Примірник №2

ДКПП 72.20.21

УКНД 35.240.99

ЗАРЕЄСТРОВАНО

ПОГОДЖЕНО

Адміністрація Держспецзв'язку України

Перший заст. голов. Державної служби спец. зв'язку та захисту інформації України

_____ Фесоцю С.О.

«31» 08 2011 р.

ЗАТВЕРДЖУЮ

Директор ТОВ «Інтер-Метл»

_____ О.В. Тарадов

"19" 10 2011 р.

Виріб програмний

Криптографічний сервіс-провайдер "ЦЕЗАРІС-CSP"

ТЕХНІЧНІ УМОВИ

ТУ У 72.2-25279440-002:2011

Державний комітет України з питань технічного регулювання та споживчої політики
(Держспоживстандарт України)
Державне підприємство
Всеукраїнський державний науково-виробничий центр стандартизації, метрології, сертифікації та захисту прав споживачів
(Укрметртестстандарт)
Ідентифікаційний код 02568182
ЗАРЕЄСТРОВАНО "21" 12 2011 р.
В книзі обліку за № 02568782/037088 1

(Введено вперше)

Дата надання чинності

«21» 12 2012 р.

Без обмеження чинності

ПОГОДЖЕНО

Перший заступник головного державного санітарного лікаря України

Висновком № 05.03.02-07/97197
від «04» 10 2011 р.

РОЗРОБЛЕНО

Директор технічний
ТОВ «Інтер-Метл»

_____ С.В. Мартиненко

"7" 06 2011 р.

2011

Вх 8184

до Вх 2144

до Вх 2622-11 до 2449

ЗМІСТ

Стор.

1 СФЕРА ЗАСТОСУВАННЯ

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

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

Криптопровайдер "Цезаріс-CSP" призначений для використання у складі комплексів оброблення та передавання інформації з метою забезпечення функцій криптографічного захисту інформації. Криптопровайдер "Цезаріс-CSP" призначений для його використання у програмних додатках та сервісах операційних системах сімейства Windows виробництва компанії Microsoft® для забезпечення інтерфейсу взаємодії з носіями інформації, генерації випадкових послідовностей, обчислення асиметричної пари ключів, обчислення особистих та відкритих ключів, генерації таємних ключів, інтерфейсу взаємодії з носіями інформації, формування та перевіряння цифрового підпису, накладення та перевірки електронного цифрового підпису, узгодження ключів, управління сертифікатами ключів, зашифрування, розшифрування, обчислення геш-функції.

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, зареєстрованим в Міністерстві юстиції України від 30.07.2007 за № 862/14129 Криптопровайдер "Цезаріс-CSP" належить до програмних

засобів криптографічного захисту інформації (КЗІ) категорій "Ш", "К", "П", виду “Б” підвиду "Б2", класу "Б1".

Криптопровайдер “Цезаріс-CSP” належить до класу А1 засобів КЗІ у випадку застосування разом з надійними апаратними носіями ключової інформації, які мають позитивний експертний висновок або сертифікат відповідності за результатами державної експертизи в галузі КЗІ, а програмне забезпечення, під управлінням якого Криптопровайдер виконує свої функції, є невід'ємною частиною цих засобів (підтримуються та інтегровані з ним за сукупністю криптографічних перетворень).

Приклад познаки Криптопровайдера “Цезаріс-CSP” при його замовленні, ідентифікації та посиланнях в інших нормативних документах:

“Криптографічний сервіс-провайдер “Цезаріс-CSP” ТУ У 72.2-25279440-002:2011”.

У Криптопровайдері “Цезаріс-CSP” не використовуються винаходи та патенти.

Виробником криптопровайдеру “Цезаріс-CSP” є ТОВ «Інтер-Метл», м. Київ.

Ці ТУ є власністю ТОВ «Інтер-Метл», м. Київ і придатні для цілей сертифікації. Ці ТУ встановлюють вимоги до криптопровайдера “Цезаріс-CSP”, 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 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 4145-2002 – Інформаційна технологія. Криптографічний захист інформації. Електронний цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння;

ДСТУ ISO/IEC 9797-1:2009 – Інформаційні технології. Методи захисту. Коди автентифікації повідомлень (MACs). Частина 1. Механізми, що використовують блокові шифри (ISO/IEC 9797-1:1999, IDT);

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 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 11770-3:2002 "Інформаційні технології. Методи захисту. Управління ключовими даними. Частина 3. Протоколи, що ґрунтуються на асиметричних криптографічних перетвореннях";

ДСТУ ISO/IEC 14888-3:2002 – Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 3. Механізми на основі сертифікатів (ISO/IEC 14888-3:1998, IDT);

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);

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 CWA 14167-3:2008 – Криптографічний модуль для послуг генерування ключів провайдером послуг сертифікації. Профіль захисту CMCKG-PP (CWA 14167-3:2004, IDT);

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

ГОСТ 12.1.003-83 ССБТ. Шум. Общие требования безопасности;

---

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

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 19.202-78 Единая система программной документации. Спецификация. Требования к содержанию и оформлению;

ГОСТ 19.505-79 Единая система программной документации. Руководство оператора. Требования к содержанию и оформлению;

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.

