НАЦІОНАЛЬНИЙ СТАНДАРТ УКРАЇНИ

НАСТАНОВА З ВИКОРИСТАННЯ ЕЛЕКТРОННИХ ПІДПИСІВ

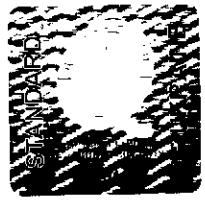
Частина 1. Юридичні та технічні аспекти

(CWA 14365-1:2004, IDT)

ДСТУ CWA 14365-1:2008

БЗ № 1– 2009/11

Видання офіційне



Київ
ДЕРЖСПОЖИВСТАНДАРТ УКРАЇНИ
2009

ПЕРЕДМОВА

1 РОЗРОБЛЕНО: Технічний комітет зі стандартизації «Інформаційні технології» (ТК 20) та Інститут кібернетики ім. В.Глушкова НАН України

ПЕРЕКЛАД І НАУКОВО-ТЕХНІЧНЕ РЕДАГУВАННЯ: **А. Гречко,** канд. фіз.-мат. наук; **О. Перевозчикова,** чл.-кор. НАНУ, д-р фіз.-мат. наук (науковий керівник)

2 НАДАНО ЧИННОСТІ: наказ Держспоживстандарту України від 22 грудня 2008 р. № 488 з 2009–04–01

3 Національний стандарт відповідає CWA 14365-1:2004 Guide on the Use of Electronic Signatures — Part 1: Legal and Technical Aspects (Настанова з використання електронних підписів. Частина 1. Юридичні та технічні аспекти)

Ступінь відповідності — ідентичний (IDT)

Переклад з англійської (en)

4 УВЕДЕНО ВПЕРШЕ

ЗМІСТ

С.

Національний вступ IV

Передмова до CWA 14365-1:2004 IV

1 Сфера застосування 1

2 Посилання 2

2.1 Нормативні посилання 2

2.2 Довідкові посилання 2

3 Терміни та визначення понять та абревіатури 3

3.1 Терміни та визначення понять 3

3.2 Абревіатури 3

4 Електронний підпис з технічної та юридичної точок зору 5

4.1 Технічне визначення послуг захисту 5

4.2 Підписи з юридичної точки зору 6

4.2.1 Технічні та юридичні аспекти 6

4.2.2 Підписи з функціональної точки зору 6

4.2.3 Потреба нетехнічного доказу 7

4.2.4 Особливості функціональних підписів 8

5 Порівняння визначень підписів 9

5.1 Термін та визначення поняття цифровий підпис 9

5.2 Термін та визначення поняття електронний підпис 10

5.3 Термін та визначення поняття розширений електронний підпис 11

5.4 Термін та визначення поняття кваліфікований електронний підпис 12

5.5 Юридична значимість різних видів електронного підпису 13

6 Випадки використання некваліфікованого електронного підпису 13

6.1 Компоненти кваліфікованих електронних підписів 14

6.2 Розширений електронний підпис без SSCD 15

6.3 Розширений електронний підпис без посиленого сертифіката 17

6.4 Цифровий підпис без подання даних 18

7 Доказ для електронних підписів 20

7.1 Докази, наявні у підписаних даних 20

7.2 Наявні у сертифікаті докази 20

7.3 Докази, наявні у політиці сертифікації та/або CPS 21

7.4 Доказ щодо статусу сертифіката 21

7.5 Докази, наявні у політиці підписання 21

7.6 Доказ в органі реєстрації 22

7.7 Доказ недоступності через підписане повідомлення 22

НАЦІОНАЛЬНИЙ ВСТУП

Цей стандарт є тотожний переклад CWA 14365-1:2004 Guide on the Use of Electronic Signatures — Part 1: Legal and Technical Aspects (Настанова з використання електронних підписів. Частина 1. Юридичні та технічні аспекти).

Технічний комітет, відповідальний за цей стандарт в Україні, — «Інформаційні технології» ТК 20.

Сфера застосування цього стандарту охоплює електронні цифрові підписи, що не виконують усі визначені у статті 5.1 Директиви Європарламенту 1999/93/ЕС вимоги до кваліфікованих електронних підписів. Тому в стандарті проаналізовано розбіжності між криптографічним механізмом цифрових підписів, кваліфікованих електронних підписів (відповідно до статті 5.1 Директиви) й електронних підписів (відповідно до статті 5.2 Директиви) у середовищах електронної комерції або в інших сферах, які потребують засобів автентифікації.

До стандарту внесено такі редакційні зміни:

— слова «CWA 14365» замінено на «цей стандарт»;

— структурні елементи стандарту: «Титульний аркуш», «Передмову», «Національний вступ» «Терміни та визначення понять», першу сторінку та «Бібліографічні дані» — оформлено згідно з вимогами національної стандартизації України;

— у розділі 2 «Посилання» наведено «Національне пояснення», виділену в тексті рамкою;

— у «Передмові CWA 14365-1:2004» наведено «Національну примітку», виділену в тексті рамкою;

— у розділі 6 текст «Error! Objects cannot be created from field codes» замінено словом «Рисунок».

Копії міжнародних стандартів, на які є посилання в цьому стандарті можна замовити у Головному фонді нормативних документів.

ПЕРЕДМОВА ДО CWA 14365-1:2004

Успішне впровадження Директиви 1999/93/ЕС Європарламенту від 13 грудня 1999 р. у комунікаційному середовищі для електронних цифрових підписів (Dir. 1999/93/IEC) вимагає стандартів для послуг, процесів, систем і продукції, які стосуються ЕЦП, як і настанов для оцінювання відповідності таких послуг, процесів, систем і продукції.

У 1999 р. Європейська ІСТ Рада стандартів, за підтримки Єврокомісії, ініціативно звела разом промисловість і громадські органи, експертів й інших гравців ринку, щоб запровадити Європейську Ініціативу стандартизації електронних цифрових підписів (EESSI).

У рамках цієї структури Європейський комітет стандартизації/ Система стандартизації інформаційного суспільства (CEN/ISSS) та Інститут європейських стандартів телекомунікації/ Інститут електронних підписів та інфраструктури (ETSI/ESI) довірили виконання робочої програми для розвитку загальноприйнятих стандартів на підтримку виконання Директиви 1999/93/ЕС і поширення Європейської інфраструктури ЕЦП.

Робоча група CEN/ISSS з електронних підписів (WS/E-SIGN) напрацювала набір комплектувальних вузлів, тобто Угоди робочої групи CEN (CWA), які зробили свій внесок у напрямку цих загальновизнаних стандартів. Цей документ одна з таких CWA.

Мета цієї серії CWA полягає в забезпеченні настанови з використання електронних підписів. Дотепер у фокусі розгляду найчастіше перебували «кваліфіковані електронні підписи», визначені в статті 5.1 Директиви 1999/93/ЕС, побічним ефектом чого стало те, що вимоги про використання загальних електронних підписів (так званих «5.2 підписів») в електронній комерції розглянуто недостатньо.

Тому мета цієї частини CWA полягає в описі загальних юридичних і технічних аспектів електронних підписів, і в такий спосіб розширенні роботи над сценаріями електронної комерції, з особливою увагою до технології з високою здатністю розгортання, що викликає довіру без потреби у задоволенні всіх строгих вимог до «5.1 підписів».

Цю частину CWA призначено для використання юридичними й технічними експертами в сфері електронних підписів, а також розробниками систем і продуктів у цій сфері.

Серія CWA складається з таких частин:

— Частина 1. Юридичні та технічні аспекти.

— Частина 2. Профіль захисту для програмних засобів накладання підпису.

Версію цієї частини CWA видано в березні 2004 року.

З переліком осіб і організацій, які підтримали технічну угоду, представлену цією CEN, можна ознайомитися в Центральному секретаріаті CEN.

Національна примітка.

