здавальні випробування, а також стосовно якого не було повідомлено постачальника про негативні результати випробувань протягом двох тижнів. При незадовільних результатах випробувань Криптопровайдер повертається для з'ясування причин невідповідності, їх усунення та отримання позитивних результатів випробувань.

5.5. Кваліфікаційні випробування

5.5.1. Кваліфікаційним випробуванням піддається перший зразок установчої серії (першої промислової партії), який витримав приймально-здавальні випробування, з метою визначення готовності виробництва до постачання Криптопровайдера на основі відпрацьованого виробничого процесу, що забезпечує стабільну якість. Обсяг установчої серії встановлюється актом приймання дослідного зразка.

5.5.2. Кваліфікаційні випробування організує і проводить підприємство-постачальник за участю розробника.

5.5.3. Кваліфікаційні випробування проводяться на підприємстві-постачальнику. Комісія по проведенню кваліфікаційних випробувань призначається керівником підприємства-постачальника.

5.5.4. Послідовність і обсяг кваліфікаційних випробувань повинні відповідати п.6.2 цих ТУ.

5.6. Періодичні випробування

5.6.1. Періодичні випробування проводить підприємство-постачальник.

5.6.2. Періодичні випробування проводять на одному зразку Криптопровайдера не рідше 1 разу на 3 роки у обсязі та у послідовності, що наведена у таблиці 1 цих ТУ. Під час проведення періодичних випробувань, постачання Криптопровайдера не припиняється.

5.6.3. Якщо в процесі періодичних випробувань виявлена невідповідність Криптопровайдера, то періодичні випробування повинні бути припинені. Також повинно бути припинено постачання Криптопровайдера до усунення невідповідності.

5.6.4. Після аналізу та усунення виявлених дефектів необхідно провести повторні випробування в обсязі періодичних випробувань на подвійній кількості виробів Криптопровайдера. Результати повторних випробувань вважають остаточними.

5.6.5. Результати періодичних випробувань оформляються актом.

5.6.6. Зразки Криптопровайдера, які не витримали періодичні випробування, постачанню споживачу не підлягають.

5.7. Типові випробування

5.7.1. Типові випробування проводять за програмою типових випробувань при внесені змін в програмне забезпечення Криптопровайдера, застосуванні нових технічних засобів постачання або зміни умов постачання.

5.7.2. Проведення типових випробувань включають в себе всі випробування, що проводяться під час приймально-здавальних випробувань. Додатково обов'язково проводиться перевірка сумісності та працездатності за методом, що зазначені в п.6.2.4 цих ТУ. У разі необхідності, програма проведення типових випробувань може бути розширена. У такому випадку виробник (постачальник) розробляє та затверджує окрему програму та методики типових випробувань.

5.7.3. Результат типових випробувань оформляють актом, до якого додають протоколи випробувань, які підтверджують можливість і доцільність внесення змін в програмну та експлуатаційну документацію та виготовлення комплексів із внесеними змінами.

5.8. Експертні дослідження в рамках державної експертизи в сфері криптографічного захисту інформації

5.8.1. Експертні дослідження в рамках державної експертизи в сфері криптографічного захисту інформації проводяться відповідно до вимог чинних нормативно-правових актів з питань криптографічного захисту інформації.

5.9. Сертифікаційні випробування

5.9.1. Сертифікаційні випродування проводяться згідно з ДСТУ 3413 та чинними нормативно-правовими актами у галузі криптографічного захисту інформації.

6. МЕТОДИ КОНТРОЛЮВАННЯ

6.1. Загальні положення

6.1.1. Всі випробування (контроль) повинні проводитися в нормальних кліматичних умовах згідно з ГОСТ 15150.

6.1.2. Технічні засоби, що використовуються при проведенні випробувань, повинні забезпечувати перевірку вказаного параметра. Перелік технічних засобів для випробувань приведений в додатку А.