3 ТЕХНІЧНІ ВИМОГИ

3.1 Загальні вимоги

Криптопровайдер "Цезаріс-CSP" повинен відповідати вимогам цих ТУ і комплекту експлуатаційної та програмної документації на програмний виріб відповідно до специфікації «Криптографічний сервіс-провайдер «Цезаріс-CSP». Специфікація», код - 32206929.1КЦ.003.В1.00.1.

3.2 Вимоги призначення

3.2.1 Криптопровайдер "Цезаріс-CSP" (далі – Криптопровайдер) повинен виготовлятися та постачатися у вигляді інсталяційного пакету CesarisCryptoPack.exe через мережу Інтернет з адреси: www.itsway.kiev.ua.

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

3.2.3 Криптопровайдер повинен забезпечувати виконання таких функцій:

- генерацію випадкових послідовностей, таємних та тимчасових (сеансових) ключів, обчислення асиметричної пари ключів, узгодження ключів, обчислення та перевіряння підпису, асиметричне зашифрування та розшифрування, взаємодію із носіями інформації, 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 від 09.11.2007 [1], у тому числі ДСТУ ISO/IEC 11770-3, ДСТУ ISO/IEC 14888-3, ДСТУ CWA 14167-3 та ISO/IEC 18031 [6], NIST SP 800-56A [50], NIST Special Publication 800-90 [51];

- формування та обробку об'єктів відповідно до вимог «Технічні специфікації форматів представлення базових об'єктів національної системи

електронного цифрового підпису» [2] і ISO/IEC 8825 [8] і PKCS #10 [44], FIPS PUB 186-3 [47];

- формування та обробку об'єктів відповідно до вимог «Технічні специфікації форматів криптографічних повідомлень. Захищені дані» [3];

- формування та обробку об'єктів національної системи електронного цифрового підпису для форматів підписаних даних відповідно до вимог міжнародних стандартів RFC 3851 [23], RFC 3852 [24], RFC 4357 [25], RFC 5008 [28], RFC 5126 [30], ETSI SR 002 176 [35], ETSI TS 101 733 [36], PKCS #7 [42];

- формування та обробку об'єктів національної системи електронного цифрового підпису для Протоколу фіксування часу відповідно до вимог міжнародних стандартів RFC 3161 [16], RFC 3628 [22], ISO/IEC 18014 [5], ETSI TS 101 861 [37], ETSI TS 102 023 [38];

- формування та обробку об'єктів національної системи електронного цифрового підпису для Протоколу визначення статусу сертифіката відповідно до вимог міжнародних документів [11];

- криптографічних алгоритмів, визначених стандартами ДСТУ 4145, ДСТУ ГОСТ 28147, ГОСТ 34.311, ГОСТ 34.310 (опціонально);

- криптографічних алгоритмів геш-функцій SHA-1, SHA-256, SHA-384, SHA-512, MD-5 відповідно до ДСТУ ISO 10118-1, ДСТУ ISO 10118-2, ДСТУ ISO/IEC 10118-3, ДСТУ ETSI TS 102 176-1, RFC 2104 [9];

- обчислення та перевірка RSA підпису відповідно до стандартів ДСТУ ETSI TS 102 176-1, ДСТУ ETSI TS 102 176-2 та PKCS #1 v2.1 (RFC 3447)[21];

- обчислення імітовставки відповідно до ДСТУ ГОСТ 28147 та MAC відповідно до ДСТУ ISO/IEC 9797-1 і FIPS 198-1 [48] NIST SP 800-38B [49];

- криптографічних алгоритмів симетричного шифрування: DES, TDEA/3DES [4] та AES [20] відповідно до ДСТУ ISO/IEC 18033-1, ISO/IEC

18033-3 [7] у режимі ECB, що визначені ISO/IEC 10116 [4];

- криптографічних алгоритмів асиметричного шифрування: RSAEncryption відповідно до схеми RSAES-PKCS1-v1_5 та схеми RSAES-OAEP згідно з стандартом ДСТУ ETSI TS 102 176-1 та RFC 3447 [21];