EESSI	— European Electronic Signature Standardization Initiative.
CEN/ISSS	— Information Society Standardization
ETSI/ESI	— Electronic Signatures and Infrastructures
CWA	— CEN Workshop Agreements
CEN	— Європейський комітет стандартизації

НАЦІОНАЛЬНИЙ СТАНДАРТ УКРАЇНИ

НАСТАНОВА З ВИКОРИСТАННЯ ЕЛЕКТРОННИХ ПІДПИСІВ

Частина 1. Юридичні та технічні аспекти

РУКОВОДСТВО ПО ИСПОЛЬЗОВАНИЮ ЭЛЕКТРОННЫХ ПОДПИСЕЙ

Часть 1. Юридические и технические аспекты

GUIDE ON THE USE OF ELECTRONIC SIGNATURES

Part 1. Legal and Technical Aspects

Чинний від 2009–04–01

1 СФЕРА ЗАСТОСУВАННЯ

Директива 1999/93/ЕС Європарламенту від 13 грудня 1999 р. за структурою співтовариства для електронних підписів [Dir.1999/93/EC] — тут і далі Директива — встановлює правові рамки для електронних підписів і послуг сертифікації, щоб сприяти їхньому офіційному визнанню. Як визначено у статті 5.1, електронні підписи, що задовольняють певні якісні показники, так звані кваліфіковані електронні підписи, виконують вимоги до рукописних підписів. У статті 5.2 наведено підсумкову умову, коли електронним підписам не відмовлено у юридичній ефективності й допустимості як доказу у процесуальних діях, навіть якщо не виконано якісних показників кваліфікованих електронних підписів.

Сфера застосування цього стандарту охоплює електронні підписи, що не задовольняють усі визначені у статті 5.1 Директиви вимоги до кваліфікованих електронних підписів. Тому в стандарті проаналізовано розбіжності між криптографічним механізмом цифрових підписів, кваліфікованими електронними підписами (відповідно до статті 5.1 Директиви) й електронними підписами (відповідно до статті 5.2 Директиви). Крім того, щоб зазначити їхню ефективність у середовищах електронної комерції або в інших сферах, де необхідні заходи автентифікації, обговорено випадки використання електронних підписів, що не виконують деякі встановлені в статті 5.1 вимоги.

Крім випадків використання, обговорено доказ, надаваний електронними підписами. Електронні підписи й послуги сертифікації поділено на основні елементи, а потім наданий кожним елементом доказ обговорено з юридичної точки зору, щоб установити зв'язок між технічними елементами та їхнім юридичним ефектом.

Частина 2 цього стандарту містить профіль захисту (PP) для програмних засобів накладання підпису [SCDev-PP], що підходять для таких загальних електронних підписів. Цей профіль захисту потрібен за умовами загального критерію (CC) [ISO 15408]. Він заснований на [SSCD PP], розробленому як стандарт для засобів, здатних створювати кваліфіковані електронні підписи.

Хоча CC PP обрано, щоб підкреслити додану вартість незалежного оцінювання наданих SCDev заходів безпеки, інші критерії оцінки також можуть служити цій меті. Приклади таких критеріїв наведено в [FIPS 140-2] або [ITSEC].

Видання офіційне

2 ПОСИЛАННЯ

2.1 Нормативні посилання

Наступні нормативні документи містять умови, які через посилання в цьому тексті становлять умови цього стандарту; ці публікації не застосовують до застарілих посилань, наступних змін або переглядів. Однак сторони, дійшовши угод, заснованих на цьому стандарті, можуть вивчити можливість застосування нових випусків зазначених нижче нормативних документів. Для недатованих посилань наведено останні видання нормативного документа.

[Dir.1999/93/EC] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a community framework for electronic signatures

[SSCD PP] CEN/ISSS WS/E-Sign Workshop Agreement 14169: Security Requirements of Secure Signature Creation Devices (SSCD), March 2002

[SCDev-PP] CEN/ISSS WS/E-Sign Workshop Agreement 14365-2: Protection Profile for Software Signature-Creation Devices

[ISO 15408] ISO/IEC 15408-1 to 15408-3: Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model, Part 2: Security functional requirements, Part 3: Security assurance requirements, 1999.

НАЦІОНАЛЬНЕ ПОЯСНЕННЯ

[Dir.1999/93/EC] Директива 1999/93/ЕС Європарламенту від 13 грудня 1999 р. про комунікаційне середовище для електронних підписів

[SSCD PP] CEN/ISSS WS/E-Sign Угода симпозіуму 14169: Вимоги безпеки для безпечних засобів накладання підписів (SSCD), березень 2002

[SCDev-PP] CEN/ISSS WS/E-Sign Угода симпозіуму 14365-2: Профіль захисту для програмних засобів накладання підписів

[ISO 15408] від ISO/IEC 15408-1 до 15408-3: Інформаційні технології. Методи захисту. Критерії оцінювання IT-безпеки. Частина 1. Вступ і загальна модель, Частина 2. Функціональні вимоги безпеки, Частина 3. Вимоги гарантій безпеки, 1999.

2.2 Довідкові посилання

[CWA 14170] CEN/ISSS WS/E-Sign Workshop Agreement 14170: Security Requirements for Signature Creation Applications

[CWA 14171] CEN/ISSS WS/E-Sign Workshop Agreement 14171: Procedures for Electronic Signature Verification

[EEC 1980/934] Convention on the law applicable to contractual obligations opened for signature in Rome on 19 June 1980, 80/934/EEC, Official Journal L266

[FIPS 140-2] NIST: Security Requirements for Cryptographic Modules, Federal Information Processing Standard FIPS PUB 140-2, 2001

[HCCH] Hague Conference on Private International Law: Status of the Hague Conventions, online avail. at http://www.hcch.net/

[ISO 10181-2] ISO/IEC 10181-2: Information technology — Open Systems Interconnection — Security frameworks for open systems: Authentication framework, 1996

[ISO 10181-4] ISO/IEC 10181-4: Information technology — Open Systems Interconnection — Security frameworks for open systems: Non-repudiation framework, 1997

[ISO 13888-1] ISO/IEC 13888-1: Information technology — Security techniques — Non-repudiation — Part 1: General, 1997

[ISO 7498-2] ISO 7498-2: Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture, 1989

[ITSEC] Commission of the European Communities: Information Technology Security Evaluation Criteria (ITSEC), Version 1.2, 1991

[TS 101456] ETSI: Policy requirements for certification authorities issuing qualified certificates, TS 101 456, v1.1.1, January 2002

[TS 101733] ETSI: Electronic Signature Formats», ETSI TS 101 733, v1.2.2, December 2000

[TS 101862] ETSI: Qualified Certificate Profile, ETSI TS 101 862, v1.2.1, June 2001

[TS 101903] ETSI: XML advanced Electronic Signatures, ETSI TS 101 903, v1.1.1, February 2002

[TS 102 038] ETSI: XML Formats for Signature Policies, ETSI TR 102 038 v0.0.3, December 2001
[UNCISG] United Nations: United Nations Convention on Contracts for the International Sale of Goods, 1980
[SMIME] B. Ramsdell: S/MIME Version 3 Message Specification, RFC 2633, 1999
[SSL] A.O. Freier, P. Karlton, P.C. Kocher: SSL Protocol, Version 3.0. Netscape Communications Corp., 1996
[TLS] T. Dierks and C. Allen: The TLS Protocol Version 1.0, RFC 2246, 1999.

НАЦІОНАЛЬНЕ ПОЯСНЕННЯ

[CWA 14170] CEN/ISSS WS/E-Sign Угода симпозіуму 14170: Вимоги безпеки для застосувань для створення підпису
[CWA 14171] CEN/ISSS WS/E-Sign Угода симпозіуму 14171: Процедури для верифікації електронних підписів
[ЕЭС 1980/934] Конвенція про закон, застосовний до договірних зобов'язань, відкритих для підписів у Римі 19 червня 1980, 80/934/EEC, Офіційний журнал L266
[FIPS 140-2] NIST: Вимоги безпеки для криптографічних модулів, Федеральний стандарт оброблення інформації FIPS PUB 140-2, 2001
[HCCH] Гаагська конференція з міжнародного цивільного права: Статус Гаазької угоди, онлайн допомога. в http://www.hcch.net/
[ISO 10181-2] ISO/IEC 10181-2: Інформаційні технології. Взаємозв'язок відкритих систем. Безпечне середовище відкритих систем: Середовище автентифікації, 1996
[ISO 10181-4] ISO/IEC 10181-4: Інформаційні технології. Взаємозв'язок відкритих систем. Безпечне середовище відкритих систем: Середовище неспростовності, 1997
[ISO 13888-1] ISO/IEC 13888-1: Інформаційні технології. Методи захисту. Неспростовність. Частина 1. Загальні положення, 1997
[ISO 7498-2] ISO 7498-2 Системи оброблення інформації. Взаємозв'язок відкритих систем. Базова еталонна модель. Частина 2. Архітектура безпеки, 1989
[ITSEC] Єврокомісія: Критерії оцінювання IT-безпеки (ITSEC). Версія 1.2, 1991
[TS 101456] ETSI: Вимоги політики для органів сертифікації, що випускають посилені сертифікати, TS 101 456, v1.1.1, січень 2002
[TS 101733] ETSI: Формати електронних підписів, ETSI TS 101 733, версія 1.2.2, грудень 2000
[TS 101862] ETSI: Профілі посилених сертифікатів, ETSI TS 101 862, версія 1.2.1, червень 2001
[TS 101903] ETSI: XML-просунуті електронні підписи, ETSI TS 101 903, версія 1.1.1, лютий 2002
[TS 102 038] ETSI: XML-формати для політик підписів, ETSI TS 102 038 v версія 0.0.3, грудень 2001
[UNCISG] Організація Об'єднаних Націй: Конвенція ООН з контрактів для міжнародного продажу товарів, 1980
[SMIME] B. Ramsdell: Специфікація повідомлення S/MIME версії 3, RFC 2633, 1999
[SSL] A.O. Freier, P. Karlton, P.C. Kocher: Протокол SSL, версія 3.0,. Netscape Communications Corp., 1996
[TLS] T. Dierks и C. Аллен: Протокол TLS, версія 1.0, RFC 2246, 1999.