6.1.3. При всіх видах випробувань відмовою Криптопровайдера вважають порушення його цілісності, часткове або повне порушення його працездатності, що приводить до невиконання або неправильного виконання його функцій. Не враховують відмови, спричинені помилками оператора, впливом дій навколишнього середовища, що перевищують задані, порушенням вимог, вказаних в експлуатаційній та програмній документації, а також порушення працездатності обчислювальної техніки або операційного програмного забезпечення.

6.2. Контроль на відповідність технічним вимогам

6.2.1. Відповідність вимогам документації (п. 3.1) проводиться зовнішнім оглядом, аналізом експлуатаційної та програмної документації та програмного забезпечення комплексу.

6.2.2. Відповідність умовам постачання (пп. 3.2.1, 3.2.2.), комплектності (п. 3.6) та маркування (п. 3.7) перевіряється шляхом встановлення факту можливості отримати програмне забезпечення Криптопровайдера у вигляді інсталяційного пакету, а також експлуатаційної та програмної документації через мережу Інтернет з адреси ВЕБ-сторінки Виробника, та перевіряння отриманого на відповідність вимогам пунктів 3.4 та 3.6 цих ТУ.

У разі якщо:

- інсталяційний пакет програмного забезпечення, експлуатаційну та програмну документацію на Криптопровайдер в будь-який час доби можливо скопіювати з адреси ВЕБ-сторінки Виробника;
- за адресою ВЕБ-сторінки Виробника можна отримати відомості, що зазначені у п. 3.7 цих ТУ;
- після проведення інсталяції програмного забезпечення Криптопровайдера його пакет містить компоненти відповідно до п. 3.4 цих ТУ, зробити висновок, що зразок програмного забезпечення відповідає вимогам постачання, комплектності та маркування, визначених у цих ТУ. В іншому випадку зробити висновок, що зразок комплексу не відповідає вимогам цих ТУ.

6.2.3. Відповідність функціональній призначеності здійснюється шляхом:

- здійснення перевірки відповідності Криптопровайдера вимогам щодо його комплектності;
- перевірки відповідності програмних компонентів відповідно до п. 3.4 цих ТУ за допомогою використання утиліти

com.amb.tools.ProvidersBrowser.class перевірки конфігурації та верифікації програмних компонентів (утиліта com.amb.tools.ProvidersBrowser.class поставляється у додатковому пакеті).

У разі, якщо комплектність Криптопровайдера відповідає вимогам п. 3.6 цих ТУ, а результати перевірки програмних компонентів відповідають переліку функцій, визначених у п. 3.2, зробити висновок, що зразок Криптопровайдера відповідає вимогам п. 3.2 цих ТУ.

6.2.4. Перевірку з метою визначення відповідності вимогам до сумісності (п. 3.3 цих ТУ) та працездатності проводити шляхом запуску на виконання програмного забезпечення Криптопровайдера на ПЕОМ під управлінням операційної системи, наприклад, Windows 7, з віртуальною машиною JVM JRE/JDK 1.6.0_45 (Java™ Platform Standard Edition 6) та вище та перевірки виконання функцій, що зазначені у п. 3.3 цих ТУ.

У разі, якщо виконання функцій не викликає повідомлення про помилку, зробити висновок, що програмне забезпечення Криптопровайдера сумісне з операційною системою.

6.2.5. Контроль вимог безпеки (пп. 4.1, 4.2 цих ТУ) щодо виробничого процесу при постачанні Криптопровайдера через мережу Інтернет здійснюється Органом санітарного нагляду в порядку та за методиками, розробленими Міністерством охорони здоров’я України.

6.2.6. Контроль пожежних вимог та забезпечення пожежної безпеки (п. 4.2.1 цих ТУ) при постановці на виробництво та під час виготовлення Криптопровайдера здійснюється згідно з ГОСТ 12.1.004 в порядку та за методиками Управління Державної пожежної охорони ГУ МВС України в м. Києві.