- криптографічних протоколів узгодження ключів (Діффі-Геллмана) відповідно до ДСТУ ISO/IEC 15946-3, RFC 2459 [10], RFC 2631 [13], PKCS #3 [39];

- підтримка формування та обробки форматів сертифікатів та списків відкликання з розширеннями відповідно до стандартів RFC 5280 [31], RFC 5480 [32], RFC 5758 [34] та PKCS #9 [41];

- збереження та використання сертифікатів відкритих ключів, формати яких відповідають вимогам технічних специфікацій форматів представлення базових об'єктів національної системи електронного цифрового підпису, затверджених спільним наказом ДСТСЗІ СБ України та Державного департаменту з питань зв'язку та інформатизації Міністерства транспорту та зв'язку України від 11.09.2006 № 99/166 [2] а також RFC 3281 [18], RFC 4491 [27], RFC 5035 [29];

- підтримка алгоритмів синтаксису криптографічних повідомлень RFC 2630[12], RFC 2634 [14], RFC 3278 [17], RFC 3370 [19], RFC 3851 [23], RFC 3852 [24], RFC 4490 [26], RFC 5008 [28], RFC 5652 [33], з розширеннями відповідно до PKCS #7 [42] та доповнення до PKCS #7 [43];

- взаємодія з носіями інформації відповідно до PKCS #11 [45], PKCS #12 [46] та згідно з RFC 2898 [15], PKCS #5 [40], формування та обробку об'єктів криптографічних сховищ ключів:

  - PCSC сховище на смарт-картках та апаратних модулях безпеки (HSM) відповідно до стандарту PKCS #11[45];
  - Файловий токен - сховище на будь-яких носіях типу диск, дискета, флеш-пам'ять тощо, у форматі об'єктів стандарту PKCS

#11 під управлінням операційної системи Windows;

- Реалізацію генераторів псевдо-випадкових чисел:
  - DSTURandom відповідно до ДСТУ 4145.

3.3 Вимоги до сумісності та працездатності

Криптопровайдер повинен бути сумісним з операційними системами Windows 2000 SP1, Windows 2003, Windows 2008, Windows XP, Windows 7 виробництва компанії Microsoft® (США).

Технічні вимоги до обчислювальної техніки, на яких має працювати криптопровайдер "Цезаріс-CSP" повинні відповідати вимогам, які висуваються до такої техніки операційними системами Windows 2000 SP1, Windows 2003, Windows 2008, Windows XP, Windows 7 виробництва компанії Microsoft® (США).

3.4 Вимоги до реалізації та складу

Криптопровайдер "Цезаріс-CSP" повинен бути скомпільований у стандартизованому двійковому форматі, який представлено у вигляді інсталяційного пакету CesarisCryptoPack.exe, що містить програмні компоненти, які забезпечують функціональність відповідно до вимог 3.2.3 та сумісності відповідно до 3.3, та інші компоненти, призначені для забезпечення функціонування зазначених базових компонентів.

До складу програмного забезпечення Криптопровайдеру "Цезаріс-CSP" повинні входити такі компоненти, що наведені у таблиці 1.

Таблиця 1 – Компоненти Криптопровайдера

№	Найменування	Коротка характеристика
1	2	3
Незмінні (базові) компоненти		
1	csrs001csp.dll	Динамічна бібліотека управління викликами для RSA
2	csrs805csp.dll	Динамічна бібліотека управління викликами для ДСТУ 4145 ПБ з RSA