3 ТЕРМІНИ ТА ВИЗНАЧЕННЯ ПОНЯТЬ ТА АБРЕВІАТУРИ

3.1 Терміни та визначення понять

Кваліфікований електронний підпис (*QES, Qualified electronic signature*)

Електронний підпис, що задовольняє вимоги, встановлені у статті 5(1) Директиви 1999/93/ЕС, тобто розширений електронний підпис, заснований на посиленому сертифікаті й створений надійним засобом накладання електронного підпису.

Директива 1999/93/ЕС

Директива Європарламенту від 13 грудня 1999 р. про комунікаційне середовище для електронних підписів в OJ EC 19.1.2000, L12/12.

3.2 Абревіатури

AS	Розширений електронний підпис	Advanced electronic Signature
CC	Загальні критерії, Версія 2.1	Common Criteria Version 2.1
CEN	Європейський комітет стандартизації	Comite Europen de Normalisation (European Committee for Standardization)

CEN/ISSS	Європейський комітет стандартизації/ Система стандартизації інформаційного суспільства	CEN Information Society Standardization System
CGA	Генеральне застосування сертифікації	Certification Generation Application
CPS	Припис (заява) практики сертифікації	Certification Practice Statement
CRL	Список скасованих сертифікатів	Certificate Revocation List
CWA	Угода Робочої групи CEN (Європейська практична угода)	CEN Workshop Agreement
DTBS	Підписувані дані	Data to be Signed
EAL	Гарантований рівень оцінювання	Evaluation Assurance Level
EC	Єврокомісія	European Commission
EESSI	Європейська ініціатива стандартизації електронних цифрових підписів	European Electronic Signature Standardization Initiative
ETSI	Європейський інститут стандартів з телекомунікації	European Telecommunications Standards Institute
ETSI SEC	Технічний комітет із безпеки ETSI	ETSI Security Technical Committee
HI	Користувацький інтерфейс	Human Interface
HW	Апаратне забезпечення	Hardware
I/O	Ввід/вивід	Input/Output
ISSS	Система стандартизації інформаційного суспільства	Information Society Standardisation System
NRO	Неспростовність	Non-Repudiation of Origin
OCSP	Мережний протокол статусу сертифікатів	Online Certificate Status Protocol
OS	Операційна система	Operating System
PC	Персональний комп'ютер	Personal Computer
PDA	Персональний цифровий асистент (помічник)	Personal Digital Assistant
PGP	Досить гарна конфіденційність	Pretty Good Privacy
PIN	Персональний ідентифікаційний номер	Personal Identification Number
PKIX	Інфраструктура відкритих ключів	Public Key Infrastructure (X.509)
PP	Профіль захисту	Protection Profile
QC	Посилений сертифікат	Qualified Certificate
RAD	Еталонна дата автентифікації	Reference Authentication Data
RSA	Алгоритм Рівеста-Шаміра-Адлемана	Rivest, Shamir, Adleman
SAR	Вимоги оцінювання безпеки	Security Assurance Requirement
SCA	Застосування накладання підписів	Signature-Creation Application
SCD	Дані накладання підписів	Signature-Creation Data
SCDev	Засіб накладання підписів	Signature Creation Device
SDO	Підписаний об'єкт даних	Signed Data Object
SFP	Політика функціонального захисту	Security Functional Policy
SFR	Вимоги функціонального захисту	Security Functional Requirement
S/MIME	Безпечний протокол передачі електронної пошти	Secure Multi-Purpose Mail Extension
SOF	Стійкість функції	Strength of Function
SSCD	Безпечний пристрій створення підпису	Secure Signature-Creation Device
SSL	Протокол захищених сокетів	Secure Socket Layer
SVD	Дані верифікації підпису	Signature-Verification Data
TLS	Протокол безпеки транспортного рівня	Transport Layer Security
TOE	Об'єкт оцінювання	Target of Evaluation
VAD	Верифіковані дані автентифікації	Verification Authentication Data
WS/E-SIGN	CEN/ISSS робоча група ЕЦП	CEN/ISSS Electronic Signatures workshop

4 ЕЛЕКТРОННИЙ ПІДПИС З ТЕХНІЧНОЇ ТА ЮРИДИЧНОЇ ТОЧОК ЗОРУ

Для подальшого обговорення в цьому стандарті різних типів електронних підписів корисно спочатку розглянути визначення ISO, що стосуються послуг захисту, які використовують механізм цифрового підпису: автентифікацію, цілісність даних і неспростовність (див. 4.1).

Крім того, потрібно врахувати чотири основних типи електронних підписів, які можна виділити з юридичної точки зору (див. 4.2).

4.1 Технічне визначення послуг захисту

автентифікація (*Authentication*)

Забезпечення необхідної ідентичності об'єкта [ISO/IEC 10181-2].

автентифікація джерела даних (*Data origin authentication*)

Підтвердження того, що джерело отриманих даних таке, як потрібно [ISO 7498-2].

автентифікація рівноправного/однорівневого об'єкта *(Peer entity authentication)*

Підтвердження того, що рівноправний/однорівневий об'єкт у з'єднанні — такий, як потрібно [ISO 7498-2].

цілісність даних (*Data integrity*)

Така властивість, що дані не змінено або знищено у несанкціонований спосіб [ISO 7498-2].

спростовність (*Repudiation*)

Заперечення одним із залучених у комунікацію об'єктів того, що він брав участь у всій або частині комунікації [ISO 7498-2].

неспростовність джерела (*Non-repudiation of origin*)

Послугу призначено для захисту від помилкової відмови ініціатора від фактів створення контента й відправлення повідомлення [ISO/IEC 13888-1].

неспростовність (*Non-repudiation*)

Послугу призначено для обрання, підтримки, надання й підтвердження незаперечних доказів щодо потрібної події або дії з урегулювання спорів про появу або непояву події чи дії [ISO/IEC 10181-4].

В **автентифікації** варто звернути увагу на те, що фактично існує два різних типи послуг автентифікації: *автентифікація джерела даних й автентифікація рівноправного/однорівневого об'єкта.*

У контексті цього документа автентифікацію джерела даних пов'язано з передачею підписаних повідомлень, які потім може перевірити одержувач. Тому автентифікація джерела даних — це послуга, якій у Директиві більше підходить загальне визначення «електронний підпис», описане в наступному розділі. Приклад застосування для цієї мети механізму цифрового підпису — підписана за протоколом S/MIME електронна пошта.

Автентифікація рівноправного/однорівневого об'єкта пов'язана з автентифікацією сторони, що спілкується в on-line-сесії. Приклад застосування для цієї мети механізму цифрового підпису — автентифікація клієнта й сервера, що використовує протокол захищених сокетів [SSL] або протокол безпеки транспортного рівня [TLS].

Цілісність даних гарантує виявлення змін у переданих даних незалежно від того, чи відбулося це внаслідок зловмисної атаки або через помилки передачі. Приклад застосування для цієї мети механізму цифрового підпису — повторно підписана за протоколом S/MIME електронна пошта.