6.2.7. Контроль цілісності та забезпечення безпеки експлуатації Криптопровайдера (п. 3.5 цих ТУ) здійснюється відповідно документу «Криптографічний сервіс-провайдер «Цезаріс-CSP-JM». Інструкція із забезпечення безпеки експлуатації. 31085786.1КЦ.019.І4.01.1»

7. ТРАНСПОРТУВАННЯ І ЗБЕРІГАННЯ

7.1. Криптопровайдер постачається споживачу через мережу Інтернет з електронної адреси ВЕБ-сторінки Виробника у вигляді інсталяційного пакету “ambprovider.jar”, та додаткового пакету “ambasn.jar”, або додатково в стиснутому/упакованому форматі “*.jar.pack.gz”.

7.2. Для контролю цілісності програмного забезпечення Криптопровайдера використовуються засоби, визначені в розділі 2 (Контроль цілісності) Інструкції із забезпечення безпеки експлуатації (31085786.1КЦ.019.І4.01.1), що входить до комплекту поставки (п. 3.6 цих ТУ).

7.3. Програмне забезпечення Криптопровайдера після його копіювання у вигляді інсталяційного пакету з адреси ВЕБ-сторінки Виробника, перевірки антивірусним програмним забезпеченням (антивірусне програмне забезпечення обирається споживачем самостійно), встановлюється на обчислювальну техніку. Інстальовані програмні компоненти Криптопровайдера перевіряються на цілісність, як визначено у розділі 2 (Контроль цілісності) Інструкції із забезпечення безпеки експлуатації (31085786.1КЦ.019.І4.01.1) , що входить до комплекту поставки (п. 3.6 цих ТУ).

7.4. Криптопровайдер зберігається разом з обчислювальною технікою, на яку його було встановлено, або у вигляді інсталяційного пакету на носії інформації.

8. ВКАЗІВКИ ЩОДО ЕКСПЛУАТАЦІЇ (ЗАСТОСУВАННЯ)

8.1. Вимоги до апаратного та програмного забезпечення

Вимоги до апаратного та програмного забезпечення щодо встановлення та експлуатації Криптопровайдера.

8.1.1. Криптопровайдер призначений для його встановлення та експлуатації під управлінням будь-якої операційної системи, – Windows, Unix/Linux, Mac OS X – з віртуальною машиною JVM JRE/JDK 1.6.0_45 (Java™ Platform Standard Edition 6) і вище виробництва корпорації Oracle.

8.1.2. Конфігурація апаратного забезпечення повинна відповідати вимогам, що висуваються операційною системою та віртуальною машиною JVM JRE/JDK.

8.2. Вимоги щодо підготовки та уведення в дію

8.2.1. Для забезпечення можливості отримання інсталяційного пакету Криптопровайдера необхідно мати можливість підключення до мережі Інтернет через будь якого провайдера послуг. З електронної адреси ВЕБ-сторінки Виробника необхідно скопіювати інсталяційний пакет програмного забезпечення Криптопровайдера, а також комплект документації відповідно до пункту 3.6 цих ТУ.

8.2.2. Інсталяція програмного забезпечення Криптопровайдера здійснюється після перевірки його інсталяційного пакету антивірусним програмним забезпеченням. Інсталяція Криптопровайдера здійснюється відповідно до Інструкції з інсталяції та ініціалізації (31085786.1КЦ.019.І1.01.1) , що входить до комплекту поставки (п. 3.6 цих ТУ).

8.2.3. Після інсталяції обов’язково здійснюється перевірка цілісності програмного забезпечення відповідно до Інструкції із забезпечення безпеки експлуатації (31085786.1КЦ.019.І4.01.1), що входить до комплекту поставки (п. 3.6 цих ТУ). У разі негативних результатів перевірки на цілісність програмного забезпечення Криптопровайдера необхідно звернутися до чергового адміністратора за контактною інформацією, що вказана на ВЕБ-сторінці Виробника.