Продовження Таблиці 1

1	2	3
3	csrs806csp.dll	Динамічна бібліотека управління викликами для ДСТУ 4145 ОНБ з RSA
4	csrs807csp.dll	Динамічна бібліотека управління викликами для ДСТУ 4145 ПБ з ECDH
5	csrs808csp.dll	Динамічна бібліотека управління викликами для ДСТУ 4145 ОНБ з ECDH
7	CesarisCrypto.dll	Бібліотека криптографічних процедур низького рівня для ГОСТ 34.311, ДСТУ ГОСТ 28147, ДСТУ 4145, RSA та ECDH
Змінні (додаткові) компоненти		
8	csrs001ex.dll	Динамічна бібліотека виклику функцій Криптопровайдера для RSA
9	csrs805ex.dll	Динамічна бібліотека виклику функцій Криптопровайдера для ДСТУ 4145 ПБ з RSA
10	csrs806ex.dll	Динамічна бібліотека виклику функцій Криптопровайдера для ДСТУ 4145 ОНБ з RSA
11	csrs807ex.dll	Динамічна бібліотека виклику функцій Криптопровайдера для ДСТУ 4145 ПБ з ECDH
12	csrs808ex.dll	Динамічна бібліотека виклику функцій Криптопровайдера для ДСТУ 4145 ОНБ з ECDH
13	cesarisstore.dll	Драйвер управління взаємодії Криптопровайдера зі сховищами ключової інформації
14	csrs_bcrypt.dll	Бібліотека інтеграції з провайдером Microsoft CNG для Windows Vista/ Windows 7
15	capicom.dll	Бібліотека Microsoft Windows для роботи з Crypto API
16	xenroll.dll	Бібліотека Microsoft Windows для роботи з запитами на сертифікат за PKCS#10 [44] та відповідями (Certificate Enrollment API)
Опціональні компоненти		
17	csrs804csp.dll	Динамічна бібліотека управління викликами для ГОСТ 34.310 з RSA та ГОСТ 34.311
18	csrs804ex.dll	Динамічна бібліотека виклику функцій Криптопровайдера для ГОСТ 34.310 з RSA та ГОСТ 34.311

Кінець Таблиці 1

1	2	3
Змінні компоненти - драйвери роботи з носіями		
19	cesaris_dispatch.dll	Диспетчер драйверів носіїв за стандартом PKCS#11 [45]
20	cesaris_virtual.dll	Драйвер реалізації стандарта PKCS#11 [45] віртуального носія
21	cesaris_file.dll	Драйвер реалізації стандарта PKCS#11 [45] файлового носія
22	cesaris_aladdin.dll	Драйвер реалізації стандарта PKCS#11 [45] носіїв фірми Aladdin
23	cesaris_ikey.dll	Драйвер реалізації стандарта PKCS#11 [45] носіїв фірми SafeNet (iKey)
24	cesaris_oberthur.dll	Драйвер реалізації стандарта PKCS#11 [45] носіїв фірми Oberthur

Компоненти з номерами 1-6 є незмінними (базовими) складовими Криптопровайдера і виконують функції реалізації всіх криптографічних алгоритмів та їх викликів у Криптопровайдері.

Інші компоненти Криптопровайдера є додатковими і можуть змінюватись. Ці компоненти призначені для наступних цілей:

Компонента 7 призначена для управління роботою Криптопровайдера зі сховищами ключової інформації і може змінюватись в залежності від необхідності підтримки різних носіїв ключової інформації.

Компоненти 8-12 (csrsXXXex.dll) призначені для управління викликами у Криптопровайдері різних гілок криптографічних функцій. Ці компоненти можуть змінюватись у випадку зміни виробником ОС Windows (фірми Microsoft) сертифікатів, призначених для перевірки підпису коду та реєстрації програмних компонент в цих ОС.

Компонента 14 призначена для сумісності з ОС Windows 7 (Windows Vista) і є необхідною для Microsoft криптопровайдерів відповідно до архітектури MSDN та CNG-технологій;

Компоненти 15 та 16 є системним програмним забезпеченням фірми Microsoft для Windows XP і включені до складу Криптопровайдера для

полегшення роботи користувача Криптопровайдера (можуть бути отримані з сайту технічної підтримки ОС Windows XP за адресами: http://www.microsoft.com/downloads/ru-ru/details.aspx?FamilyID=860ee43a-a843-462f-abb5-ff88ea5896f6 та http://www.microsoft.com/downloads/en/details.aspx?familyid=ca930018-4a66-4da6-a6c5-206df13af316&displaylang=en);

Компоненти 17 та 18 є опціональними і виконують функції реалізації криптографічних алгоритмів ГОСТ 34.310 з RSA та ГОСТ 34.311 та їх викликів у Криптопровайдері;

Компоненти 13,19-24 є драйверами роботи з файловим та віртуальним носіями, а також зі СМАРТ-картами та криптотокенами різних виробників і їх список може поповнюватись в залежності від необхідності підтримки носіїв ключової інформації різних виробників такого обладнання.

Додаткові компоненти Криптопровайдера можуть змінюватись в залежності від змін (оновлень) програмного забезпечення Microsoft для ОС Windows (3.2) та переліку носіїв ключової інформації, які підтримуються Криптопровайдером. Відповідно, змінюється номер версії Криптопровайдера, який складається з 3-х цифр, розділених точками, а версія Криптопровайдера фіксується у інсталяційному пакеті CesarisCryptoPack.exe.