Для **неспростовності** стандарти [ISO 7498-2] та [ISO/IEC 13888-1] визначають кілька типів послуг неспростовності. Загальне визначення послуг неспростовності наведено в [ISO/IEC 10181-4]. Ту з них, яку зазвичай пов'язують з електронними підписами, насправді визначено як «неспростовність джерела». Застосовуючи це визначення, варто врахувати, що «факт створення контенту повідомлення» стосується електронного підпису, створеного підписувачем, і не обов'язково підписаного документа. Неспростовність джерела (NRO) також є послугою, якій у Директиві найбільше підходить визначення кваліфікованого електронного підпису («5.1 підпису»), описане далі в цьому стандарті. Зазвичай, послуга NRO не захищає підписувача від подальшої відмови від його електронного підпису; вона лише ускладнює для нього доказ цього у разі суперечки, а в деяких юридичних системах послуга NRO навіть

припускає, що електронний підпис є справжнім. Приклад застосування з цією метою механізму цифрового підпису — підписана юридично обов'язкова угода, що задовольняє всі вимоги безпеки кваліфікованого електронного підпису.

4.2 Підписи з юридичної точки зору

4.2.1 *Технічні та юридичні аспекти*

Як обговорено в попередньому розділі, цілісність даних, автентифікація в з'єднанні рівноправних вузлів і автентифікація джерела даних — це просто технічні визначення, взяті з технічних стандартів. Щоб юридично оцінити послуги, надавані їхньою технічною реалізацією, варто покластися на науковий і технологічний доказ, перевіривши таке:

a) якщо електронний підпис справжній, тобто

— він відповідає конкретній людині і

— його не підроблено;

b) якщо підписані дані справжні, тобто

— вони відповідають даним, наданим підписувачеві, і

— їх не змінено.

Неспростовність — це складніша послуга, при цьому технологію варто доповнити юридичним поняттям неспростовності. Неспростовність у юридичному середовищі стосується не тільки самого підпису, а й усних оголошень і поведінки.

У юридичних термінах неспростовність підпису визначають у такий спосіб:

a) відповідно до застосовуваних правових норм у відкритих співтовариствах, і/або

b) відповідно до угоди в конкретних співтовариствах, які можуть бути відкритими або закритими, залежно від їхньої політики.

Елементи юридичної неспростовності також відрізняються залежно від функції підпису й типу підписаного документа/даних. Серед них можна виділити три різних типи:

a) несемантичні (тобто просто технічні) елементи, наприклад дійсність, цілісність;

b) контекстні або семантичні елементи, що залежать від технічних і юридичних оцінок, наприклад знання, намір, задум, розуміння, інтерпретація, насильство, помилка, обман, дійсна недієздатність тощо;

c) просто юридичні елементи, наприклад законна сила/недієздатність, правоздатність/неправоздатність, повноваження.

Неправильно й марно давати технічне визначення неспростовності без врахування юридичних елементів неспростовності, наданих відповідно до застосовуваних правових норм і/або згідно з угодою. Більше того, якщо є всі технічні докази, у сторін усе ще, можливо, немає достатньої інформації для висновку юридично обов'язкової угоди.

Юридичні аспекти функціональності підпису не залежать від рівня достовірності/довіри. Письмовий документ і підписаний олівцем папір — правочинні, незалежно від рівня достовірності/довіри паперу й олівця. Завжди краще мати функціональність, підібрану до відповідного рівня достовірності/довіри. Проте юридично функціональність підпису як і раніше доступна (або може бути доступна). Технічне й юридичне визначення неспростовності логічно або автоматично не еквівалентні. Навіть якщо технічні особливості підпису не повністю адекватні (написаний від руки заповіт; сформульована й підписана на папері письмова угода), підпис можна вважати юридично обґрунтованим. У статті 5.2 Директиви передбачено, що електронні підписи не потрібно дискримінувати через їхні технічні недоліки, а треба визнати як можливий доказ за аналогією з тим, як визнають як доказ сучасні технічно слабкі рукописні підписи.

4.2.2 *Підписи з функціональної точки зору*

Ґрунтуючись на певних характеристиках підписів з юридичної точки зору, наступні визначення описують чотири основних функції підписів — підпису для ідентифікації, підпису для автентифікації, підпису як оголошення знання і підпису як волевиявлення. Використовуючи механізм цифрового підпису, всі подані нижче підписи (за винятком підпису для ідентифікації) також забезпечують цілісність даних.

A. Підпис для ідентифікації (*Signatures for Identification*). Цей підпис збігається з визначенням ISO для автентифікації рівноправних/однорівневих об'єктів. Приклад такого підпису — виклик/відповідь у разі автентифікації клієнт—сервер, використовуваної в таких протоколах, як SSL і TLS. У цьому разі жодний документ не підписується; підписується тільки беззмістовне «nonce», що надає «доказ воло-

діння» секретним ключем. Найчастіше їх не розглядають як «електронний підпис» у термінах Директиви, оскільки вони не пов'язані з якими-небудь даними, а трактуються як специфічне застосування механізму «цифрового підпису».

B. Підпис для автентифікації *(Signatures for Authentication)*. Цей підпис збігається з визначенням ISO для автентифікації джерела даних, якщо дані розглядають як об'єкт, а не як документ із певним семантичним значенням. (Якщо в підписаних даних є певне семантичне значення, яке підпис має підтвердити, то у нас є й/або буде підпис для оголошення знання). Підпис призначено тільки для підтвердження того, що повідомлення створене зазначеним відправником. Власне підпис не має на увазі, що відправник якось схвалює вміст (контент) повідомлення, і може бути повністю автоматизований без втручання або розуміння людини. Приклад такого електронного підпису — S/MIME-підпис, використовуваний у багатьох поштових застосуваннях.

C. Підпис для оголошення знання *(Signatures for declaration of knowledge)*. Цей тип підпису — щось середнє між попереднім і наступним типом підпису. Цей підпис також забезпечує автентифікацію джерела даних (відповідно до визначення ISO), але при цьому дані також мають семантичну значимість. Важливо знати семантичне значення підписаних даних, але немає потреби в особливому волевиявленні/намірі сторони, що підписує; зазвичай вистачить того факту, що оголошення підписано. Іноді з юридичної точки зору несуттєво, чи підпис зроблено навмисно, важливо тільки, що він справжній і що підписаний документ постачає правильну інформацію. Тоді процедура створення підпису також не важлива: не має значення, чи відбулася помилка, чи навмисна омана. Має значення тільки, що підпис і вміст (контент) документа — справжні. Інакше кажучи, якщо використано такий тип підпису, виходить, що сторона-підписувач повідомляє, що вона прийняла знання семантичного значення підписаних даних, але це не означає, що вона схвалює підписані дані. У сторони-підписувача немає певного волевиявлення. Цей підпис може підтримувати послуга неспростовності (відповідно до визначення ISO) зі спеціальною ознакою, включеною в елементи підписаних даних, для оголошення намірів підпису: оголошення знання. Альтернативний інструмент для розпізнання підписаного оголошення знання може надати IT-інфраструктура.

D. Підпис як волевиявлення *(Signatures as declaration of will)*. Цей підпис надає неспростовність (відповідно до визначення ISO), за якої дані мають семантичну значимість і описують необхідний випадок або дію. Однак оскільки підпис виражає певне волевиявлення сторони-підписувача, необхідно не тільки знання семантичного контенту, а й належне розуміння (семантичного й процедурного) контексту створення підпису. Тому такий підпис необхідно генерувати під повним контролем сторони-підписувача.

4.2.3 *Потреба нетехнічного доказу*

У паперовому світі зміст і функцію підпису оцінюють через:

— фізичний контекст підпису (за яким видом підтримки його закріплено, семантика підтримки тощо). Фізичний контекст підпису самоочевидний і (зазвичай) не вимагає технічних інструментів, які перевірятимуть й оцінюватимуть;

— семантичний контекст накладення підпису (час, місце й інші зовнішні обставини, за яких підпис створено). Зазвичай така інформація стає доступною або через підтримку підписання, або через свідків;

— семантичний контекст перевірки (час, місце й інші зовнішні обставини, за яких підпис перевірено). Зазвичай контекст такої перевірки — легальний засіб (суд, юридична фірма тощо).