8.3. Особливості експлуатації Криптопровайдера

8.3.1. Для застосування Криптопровайдера необхідно мати відповідний досвід роботи та знання криптографічної архітектури Java JCA/JCE (Java™ Cryptography Architecture). Криптопровайдер не висуває специфічних вимог до режиму роботи обслуговуючого персоналу. Безпека при використанні досягається за умов дотримання Інструкції із забезпечення безпеки експлуатації (31085786.1КЦ.019.І4.01.1), що входить до комплекту поставки (п. 3.6 цих ТУ), а також інструкції щодо порядку генерації ключових даних і поводження (обліку, зберігання, знищення) з ключовими документами.

8.3.2. Робоче місце користувача повинно відповідати вимогам ДСанПіН 3.3.2 007.

8.3.3. Підставою для початку експлуатації Криптопровайдера в організації (у тому числі її філіях або регіональних представництвах), є відповідний наказ керівника цієї організації. Експлуатація повинна здійснюватися відповідно до вимог Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту конфіденційної інформації та відкритої інформації з використанням електронного цифрового підпису, затвердженим наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України № 141 від 20.07.2007, зареєстроване в Міністерстві юстиції України за № 862/14129 від 30.07.2007.

8.3.4. Криптопровайдер не відноситься до відновлювальних виробів, та не підлягає технічному обслуговуванню окремо від обчислювальної техніки, на якій його встановлено.

8.3.5. У випадку укладання з постачальником відповідної угоди, користувач може отримувати технічну підтримку постачальника щодо використання Криптопровайдера.

9. ГАРАНТІЇ ВИРОБНИКА (ПОСТАЧАЛЬНИКА)

9.1. Підприємство-виробник ТОВ «Базис» гарантує відповідність Криптопровайдера вимогам цих ТУ при дотриманні умов інсталяції, експлуатації, зберігання і транспортування.

9.2. Гарантійний термін експлуатації – необмежений, при необхідності користувач може знову отримати інсталяційний пакет та встановити його на обчислювальну техніку під управлінням операційної системи Windows, Unix/Linux, Mac OS X з віртуальною машиною JVM JRE/JDK 1.6.0_45 (Java™ Platform Standard Edition 6) і вище.

ДОДАТОК А

(рекомендований)

ПЕРЕЛІК ТЕХНІЧНИХ ЗАСОБІВ ІНСТРУМЕНТУ, ОСНАЩЕННЯ, НЕОБХІДНИХ ДЛЯ КОНТРОЛЮ І ВИПРОБУВАНЬ

Таблиця А.1 - Перелік засобів

Найменування	Границя допустимої основної похибки	Кількість
ПЕОМ з однією із операційних систем Windows XP/2003/2008/7/8, Unix/Linux, Mac OS X	-	1
Програмне забезпечення віртуальної машини Java 1.6.0_45 (Java ™ Platform Standard Edition 6) та вище	-	1
Утиліта ProvidersBrowser.class перевірки конфігурації та верифікації програмних компонентів (додатково)	-	1

ДОДАТОК Б

(довідковий)
БІБЛІОГРАФІЯ

1. Методика генерації та розподілу ключових даних «Цезаріс-RNG-JM», 31085786.1КЦ.019.М1.01.1;

2. Технічне завдання «Криптографічний сервіс-провайдер «Цезаріс-CSP-JM» (код - 31085786.1КЦ.019.ТЗ.01.1), погоджене Адміністрацією Держспецзв'язку України;

3. ДСТУ ISO/IEC 8824-1:2008 Інформаційні технології- Нотація абстрактного синтаксису (ASN.1)- Частина 1: Специфікація базової нотації

4. ДСТУ ISO/IEC 8825-1:2008 Інформаційні технології - ASN.1 правила кодування - Частина 1: Специфікація правил базового кодування (BER), правил канонічного кодування (CER) і правил витонченого кодування (DER).