Крім Криптопровайдера користувачу можуть поставлятись додаткові програмні засоби (утиліти, програмні бібліотеки тощо) для використання Криптопровайдера в інформаційно-телекомунікаційних системах різного призначення, постачання яких відбувається відповідно до умов 8.3.5.

3.5 Вимоги надійності та безпеки використання

Робота Криптопровайдера "Цезаріс-CSP" не повинна викликати спотворення інформації, збоїв та блокування роботи операційної системи Windows (3.2).

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.

Процедури Криптопровайдера "Цезаріс-CSP", які використовують ключові дані, повинні здійснювати знищення ключових даних в оперативному запам'ятовуючому пристрої комп'ютера відразу після їхнього використання.

Контроль цілісності Криптопровайдеру "Цезаріс-CSP" забезпечується перевіркою цифрового підпису Криптопровайдера "Цезаріс-CSP", що накладений компанією Microsoft® (США), автоматично бібліотекою advapi32.dll, яка входить до складу операційних систем Windows 2000 SP1, Windows 2003, Windows XP, а також вбудованою функцією, яка перевіряє цілісність модулів при будь-якому виклику зовнішнім програмним застосуванням.

Контроль цілісності Криптопровайдера та забезпечення безпеки експлуатації повинні відповідати документу «Криптографічний сервіс-провайдер «Цезаріс-CSP». Інструкція із забезпечення безпеки експлуатації», код 32206929.1КЦ.003.І4.01.1.

3.6 Комплектність

До комплекту постачання повинно входити:

- інсталяційний пакет CesarisCryptopack.exe, який містить програмні компоненти відповідно до 3.2 та 3.3 та інформацію про зміст версії Криптопровайдера (3.4);

- Інструкція з інсталяції та ініціалізації «Криптопровайдер «Цезаріс-CSP». Інструкція з експлуатації», 32206929.1КЦ.003.І3.01.1, відповідно до ГОСТ 19.505 у вигляді у вигляді PDF файлу ManualCesaris.pdf;

- Специфікація «Криптографічний сервіс-провайдер «Цезаріс-CSP». Специфікація», 32206929.1КЦ.003.В1.00.1, відповідно до ГОСТ 19.202, у вигляді PDF файлу (register.pdf);

- Інструкція із забезпечення безпеки експлуатації «Криптографічний сервіс-провайдер «Цезаріс-CSP». Інструкція із забезпечення безпеки експлуатації. 32206929.1КЦ.003.І4.01.1»;

- Керівництво програміста «Криптографічний сервіс-провайдер «Цезаріс-CSP». Керівництво програміста. 32206929.1КЦ.003.І2.01.1», відповідно до ГОСТ 19.505, у вигляді PDF файлу ProgrCesaris.pdf.

Інструкція з інсталяції та ініціалізації, специфікація, керівництво програміста, інструкція із забезпечення безпеки експлуатації Криптопровайдера, можуть бути доступні для перегляду на інтернет-сторінці www.itsway.kiev.ua.

Для програмних засобів та комплексів, де застосовується Криптопровайдер, додатково 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.

Перелік незмінних та змінних компонент Криптопровайдера "Цезаріс-CSP" вказаний у 3.4. Змінні програмні компоненти можуть змінюватися без впливу на криптографічні та спеціальні якості Криптопровайдера.

3.7 Маркування

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

- повна назва Криптопровайдера українською мовою та позначення цих ТУ: «Виріб програмний. Криптографічний сервіс-провайдер "Цезаріс-CSP", ТУ У 72.2-25279440-002:2011»;

- назва Криптопровайдера англійською мовою: "CESARIS - CSP";

- назва країни та підприємства виробника, його знак для товарів та послуг (при наявності);

- версія Криптопровайдера;

- 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 щодо постачання Криптопровайдера через мережу Інтернет.

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 ДСанПіН 3.3.2.007, ДСН 3.3.6.096, ДСН 3.3.6.037, ГОСТ 12.2.032.

5 ПРАВИЛА ПРИЙМАННЯ

5.1Загільні положення

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

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

5.1.3 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.

5.2 Приймально-здавальні випробування

5.2.1 Склад і послідовність приймально-здавальних випробувань повинні відповідати наведеним в таблиці 2.

5.2.2 Приймально-здавальним випробуванням підлягає кожний зразок Криптопровайдера.

5.2.3 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.

Таблиця 2 - Склад і послідовність приймально-здавальних випробувань

Найменування випробувань (перевірок)	Номери пунктів		Категорія випробувань	
	Техніч-них вимог	методів випробу-вань	Приймаль но-здавальні	Пе-ріодичні
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 та працездатності	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 використання	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 навколишнього середовища *	4.1	6.2.5	–	–
10. Вимоги до безпеки процесу виробництва *	4.2	6.2.5, 6.2.6	–	–

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

5.3 Кваліфікаційні випробування

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

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

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

5.3.4 Послідовність і обсяг кваліфікаційних випробувань повинні відповідати 6.2 цих ТУ.