У світі цифрових технологій фізичний контекст підпису, створення підпису, контекст перевірки не є настільки явними. Свідки зазвичай недоступні з огляду на те, що зазвичай електронні підписи використовують дистанційно (транзакції на відстані). Це означає, що тільки електронний підпис, що здатен нести (по суті) також багато очевидної інформації, як і рукописний, є електронним підписом, якому притаманна значимість, що не залежить від семантики підписаних даних та контексту створення й перевірки підпису. Такими електронними підписами є тільки підписи для ідентифікації й автентифікації.

Щоб належним чином оцінити електронні підписи для оголошення знання або волевиявлення, необхідна докладніша інформація. У контексті EESSI частково зачіпають ці проблеми ETSI-специфікації щодо профілю посиленого сертифіката [TS 101862], специфікації за вимогами політики для CSP [TS 101456], політики підписання [TR 102 038] і форматами електронних підписів [TS 101 733] [TS 101 903] і CEN-специфікації для створення [CWA 14170] і перевірки підпису [CWA 14171].

У минулому столітті процес накладання й перевірки достовірності підпису для рукописних підписів був досить неформальним. Відповідні специфікації для електронних підписів формалізують і структурують ці процеси й тому не в змозі врахувати всі можливі контексти й значимість підпису, використовуваного й прийнятого сьогодні в юриспруденції.

4.2.4 ***Особливості функціональних підписів***

У таблиці наприкінці цього розділу показано складність людської діяльності, пов'язану з чотирма розглянутими функціональностями підписів людини.

Для розуміння таблиці, у якій розглянуто рукописні й електронні підписи, треба знати суттєві відмінності між рукописними й електронними підписами. Ці відмінності впливають на оцінку процесу створення підпису з юридичної/функціональної точки зору:

- Процес рукописного підпису сприймається, впливає й контролюється безпосередньо через відчуття людини (зір, дотик, слух, мова); єдиний інструмент, використовуваний у такому процесі, має несамостійну функціональність і повністю пасивний у руках сторони-підписувача. Процес створення електронного підпису набагато складніший, підтримується й контролюється підписувачем лише за допомогою дуже складної інфраструктури, що по суті не перебуває під його/її повним керуванням. Підписувач управляє, можливо, тільки засобом SCDev, який зазвичай є лише одним з багатьох компонентів, необхідних для виконання електронного підпису.
- Процес створення рукописного підпису здалеку підписувач завжди сприймає як такий і має повністю відмінний ритуал (й інакше юридично оцінюється) від со-розташованого процесу створення рукописного підпису. Процес створення електронного підпису не так відрізняється, якщо він виконується на відстані або со-розташований, крім можливості особистої біометричної ідентифікації залучених сторін: основну відмінність створюють засоби захисту й відкритість IT-інфраструктури, на якій його виконано. Абстрактно IT-інфраструктура може перебудовувати всі особливості со-розташованого підпису, включаючи біометричну ідентифікацію, що навіть збільшує надійність процесу створення підпису, порівняно з надійністю со-розташованого рукописного підпису.
- Свідки працюють належним чином у процесі створення рукописного підпису, якщо такий процес со-розташований: фактично свідок корисний у юридичних термінах, якщо в нього є повне й пряме сприйняття будь-якої юридично обґрунтованої рушійної сили. Якщо рукописні підписи створено на відстані, свідок також повинен бути носієм DTBS, щоб бути ефективним свідком. Для цього свідок електронних підписів повинен знати про два види фактів: (a) як працює метод, використовуваний IT-інфраструктурою для накладання підпису; (b) людська діяльність підписувачів і її контекст. Спосіб передачі даних має значення тільки тоді, якщо дуже слабкі технічні особливості створених підписів.

Усі згадані вище розбіжності не впливають на перевірку технічних характеристик підпису. Вони також несуттєві з позицій технічної неспростовності: фактично технічна неспростовність — це збирання незаперечних доказів для розв'язання спорів про входження або невходження волевиявлення, породженого під конкретною назвою, що входить до сертифікату відкритого ключа. Не можна з технічної неспростовності зробити висновок про юридичну неспростовність. Як показано в 4.2.1, законність підпису юридично не залежить (винятково) від його технічної якості, але залежить від якості контексту процесу накладання підпису й від особистих якостей (знання, воля вибору, розумова здатність тощо) підписувача. Технічна якість підпису — це лише незначна проблема в процесі юридичного оцінення підпису.

Проте вплив контексту на функціональну змістовність і на юридичну значимість підпису значно відрізняється, залежно від того, що є спеціальною функцією такого підпису. І знову ці відмінності мають значення тільки з винятково технічної точки зору.

У наведеній нижче таблиці показано корисний інструмент для розуміння різних взаємодій між контекстом, семантикою й процесом створення підпису.

Характеристики	Підпис для автентифікації	Підпис для оголошення знання	Підпис як волевиявлення/ оголошення про наміри
1 Індивідуальність	Я знаю, хто я	Я знаю, хто я	Я знаю, хто я
2 Місце	Я знаю, де я[1]	Я знаю, де я[1]	Я знаю, де я[1]
3 Дані	Дані можуть мати значення/сенс	Дані мають значення/сенс	Дані повинні мати значення/сенс
4 Контекст створення підпису	Дані беруть участь у процесі	Дані беруть участь у процесі і, можливо, підписувач також	Дані беруть участь у процесі і підписувач також повинен
5 Знання даних	Я можу розуміти значення/сенс даних	Я можу розуміти значення/сенс даних і ...	Я розумію, що значення/сенс даних залежить від моїх намірів і ...
6 Особливий намір	Немає значення	...тому я хочу підписатися	... тому я хочу підписатися
7 Інформованість процесу	Необов'язкова	Обов'язкова	Обов'язкова
8 Дивись, що я підписав	Можливо, мені знадобиться побачити те, що я підписав	Мені необхідно бачити те, що я підписав	Мені необхідно бачити те, що я підписав
9 Дія підписання	Підписувач може бути пасивний	Підписувач активний	Підписувач активний
10 Зв'язок з даними у процесі	Між підписувачем і даними є зв'язок. Обоє важливі як факти	Між підписувачем і даними є зв'язок. Обоє важливі як факти. У контексті створення підпису важлива семантика	Між підписувачем і даними є зв'язок. Обоє важливі як факти. У контексті створення підпису важлива семантика
11 Повністю функціональний	Так	Можуть знадобитися недодаткові дії	Зазвичай можуть знадобитися недодаткові дії

5 ПОРІВНЯННЯ ВИЗНАЧЕНЬ ПІДПИСІВ

5.1 Термін та визначення поняття цифровий підпис

цифровий підпис (*Digital signature*) **ISO 7498-2:1989**

Дані, прикріплені до або криптографічно перетворені елементи даних, що дають змогу одержувачеві елементів даних перевірити джерело елементів даних і захистити від фальсифікації/підроблення, наприклад одержувачем

Це визначення допускає використовувати механізм цифрового підпису для захисту електронних елементів даних у різних контекстах. Підписувач/одержувач елемента даних не обов'язково є людиною: це може бути апаратний пристрій, комп'ютерна програма або будь-який інший об'єкт. Уявіть, наприклад комунікацію між універсальним комп'ютером і вимірювальними приладами агентства з прогнозування погоди, коли датчики відправляють дані на універсальний комп'ютер через супутникове з'єднання. Для цього виду застосувань цифрові підписи можна використовувати як механізм для забезпечення передачі даних від пристроїв у мережі. Це приклад застосування цифрових підписів у середовищі, де комунікація відбувається не між людьми, а між машинами. Аналогічно цифрові підписи можна використовувати для перевірки джерела й цілісності Java-аплета, активізованого між сервером і клієнтом в Інтернеті, або для захисту зображення, знятого камерами контролю за швидкістю руху дорожнього транспорту. Цифрові підписи також дають можливість контролювати достовірність і цілісність програмних виправлень, проведених через Інтернет. Аналогічно цифрові підписи можна використовувати між людьми для забезпечення автентифікації джерела даних, цілісності даних і неспростовності.

Усупереч певним законам підпису визначення ISO не обмежує цифровий підпис використанням асиметричної криптографії, хоча нині це найчастіше використовувана технологія. Однак використовуючи асиметричну криптографію для цифрових підписів, механізм цифрового підпису не надає двох головних властивостей:

— знання власника відкритого ключа;

— знання того, що секретний ключ під час підписання перебував під повним керуванням підписувача.

Перша властивість зазвичай надається у разі використання сертифікатів відкритих ключів. Другу властивість, наприклад можна надати у разі використання інформації про статус сертифіката (CRL або OCSP) або токена штемпеля часу або мітки часу.