5. ГОСТ Р 34.10-2001 - Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи (ГОСТ 34.310-2004);

6. ISO/IEC 10116 "Information technology - Security techniques - Modes of operation for an n-bit block cipher" (Інформаційні технології – Технології безпеки – Режими операцій для n-розрядного блочного шифрування);

7. ISO/IEC 18014 "Information technology - Security techniques - Time-stamping services" (Інформаційні технології – Технології безпеки – Сервіси позначок часу);

8. ISO/IEC 18031:2005 - Information technology -- Security techniques -- Random bit generation (Інформаційні технології – Методики з безпеки – Генерація випадкових бітів);

9. ISO/IEC 18033-3 "Information technology - Security techniques - Encryption algorithms – Part 3: Block ciphers" (Інформаційні технології – Технології безпеки – Алгоритми шифрування – Частина 3: Блочне шифрування);

10. ETSI TS 101 733 V1.7.4 (2008-07) - Technical Specification. Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES) (Технічна специфікація. Електронні підписи та інфраструктура (ESI); CMS розширені електронні підписи (CAdES));

11. ETSI TS 102 176-1 V2.0.0 (2007-11) – Technical Specification. Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms (Технічна специфікація. Електронні підписи та інфраструктури (ESI); Алгоритми та параметри для безпеки електронних підписів; Частина 1: Геш-функції та асиметричні алгоритми);

12. ETSI SR 002 176 V1.1.1 (2003-03) - Special Report - Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures (Спеціальний Доклад. Електронні підписи та інфраструктура (ESI); Алгоритми та параметри для безпеки електронних підписів).

13. ETSI TS 101 861 "Technical Specification - Time stamping profile" (Технічна специфікація – Профіль позначки часу);

14. ETSI TS 102 023 "Technical Specification - Policy requirements for time-stamping authorities" (Технічна специфікація – Вимоги політики керування позначками часу);

15. RFC 2104:1997 - HMAC: Keyed-Hashing for Message Authentication - February 1997 (HMAC: геш-кодування для автентифікації повідомлень – Лютий 1997);

16. RFC 2268:1998 "A Description of the RC2(r) Encryption Algorithm" (Опис алгоритму шифрування RC2(r));

17. RFC 2459:1999 - Internet X.509 Public Key Infrastructure Certificate, January 1999 (Sec.7.3.2 Diffie-Hellman Key Exchange Key) (Інфраструктура сертифікатів відкритих ключів Internet X.509, Обмін ключами згідно Diffie-Hellman);

18. RFC 2560 - Internet X.509 Public Key Infrastructure Online Certificate Status Protocol – OCSP (Інфраструктура публічних ключів. Протокол визначення статусу сертифікату в реальному часі);

19. RFC 2630:1999 - Cryptographic Message Syntax (Синтаксис криптографічних повідомлень);

20. RFC 2631:1999 - Diffie-Hellman Key Agreement Method (Метод узгодження ключів Diffie-Hellman);

21. RFC 2632:1999 - S/MIME Version 3 Certificate Handling (S/MIME версії 3 поводження з сертифікатами);

22. RFC 2633:1999 - S/MIME Version 3 Message Specification (S/MIME версії 3 специфікація повідомлень);

23. RFC 2634:1999 - Enhanced Security Services for S/MIME, June 1999 (Посилені послуги безпеки для S/MIME, Червень 1999);

24. RFC 2797:2000 - Certificate Management Messages over CMS (управління сертифікатами у повідомленнях для CMS);

25. RFC 2898:2000 - PKCS #5: Password-Based Cryptography Specification, Version 2.0 (PKCS #5: Специфікація криптографії, заснованої на паролі, Версія 2.0);

26. RFC 3161 - Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) (Інфраструктура публічних ключів. Протокол позначки часу);

27. RFC 3278:2002 - Use of Elliptic Curve Cryptography (ECC) Algorithms in Cryptographic Message Syntax (CMS), April 2002 (Застосування алгоритмів еліптичних криптографічних кривих (ECC) у криптографічному синтаксисі повідомлень (CMS), Квітень 2002);