5.4 Періодичні випробування

5.4.1 Періодичні випробування проводить підприємство-постачальник.

5.4.2 Періодичні випробування проводять не рідше одного разу на 2 роки, у час, затверджений керівником підприємства-постачальника, у обсязі та у послідовності, що наведена у таблиці 2 цих ТУ. Під час проведення періодичних випробувань, постачання Криптопровайдеру "Цезаріс-CSP" не припиняється.

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

5.4.4 Після аналізу та усунення виявлених дефектів необхідно провести повторні випробування в обсязі періодичних випробувань на подвійній

кількості Криптопровайдера. Результати повторних випробувань вважають остаточними.

5.4.5 Результати періодичних випробувань оформляються актом.

5.4.6 Зразки Криптопровайдера "Цезаріс-CSP", які витримали періодичні випробування, постачанню споживачу не підлягають.

5.5 Типові випробування

5.5.1 Типові випробування проводять за програмою типових випробувань при внесені змін в програмне забезпечення Криптопровайдера "Цезаріс-CSP", застосуванні нових технічних засобів постачання або зміни умов постачання. Типові випробування не проводяться при зміні програмних компонентів, які є змінною частиною програмного забезпечення Криптопровайдера відповідно до таблиці 1 цих ТУ.

5.5.2 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 6.2.4. В разі необхідності програма проведення типових випробувань може бути розширена, у такому випадку виробник (постачальник) розробляє та затверджує окрему програму та методики типових випробувань.

5.5.3 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.

5.6 Експертні дослідження в рамках державної експертизи в сфері криптографічного захисту інформації

Експертні дослідження в рамках державної експертизи в сфері криптографічного захисту інформації проводяться відповідно до вимог

чинних нормативно-правових актів з питань криптографічного захисту інформації.

5.7 Сертифікаційні випробування

Сертифікаційні випробування 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 наведено у 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, перевищуючих задані, порушенням вимог, указаних 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 Криптопровайдера "Цезаріс-CSP" вимогам документації (3.1) проводиться зовнішнім оглядом, аналізом експлуатаційної та програмної документації та програмного забезпечення комплексу.

6.2.2 Відповідність Криптопровайдера умовам постачання (3.2.1, 3.2.2), комплектності (3.6) та маркування (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 www.itsway.kiev.ua, та перевіряння отриманого виробу на відповідність вимогам пункту 3.4 та 3.6 та цих ТУ.

У разі якщо:

- інсталяційний пакет CesarisCryptopack.exe програмного забезпечення Криптопровайдера "Цезаріс-CSP", експлуатаційну та програмну документацію на Криптопровайдер "Цезаріс-CSP", в будь який час доби можна скопіювати з адреси: www.itsway.kiev.ua;

- за адресою www.itsway.kiev.ua можна отримати відомості, що зазначені у 3.7;

- після проведення інсталяції програмного забезпечення Криптопровайдера його незмінна частина містить компоненти відповідно до таблиці 2 у 3.4;

зробити висновок, що зразок програмного забезпечення Криптопровайдера "Цезаріс-CSP" відповідає вимогам постачання, комплектності та маркування, визначених в цих ТУ. В противному випадку зробити висновок, що зразок комплексу не відповідає цим вимогам.

6.2.3 Відповідність Криптопровайдера його функціональної призначеності здійснюється шляхом:

- здійснення перевірки відповідності Криптопровайдеру "Цезаріс-CSP" вимогам щодо його комплектності;

- перевірки відповідності програмних компонентів Криптопровайдера "Цезаріс-CSP" таблиці 2 цих ТУ за допомогою його вбудованої компоненти, що поставляється разом з інсталяційним пакетом CesarisCryptoPack.exe.

У разі, якщо комплектність Криптопровайдера "Цезаріс-CSP" відповідає вимогам 3.6 цих ТУ, а результати перевірки програмних компонентів Криптопровайдера відповідають переліку функцій, визначених у 3.2.3, зробити висновок, що зразок Криптопровайдера відповідає вимогам 3.4 цих ТУ.