Для цифрового підпису, який засновано на сертифікаті відкритого ключа й вважають технічно достовірним (згідно з визначенням ISO цифрового підпису), необхідно довести, що цифровий підпис застосований у той час як сертифікат підписувача був чинний. Оскільки в багатьох випадках не можна покладатися на зазначений підписувачем час або знання того, коли підпис створено, то можна використовувати верхню межу часу, отриману у разі використання токена штемпеля часу або мітки часу, прикріплених до цифрового підпису:

— Мітка часу — це запис у контрольному журналі безпеки, принаймні, що включає достовірне значення часу й геш-подання елемента даних.

— Токен штемпеля часу — це підписана структура даних, яку випустив Орган штемпелювання часу й яка включає, принаймні, достовірне значення часу й геш-подання елемента даних.

Якщо використано штемпель часу або мітки часу, то для доказу, що цифровий підпис згенеровано в той момент, коли діяв сертифікат підписувача, цифровий підпис варто перевірити на виконання двох умов:

— токен штемпеля часу або мітка часу застосовані до закінчення періоду чинності сертифіката підписувача;

— токен штемпеля часу або мітку часу застосовано або в момент, коли сертифікат підписувача ще не було скасовано, або до дати скасування сертифіката.

5.2 Термін та визначення поняття електронний підпис

Стаття 2 Директиви 93/1999/ЕС
Визначення

Для цілей цієї Директиви:

1. «електронний підпис» означає дані в електронній формі, **які приєднані до або логічно пов'язані з іншими електронними даними** і *слугують методом автентифікації;*

2. «розширений електронний підпис» означає електронний підпис, що виконує такі вимоги:

(a) він унікально пов'язаний із підписувачем;

(b) він може ідентифікувати підписувача;

(c) його створено з використанням засобів, які підписувач може повністю контролювати;

(d) пов'язаний з даними таким чином, що можна легко виявити будь-яку наступну зміну даних.

Електронний підпис — це дані, прикріплені до або логічно пов'язані з (так звані окремі підписи) іншими електронними даними, які мають функцію, що допускає встановити зв'язок між підписаними даними й людиною. Цей зв'язок може слугувати тільки для оцінення присутності перед даними, знанням даних, прийняттям даних, оголошенням даних і/або джерелом/продукцією даних. Отже, електронний підпис — це набір цифрових процедур для підтвердження можливої юридичної значущості даних для конкретної людини або групи людей. Точну семантику електронного підпису визначають деякі інші засоби.

Відповідно до статті 5.2 Директиви держави — члени ЄС мають визнавати юридичну значимість електронно підписаних даних. Для визначення правових меж юридичної значимості будь-яких технічних засобів для підписання, перевірки достовірності, підтвердження й прийняття цифрових даних у Директиві виділено категорію «електронні підписи».

У такий спосіб «електронний підпис» — це здебільшого юридичне поняття, тому вони існують тільки там, де юридична система допускає юридичну значимість цифрового доказу.

У юридичній науці зазвичай розрізняють факт і навмисну дію. У кожній юридичній системі межі між цими двома поняттями можуть істотно відрізнятися. Проте між документом з підписом, що має значення навмисної дії, і документом, розглянутим тільки як доказ факту, є фундаментальна розбіжність, визнана в будь-якій юридичній системі. У багатьох юридичних системах рукописний підпис — це безперечний доказ існування навмисного оголошення. В інших системах для оцінення існування навмисної дії треба розглянути більше аспектів.

Тому ці юридичні відмінності не можуть вплинути на технічні особливості електронного підпису: юридичну значимість електронного підпису визначають тільки в конкретній юридичній системі, у якій його застосовують.

Слід також зазначити, що за визначенням «електронний підпис» не пропонує використовувати асиметричну криптографію; можна застосовувати й симетричну криптографію. Фактично за визначенням навіть не потрібно використовувати криптографію, якщо виконано встановлені вимоги.

5.3 Термін та визначення поняття розширений електронний підпис

Розширений електронний підпис — це електронний підпис, що виконує чотири вимоги безпеки, викладені вище й обведені у рамку у статті 2 розділу 5.2 Директиви. Вимоги сформульовано без прив'язки до якої-небудь технології: несуттєво, якими технологічними засобами досягають мети безпеки. Тому визначення залишає простір для подальших нововведень у цій сфері.

Проте на практиці вкрай важко працювати з таким широким і не прив'язаним до якої-небудь технології визначенням. У разі суперечки суддя, арбітр або експерт щоразу має перевірити, виконано чи ні чотири вимоги безпеки. Оскільки вимоги сформульовано досить узагальнено, залишається великий простір для особистих суджень, результат яких важко вгадати. Тому ця настанова прагне допомогти у визначенні юридичних наслідків технічних розбіжностей між електронними підписами загалом і розширеними електронними підписами.

Технічна відмінність між електронними підписами й розширеними електронними підписами прямо не впливає на юридичну значимість цих підписів. Ці технічні відмінності можуть вплинути тільки на спосіб подання суду технічних доказів для визначення точної юридичної значимості підписаних даних.

Щоб одержати критерії відмінності розширеного підпису від електронного, потрібно не тільки просто виконувати чотири вимог, наведені у статті 2.2 Директиви. Можливі різні тлумачення статті 2.2. Тому необхідно проаналізувати різні вимоги розширеного електронного підпису.

a) «Унікально пов'язаний з підписувачем» як найчастіше використовуваний нині механізм для його реалізації — це сертифікат aX.509. Можливі такі унікальні посилання на підписувача:
   i) посилений сертифікат (X509), який за визначенням завжди випускає третя довірена сторона;
   ii) непосилений сертифікат X509:
      1) випущений третьою довіреною стороною;
      2) випущений безпосередньо підписувачем;
   iii) будь-який інший вид електронної атестації, що відповідає визначенню, установленому в статті 2.9 Директиви, тобто який поєднує дані верифікатора підпису з підписувачем і підтверджує їхню ідентичність підписувачеві (як можливу через надійні середовища, банківську справу, кліринг, телекомунікацію, ISP-служби тощо).

Зв'язок між розширеним електронним підписом і підписувачем створено за допомогою посилання на сертифікат у підписі. Сам сертифікат також довільно можна прикласти до підписаного документа. Це дає можливість підтверджувати електронний підпис, без потреби on-line-роботи і завантаження даних верифікації підпису (SVD — Signature Verification Data) від провайдера послуг сертифікації (CSP — Certification Service Provider).

Незважаючи на орієнтацію цього документа переважно на інфраструктуру відкритих ключів X.509 (PKIX — Public Key Infrastructure), можливі й інші, засновані на X.509 сертифікати, які можуть також відповідати умовам Директиви.

b) «Здатний до ідентифікації підписувач»: Це означає, що має існувати можливість ідентифікації підписувача через переданий на розгляд сертифікат. Без наявності такої технічної особливості це буде тільки електронний (а не розширений електронний) підпис. Навіть якщо посилання на підписувача можна довести іншими засобами (наприклад звіти ISP, E-свідок або запам'ятовування транзакції через мережного провайдера), неможливо класифікувати такий підпис як розширений. Проте якщо CSP містить анкетні дані, які ідентифікують підписувала, то можна одержати посилання на нього, використовуючи псевдонім зі сертифіката.

c) «Створене використання означає, що підпис може перебувати під його повним контролем». Ця вимога для керування доступом до засобу створення підпису (SCDEV), що містить дані про створення підпису (SCD). Керування доступом реалізують так, щоб підписувач, використовуючи певну процедуру, міг переконатися в тому, що його/її SCD і/або SCDev можна використовувати тільки для підписання даних. Це означає, що підписувачеві так чи інакше, ймовірно, доведеться бути «активним» у захисті його/її секретних даних.

(Примітка. Як визначено в Додатку III і потрібно для кваліфікованих електронних підписів, з надійним засобом накладання підпису (SSCD) від підписувача не потрібно жодних дій на підтримку таємниці його/її SCD. Йому варто втриматися тільки від розкриття даних активації його SCD, збережених у його SSCD).