28. RFC 3279 "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" (Алгоритми та ідентифікатори для Internet X.509 інфраструктури сертифікатів відкритих ключів та списку відкликаних сертифікатів);

29. RFC 3281 - An Internet Attribute Certificate Profile for Authorization (Інтернет атрибути профілю сертифікату для підтвердження/авторизації);

30. RFC 3369:2002 - Cryptographic Message Syntax (CMS) (синтаксит криптографічних повідомлень);

31. RFC 3370:2002 - Cryptographic Message Syntax (CMS) Algorithms (Алгоритми синтаксису криптографічних повідомлень (CMS));
32. RFC 3394:2002 - Advanced Encryption Standard (AES) Key Wrap Algorithm (Сучасний алгоритм шифрування (AES) алгоритм обміну ключами);
33. RFC 3447:2003 - Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography, Specifications Version 2.1 (Стандарт криптографії з відкритими ключами (PKCS) #1: RSA криптографія, Специфікації версії 2.1);
34. RFC 3628:2003 - Policy Requirements for Time-Stamping Authorities (TSAs) (Вимоги політики для управління позначками часу);
35. RFC 3851:2004 «Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1, Message Specification» (Розширення для безпечних/універсальних Інтернет повідомлень);
36. RFC 3852 - Cryptographic Message Syntax (CMS) (Криптографічний синтаксис повідомлень);
37. RFC 4357:2006 - Additional Cryptographic Algorithms for Use with GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms (Додаткові криптографічні алгоритми для використання з алгоритмами GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, та GOST R 34.11-94);
38. RFC 4490:2006 - Using the GOST 28147-89, GOST R 34.11-94, GOST R 34.10-94, and GOST R 34.10-2001 Algorithms with Cryptographic Message Syntax (CMS), May 2006 (Використання алгоритмів GOST 28147-89, GOST R 34.11-94, GOST R 34.10-94, та GOST R 34.10-2001 у синтаксисі криптографічних повідомлень (CMS), Травень 2006);
39. RFC 4491:2006 - Using the GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile (Використання алгоритмів GOST R 34.10-94, GOST R 34.10-2001, та GOST R 34.11-94 в інфраструктурі сертифікатів відкритих ключів Internet X.509 та профілі CRL);
40. RFC 5008:2007 - Suite B in Secure/Multipurpose Internet Mail Extensions (S/MIME)", September 2007 (Набір B у розширенні стандарту Інтернету для шифрованих/багатоцільових повідомлень електронної почти (S/MIME), Вересень 2007);
41. RFC 5019:2007 - The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments, September 2007 (Легкий Протокол визначення статусу сертифікату в реальному часі (OCSP) профілю для великомасштабних середовищ, вересень 2007 р.);
42. RFC 5035:2007 - Enhanced Security Services (ESS) Update: Adding CertI - Updates: RFC 2634, August 2007 (Оновлення щодо посилених послуг безпеки (ESS): доповнення CertI – Доповнення RFC 2634, Серпень 2007);
43. RFC 5126 "CMS Advanced Electronic Signatures" (CMS Розширені електронні підписи);
44. RFC 5280:2008 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (Інфраструктура Сертифікатів відкритих ключів Internet X.509 та профілі списку відкликаних сертифікатів (CRL));

45. RFC 5480:2009 - Elliptic Curve Cryptography Subject Public Key, March 2009 (Криптографія на еліптичних кривих для відкритих ключів, Березень 2009);

46. RFC 5639:2010 - Elliptic Curve Cryptography (ECC) Brainpool Standard (Стандарт Brainpool для криптографії на еліптичних кривих (ECC));

47. RFC 5652:2009 - Cryptographic Message Syntax (CMS), September 2009 (Синтаксис криптографічних повідомлень (CMS), Вересень 2009);