6.2.4 Перевірку Криптопровайдера "Цезаріс-CSP" з метою визначення відповідності вимогам до сумісності (3.3) та працездатності проводити шляхом запуску на виконання програмного забезпечення Криптопровайдеру

"Цезаріс-CSP" на ПЕОМ під Windows 7, Windows Vista , Windows XP SP2, Windows 2003, Windows 2000 SP1, виробництва компанії Microsoft® (США) та перевірки виконання функцій, що зазначені у 3.3 цих ТУ.

У разі, якщо виконання функцій не викликає повідомлення про помилку, зробити висновок, що програмне забезпечення Криптопровайдеру "Цезаріс-CSP" сумісне з операційними системами Windows 2000 SP1, Windows 2003, Windows XP, Windows Vista, Windows 7.

6.2.5 Контроль вимог безпеки (4.1, 4.2) щодо виробничого процесу при постачанні Криптопровайдера "Цезаріс-CSP" 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 (4.2.1) при постановці на виробництво та під час виготовлення Криптопровайдера "Цезаріс-CSP" 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 (3.5) здійснюється відповідно документу «Криптографічний сервіс-провайдер «Цезаріс-CSP». Інструкція із забезпечення безпеки експлуатації. 32206929.1КЦ.003.І4.01.1».

7 ТРАНСПОРТУВАННЯ І ЗБЕРІГАННЯ

7.1 Криптопровайдер постачається споживачу через мережу Інтернет з електронної адреси www.itsway.kiev.ua у вигляді інсталяційного пакету CesarisCryptopack.exe.

7.2 Для контролю цілісності програмного забезпечення Криптопровайдера використовуються засоби, визначені в розділі 2 (Контроль цілісності) Інструкції із забезпечення безпеки експлуатації (32206929.1КЦ.003.І4.01.1), що входить до комплекту поставки (3.6).

7.3 Програмне забезпечення Криптопровайдеру "Цезаріс-CSP" після його копіювання у вигляді інсталяційного пакету CesarisCryptopack.exe з адреси: www.itsway.kiev.ua, перевірки антивірусним програмним забезпеченням (антивірусне програмне забезпечення обирається споживачем окремо самостійно), встановлюється на обчислювальну техніку під управління однієї з наступних операційних систем: Windows 2000 SP1, Windows 2003, Windows XP, Windows Vista, Windows 7. Інстальовані програмні компоненти Криптопровайдеру "Цезаріс-CSP" перевіряються на цілісність, як визначено у розділі 2 (Контроль цілісності) Інструкції із забезпечення безпеки експлуатації (32206929.1КЦ.003.І4.01.1) , що входить до комплекту поставки (3.6).

7.4 Криптопровайдер "Цезаріс-CSP" зберігається разом з обчислювальною технікою, на яку його було встановлено або у вигляді інсталяційного пакету CesarisCryptopack.exe на носії інформації.

8 ВКАЗІВКИ ЩОДО ЕКСПЛУАТАЦІЇ (ЗАСТОСУВАННЯ)

8.1 Вимоги до апаратного та програмного забезпечення

Вимоги до апаратного та програмного забезпечення для встановлення та експлуатації Криптопровайдеру "Цезаріс-CSP".

8.1.1 Криптопровайдер "Цезаріс-CSP" призначений для його встановлення та експлуатації під керуванням однієї з операційних систем Windows 2000 SP1, Windows 2003, Windows XP, Windows Vista, Windows 7.

8.1.2 Конфігурація апаратного забезпечення повинна відповідати вимогам, що висуваються операційною системою за 8.1.1.

8.2 Вимоги щодо підготовки та уведення в дію

Для забезпечення можливості отримання інсталяційного пакету Криптопровайдеру "Цезаріс-CSP" необхідно мати можливість підключення до мережі Інтернет через будь якого провайдера послуг.

З електронної адреси www.itsway.kiev.ua необхідно скопіювати інсталяційний пакет програмного забезпечення Криптопровайдера "Цезаріс-CSP" CesarisCryptopack.exe, а також комплект документації відповідно до пункту 3.6 цих ТУ.

8.2.1 Інсталяція програмного забезпечення Криптопровайдера здійснюється після перевірки його інсталяційного пакету антивірусним програмним забезпеченням. Інсталяція Криптопровайдера здійснюється відповідно до Інструкції з інсталяції та ініціалізації (32206929.1КЦ.003.І1.01.1), що входить до комплекту поставки (3.6).

8.2.2 Після інсталяції обов'язково здійснюється перевірка цілісності програмного забезпечення відповідно до Інструкції із забезпечення безпеки експлуатації (32206929.1КЦ.003.І4.01.1), що входить до комплекту поставки (3.6). У разі негативних результатів перевірки на цілісність програмного забезпечення Криптопровайдера необхідно звернутися до чергового

адміністратора за контактною інформацією, що вказана на сайті www.itsway.kiev.ua.