У такий спосіб керування доступом для створення розширеного електронного підпису має такі характеристики:

i) якщо SCDev — це незалежний засіб, що має лише одну функцію підписання даних, таку вимогу можна застосовувати тільки до SCDev;

ii) якщо SCDev — це багатофункціональний засіб, наприклад ПК, ноутбук, кишеньковий комп'ютер або мобільний телефон, вимогу має виконувати застосування створення підпису (SCA) і/або доступ до SCD;

iii) можна застосовувати резервну копію/відновлення ключа зі спеціальними процедурами для взяття його під повний контроль підписувача;

iv) заборонено застосовувати умовне депонування ключа, оскільки за визначенням воно унеможливлює повний контроль над SCD.

Необхідно зазначити, що вимога про повний контроль унеможливлює використання симетричної криптографії, за якої секретний ключ відомий як підписувачеві, так і верифікатору.

d) «Так пов'язаний з даними, до яких він має стосунок, щоб було легко виявити будь-яку наступну їхню зміну». Це призводить до таких вимог:

i) підписання справжнього подання даних. Зазвичай це реалізують підписанням криптографічного гешування даних. Тільки задовольняючи певні якісні метрики, геш-функції можуть забезпечити надійний спосіб виявлення змін у підписаних даних. Тому не прийнятний, наприклад циклічний надлишковий контроль (CRC);

ii) особливості безпеки:

1) алгоритм підписання має відповідати потрібній безпеці (алгоритм достатньої сили);

2) ключові дані мають відповідати потрібній безпеці. Особливо треба убезпечити довжину ключа від грубих силових рішень «у лоб» та інших атак.

5.4 Термін та визначення поняття кваліфікований електронний підпис

Стаття 5 Директиви 93/1999/ЕС

1. Держави-члени мають гарантувати, що засновані на посиленому сертифікаті й накладені засобом надійного створення розширені електронні підписи:

(a) виконують юридичні вимоги до підпису стосовно даних в електронній формі тим самим способом, яким рукописний підпис виконує ці вимоги стосовно паперових даних; і

(b) прийнятні як доказ у процесуальних діях.

Щоб уникнути технічно і юридично складної оцінки доказу, у статті 5.1 Директиви 93/1999/ЕС уведено третій рівень підпису, який зазвичай називають **«кваліфікований електронний підпис»**. Кваліфіковані електронні підписи — це розширені електронні підписи, що виконують вимоги безпеки, перелічені у додатках Директиви. Вимоги стосуються вмісту (контенту) сертифіката, на якому засновано електронний підпис (додаток I), якості випускального цей сертифікат (додаток II) і технічних засобів, використовуваних для створення підпису (додаток III).

За наведеним у Директиві визначенням, кваліфікований електронний підпис — це, по-перше, розширений електронний підпис.

Дотримуючись наведеного (зокрема) у статті 2.2 Директиви визначення й доповнюючи його вимогами, поданими в додатках I, II і III Директиви, до кваліфікованого електронного підпису висувають такі вимоги:

a) кваліфікований електронний підпис має містити посилання на посилений сертифікат, випущений CSP, що задовольняє вимогам додатка II;

b) кваліфікований електронний підпис має допускати ідентифікацію підписувача за посиленим сертифікатом, на який посилається. Якщо використано псевдонім, відповідно до національного законодавства, CSP може бути зобов'язаний показати особисті ідентифікувальні дані власника сертифіката;

c) для створення кваліфікованого електронного підпису варто використовувати SSCD. Крім того, не можна використовувати умовне депонування ключа, оскільки воно за визначенням виключає повний контроль над SCD;

d) кваліфікований електронний підпис має бути так пов'язаний із даними, яких він стосується, щоб можна було виявити будь-яку наступну зміну даних, як описано вище.

Проте найсуттєвіші відмінності мають юридичну природу і є наслідком формулювання статті 5.1 Директиви, у якій визначено не технічні засоби, а функціональні вимоги й вимоги безпеки. Тому покладемося на формально обґрунтоване визначення відмінностей між розширеними й кваліфікованими електронними підписами, щоб не ввести в оману.

Наслідок з юридичної точки зору можна сформулювати в такий спосіб: **Це відповідальність одержувача підписаного повідомлення за перевірку того, що підпис дійсно є кваліфікованим електронним підписом, і тому заслуговує на довіру як такий.** Це можна описати так (посилаючись на попередній параграф):

a) сертифікат, на який посилаються у підписаному повідомленні, варто ідентифікувати як посилений (наприклад використовуючи розширення QC або посилаючись на політику QC);

b) схема контролю має гарантувати, що посилений сертифікат, який випустив CSP, задовольняє вимоги, викладені у додатку II Директиви;

c) використовувану для створення підпису технологію SSCD схвалено;

d) якщо в сертифікаті заявлено політику «QC + SSCD», CA має гарантувати, що SCD утримується в SSCD. Інакше треба якимосць іншим способом забезпечити його одержувача.

5.5 Юридична значимість різних видів електронного підпису

У статті 5 Директиви 93/1999/ЕС європейський законодавець визначив юридичну значимість:

— «5.1 підписам» надавати ту саму значимість, що й рукописним підписам, жадати від національного законодавства гарантій того, що кваліфіковані електронні підписи виконують юридичні вимоги до підпису стосовно даних в електронній формі так, як рукописні підписи виконують ці вимоги щодо паперових даних;

— «5.2 підписам» не можна відмовити в юридичній значимості винятково на такій підставі:

Стаття 5 Директиви 93/1999/ЕС

1. (Викладені вище)

2. Держави-члени мають гарантувати, що в процесуальних діях не заперечують юридичну ефективність і допустимість як доказу електронного підпису винятково на тій підставі, що він:

— в електронній формі; або

— не заснований на посиленому сертифікаті;

— не заснований на посиленому сертифікаті, випущеному акредитованим провайдером послуг сертифікації;

— не створений надійним засобом накладання підпису.

Основна відмінність між юридичними визначеннями двох типів електронних підписів у статті 5 полягає в тому, що є позитивне визначення 5.1 підписів і лише відмінне визначення іншого електронного підпису, оскільки з юридичної точки зору 5.2 підпис — це будь-який електронний підпис, що не є 5.1 підписом.

Тому варто роз'яснити випадки, коли є тільки один тип або багато типів 5.2 підписів. Відповідь очевидна: є принаймні два типи 5.2 підписів, розширений і нерозширений.

Чи існують інші підписи, відмінні за формулюванням від двох типів 5.2 підписів? Раніше стверджувалося, що відмінність юридичної значимості не можна визначити окремо від конкретної юридичної системи. Юридична значимість підписів також значно відрізняється в кожній юридичній системі.

6 ВИПАДКИ ВИКОРИСТАННЯ НЕКВАЛІФІКОВАНОГО ЕЛЕКТРОННОГО ПІДПИСУ

У реальних системах проектувальники можуть умонтувати систему, що не містить усіх компонентів, потрібних кваліфікованому електронному підпису відповідно до Директиви, але використовує описану в Директиві інфраструктуру. У цьому розділі обговорено електронні підписи, що не є кваліфікованими, оскільки в них відсутні деякі з визначених у статті 5.1 Директиви елементи, проте вони показують цінні випадки використання.

Можливі багато які інші випадки некваліфікованих електронних підписів, але вони не залучені в розглядувану сферу застосування.

Додана обробляннням вартість електронних підписів, якою користуються деякі, але не всі елементи, визначені в статті 5.1 для кваліфікованих електронних підписів, також явно сформульовані в докладному описі (20) Директиви в такий спосіб.

Докладний опис (20) з Директиви 93/1999/ЕС

(20) Погоджені критерії щодо юридичних результатів електронних підписів зберігають послідовні правові рамки у всьому Співтоваристві; національне законодавство встановлює різні вимоги до юридичної законності рукописних підписів; оскільки сертифікати можна використовувати для підтвердження ідентичності людини, що підписується електронно; **засновані на посилених сертифікатах розширені електронні підписи прагнуть підвищеного рівня безпеки**; засновані на посиленому сертифікаті й накладені засобом надійного створення розширені електронні підписи можна вважати юридично еквівалентними рукописним підписам, тільки якщо виконано вимоги до рукописних підписів

У цьому розділі спочатку описано випадок використання кваліфікованого електронного підпису, а потім — електронного підпису, у якому один компонент одноразово відсутній. По-перше, в 6.2 обговорено випадок використання, надрукований **грубим шрифтом** у цитаті наведеного вище докладного опису (20), а в 6.3 — електронні підписи, у яких відсутнє придатне подання документа. Нарешті, в 6.4 обговорено розширені електронні підписи, що використовують засоби SSCD, але не засновані на посилених сертифікатах.