48. RFC 5758:2010 - Internet X.509 Public Key Infrastructure: Additional Algorithms and Identifiers for DSA and ECDSA, January 2010 (Інфраструктура відкритих ключів Internet X.509: додаткові алгоритми та ідентифікатори для DSA та ECDSA, Січень 2010);

49. RFC 5832:2010 - GOST R 34.10-2001: Digital Signature Algorithm (ГОСТ Р 34.10-2001. Алгоритм цифрового підпису);

50. PKCS #1 v2.1: RSA Cryptography Standard - RSA Laboratories, June 14, 2002;

51. PKCS #3: Diffie-Hellman Key-Agreement Standard - An RSA Laboratories Technical Note Version 1.4, Revised November 1, 1993 (Стандарт узгодження ключів Diffie-Hellman – Технічні вказівки Лабораторії RSA Версії 1.4, оновлено 1 Листопада 1993);

52. PKCS #5 v2.1: Password-Based Cryptography Standard - RSA Laboratories (Стандарт криптографії, заснованої на паролі, RSA Лабораторія);

53. PKCS #7 - The Public key cryptography standards - Part 7: Cryptographic message syntax standard, - version 1.6, 1997 (Криптографічні стандарти відкритих ключів – Частина 7: стандарт криптографічного синтаксису повідомлень – версія 1.6, 1997);

54. Extensions and Revisions to PKCS #7 - An RSA Laboratories Technical Note, May 13, 1997 (Розширення та зміни до PKCS #7 - Технічні нотатки Лабораторії RSA, Травень 13, 1997);

55. PKCS #9 v2.0: Selected Object Classes and Attribute Types - RSA Laboratories (Вибір об’єктних класів та атрибутів типів - Лабораторії RSA);

56. PKCS #11 - The Public key cryptography standards – Part 11: Cryptographic token interface standard", version 2.20, 2003 (Стандарт криптографії відкритих ключів. Частина 11: Стандарт інтерфейсу криптографічного токену);

57. PKCS #12 v1.0: Personal Information Exchange Syntax - RSA Laboratories (Синтаксис обміну персональною інформацією - RSA Лабораторія);

58. NIST SP 800-38B:2005 - Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, - MD 20899-8930, May 2005 (Рекомендації щодо роботи режимів блочного шифрування: режим CMAC для автентифікації, MD 20899-8930, Травень 2005);

59. NIST SP 800-56A:2007 - Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, - March, 2007 (Рекомендації для схем створення пари ключів з використанням дискретної логарифмічної криптографії, Березень, 2007);

60. NIST Special Publication 800-90:2007 - Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised) - March

2007 (Рекомендації для генерації випадкових чисел з використанням генератора детермінованих випадкових бітів (Виправлена) – Березень 2007);

61. FIPS 198-1:2008 - The Keyed-Hash Message Authentication Code (HMAC), July 2008 (Геш-кодування для коду автентифікації повідомлень (HMAC), Липень 2008);

62. FIPS PUB 186-3:2009 – FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION. Digital Signature Standard (DSS) (Публікації федерального стандарту з обробки інформації. Стандарт цифрового підпису (DSS));

63. ISO/IEC 8825-1:2002 - Information Technology -- ASN.1 Encoding Rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER), and Distinguished Encoding Rules (DER). 2002;

64. ANSI X9.62: The Elliptic Curve Digital Signature Algorithm (ECDSA) (Алгоритм цифрового підпису на еліптичних кривих);

65. «Про затвердження вимог до форматів, структури та протоколів, що реалізуються у надійних засобах електронного цифрового підпису», Наказ Мінюста та Держспецзв'язку № 1236/5/453 від 20.08.12 р.

АРКУШ РЕЄСТРАЦІЇ ЗМІН

№ зміни	Номери листів				Всього листів (сторінок)	№ докум.	Вхідний № супровідного документа і дата	Підпис	Дата
	Змінених	Замінених	Нових	Анульованих					