8.3 Особливості експлуатації Криптопровайдера

8.3.1 Для застосування Криптопровайдера "Цезаріс-CSP" необхідний досвід роботи та знання інтерфейсів користувача в операційних системах Windows. Криптопровайдер не висуває специфічних вимог до режиму роботи обслуговуючого персоналу. Безпека при використанні Криптопровайдеру "Цезаріс-CSP" досягається за умов дотримання Інструкції із забезпечення безпеки експлуатації (32206929.1КЦ.003.І4.01.1), що входить до комплекту поставки (3.6), а також інструкції щодо порядку генерації ключових даних і поводження (обліку, зберігання, знищення) з ключовими документами.

8.3.2 Робоче місце користувача Криптопровайдера має відповідати вимогам ДСанПіН 3.3.2.007.

8.3.3 Підставою для початку експлуатації Криптопровайдеру "Цезаріс-CSP" в організації (у тому числі її філіях або регіональних представництвах), є відповідний наказ керівника цієї організації. Експлуатація Криптопровайдеру 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 від 30.07.2007 за № 862/14129.

8.3.4 Криптопровайдер "Цезаріс-CSP" не відноситься до відновлювальних виробів та не підлягає технічному обслуговуванню окремо від обчислювальної техніки, в яку його встановлено.

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

9 ГАРАНТІЇ ВИРОБНИКА (ПОСТАЧАЛЬНИКА)

9.1 Підприємство-виробник ТОВ «Інтер-Метл» гарантує відповідність Криптопровайдера "Цезаріс-CSP" 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 Криптопровайдера та встановити його на обчислювальній системі.

9.3 Гарантія виробника не поширюється на події, пов'язані із модифікаціями (оновленнями) операційної системи у ході експлуатації Криптопровайдера. Підтримка, пов'язана з оновленнями операційної системи, забезпечується виробником відповідно до 8.3.5.

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 2000 SP1, Windows 2003, Windows XP, Windows Vista, Windows 7	-	1
Програмне забезпечення Криптопровайдера “Цезаріс-CSP” у вигляді інсталяційного пакету CesarisCryptopack.exe	-	1

ДОДАТОК Б

(довідковий)

БІБЛІОГРАФІЯ

1. Методика генерування ключів та розподілення ключових даних «Цезаріс-М», 32206929.1КЦ.017.М1.01.1, погоджена з адміністрацією Держспецзв'язку 9.11.2007 року ;

2. Технічні специфікації форматів представлення базових об'єктів національної системи електронного цифрового підпису, - затверджені наказом 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 р.;

3. Технічні специфікації форматів криптографічних повідомлень. Захищені дані, - Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України №112 від 14.05.2010 р.;

4. 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);

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

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

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

8. 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)" (Інформаційні технології – Правила кодування ASN.1 – Частина1: Специфікації базових правил кодування (BER), правила канонічного кодування (CER) та розпізнавального кодування (DER));

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

10. 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);

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

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

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

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

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

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

17. 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);

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

19. RFC 3370:2002 - Cryptographic Message Syntax (CMS) Algorithms (Алгоритми синтаксису криптографічних повідомлень (CMS));

20. RFC 3394:2002 - Advanced Encryption Standard (AES) Key Wrap Algorithm (Сучасний алгоритм шифрування (AES) алгоритм обміну ключами);

21. 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);

22. RFC 3628:2003 - Policy Requirements for Time-Stamping Authorities (TSAs) (Вимоги політики для управління позначками часу);

23. RFC 3851:2004 «Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1, Message Specification» (Розширення для безпечних/універсальних Інтернет повідомлень);

24. RFC 3852 - Cryptographic Message Syntax (CMS) (Криптографічний синтаксис повідомлень);

25. 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);

26. 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);

27. 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);

28. 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);

29. 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);

30. RFC 5126 "CMS Advanced Electronic Signatures" (CMS Розширені електронні підписи);

31. 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));

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

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

34. 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);

35. 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).

36. 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));

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

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

39. 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);

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

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

42. 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);

43. 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);

44. PKCS #10, "The Public key cryptography standards – Part 10: Cryptographic request syntax standard", version 1.7, 2000;

45. 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);

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

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

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

49. 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);

50. 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);

51. 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);

АРКУШ РЕЄСТРАЦІЇ ЗМІН									
Зм.	Номери листів (сторінок)				Всього листів (сторінок)	N докум.	Вхідний N супровідного документа і дата	Підпис	Дата
	Змінених	Замінених	Нових	анульованих					