6.1 Компоненти кваліфікованих електронних підписів

Як визначено в Директиві, у системи підпису є три основних компоненти: розширена сигнатура (AS), посилений сертифікат (QC) і надійний засіб створення підпису (SSCD). Використання цих компонентів під час перевірки підпису верифікатором проілюстровано на наступному рисунку.

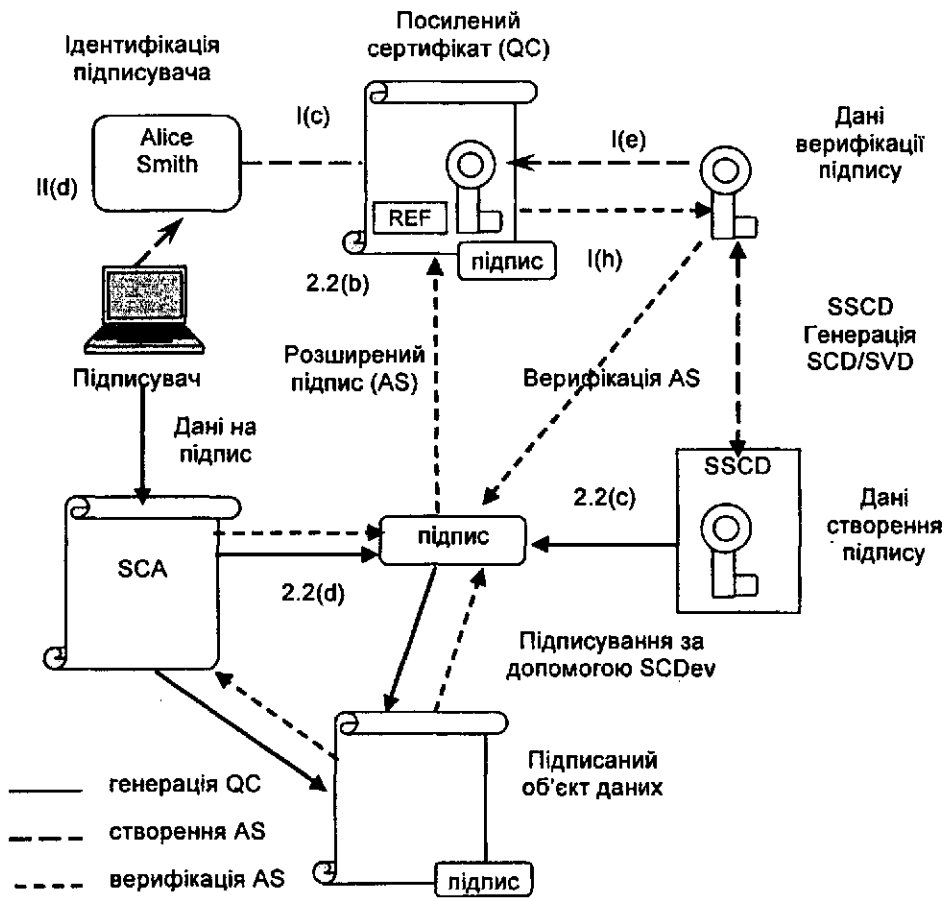


Рисунок 1

AS, QC і SCDev пов'язують елементи формування сертифіката, створення й перевірки електронних підписів. Для простоти припустимо, що SCDev реалізує обидва криптографічних механізми: для формування пари SCD/SVD і цифрових підписів як частин AS.

QC містить ім'я підписувача або псевдонім, ідентифікований як такий (див. додаток I, c). Ідентичність людини, для якої випускають QC, варто перевіряти за допомогою CSP (див. додаток II, d). CSP перевіряє відповідність SVD, включеного в QC, SCD, що перебуває під контролем підписувача (див. додаток I, e). Якщо CSP одержує SVD від SSCD, то CSP пов'язує підписувача й SSCD і просить SSCD забезпечити доказ відповідності між SCD і SVD. CSP вживає заходи захисту від підроблення сертифікатів (див. додаток II, h) і підписує QC за допомогою AS (див. додаток I, h). QCP може визначати спеціальні правила для використання SSCD і наданих послуг SSCD.

Підписувач використовує SCA для підготовки даних, які підписують (DTBS) для створення розширеного підпису (AS). AS пов'язує DTBS і AS таким чином, щоб виявляти будь-яку подальшу зміну даних (стаття 2.2, d). Це посилання встановлює механізм цифрового підпису, складений з геш-функції й алгоритму підписання. Повний контроль підписувача SCD (стаття 2.2, c) приводить до:

(a) асиметричних криптографічних методів для створення підпису за допомогою SCD і для перевірки підпису за допомогою SVD;

(b) контролю над використанням SCD.

Зазначимо, що використовуючи код автентифікації повідомлення (MAC), заснований на таких симетричних криптографічних механізмах, як ISO 9797, можна створити електронний, а не розширений електронний підпис. Той самий ключ використовують для формування й перевірки MAC і він не може перебувати під повним контролем підписувача. Контроль за використанням підписувачем SCD залежить від життєвого циклу SCD і SSCD, реалізованого SCD. Докладніше це питання обговорено у наступному підрозділі.

6.2 Розширений електронний підпис без SSCD

У статті 2(6) Директиви визначено засіб створення підпису, що відповідає встановленим у Додатку III вимогам, як «засіб надійного створення підпису». У преамбулі Директиви заявлено в докладному описі (15), що Додаток III покриває вимоги для надійних засобів створення підпису для гарантії функціональності розширених електронних підписів. Держави — члени ЄС визначають уповноважені органи влади, відповідальні за оцінку відповідності надійних засобів підпису відповідно до Додатка III.

Безпека SCD і створення підпису залежить від SSCD і методу його використання. Середовище SSCD визначає загрози, яких стосується SSCD за умови використання TOE. SSCD реалізує всі функції IT-безпеки, необхідні для гарантування таємниці SCD і заходів підтримки безпеки для захисту передачі SVD в CGA і середовище створення підпису.

Проте засіб створення підпису (SCDEV), використовуваний для накладання розширеного підпису, не можна розглядати як SSCD у контексті статті 5.2, оскільки:

a) у разі дуже високої безпеки й реального задоволення вимог Додатка III безпеку не оцінює й не схвалює вповноважений орган влади;

b) SCDev не в змозі забезпечити достатні заходи безпеки на виконання вимог Додатка III.

У першому випадку безпека електронного підпису не може залежати від гарантії властивостей безпеки SCDev, даної відповідно до оцінки безпеки вповноваженого органа влади. Гарантія властивостей безпеки SCDev може ґрунтуватися на оголошенні виробника або може бути відсутня. Підписувач, що скасовує свій підпис, може послатися на потенційні слабкості безпеки в життєвому циклі SCD, які уможливлюють підроблення підпису. Тому безпеку SCD і SCDev для неспростовності підписів важко продемонструвати. Проте розширений електронний підпис може все-таки послужити меті автентифікації джерела й цілісності даних.

Другий випадок стосується широкої сфери практичних рішень із захисту SCD і процесу створення підпису за додаткової умови використання SSCD. Ключова умова — безпечне IT-середовище. Припустимо, що SCDev реалізовано як програмне забезпечення для стандартних персональних комп'ютерів. Тоді SCDev працює під операційною системою (OS), що забезпечує кожному процесу доступ до таких IT-ресурсів, як збережені дані, екран, клавіатура й пам'ять. Неактивний SCDev — це просто ряд даних, які можна читати й обробляти. Тому захист SCD і самозахист SCDev обмежені. Заходи безпеки SSCD від інших загроз істотно залежать від IT- і не IT-середовища. Підписувачу варто гарантувати ці заходи безпеки. Це здійсненно, якщо SCD, SCDev і IT-середовище перебувають під його повним керуванням.

Але повністю управляти IT-середовищем дуже важко або неможливо, навіть якщо на ПК підписувача працює SCDev. Отже, підписувач зобов'язаний домогтися компромісу між необхідною для його електронного підпису безпекою й заходами безпеки середовища підписання, включаючи SCDev.

У профілі захисту в документі [SCDEV-CTP] описано один потенційний підхід, який можна прокоментувати у такий спосіб:

(1) SCDev перебуває під повним контролем підписувача. Підписувач — це єдиний зареєстрований користувач SCDev, включаючи всі такі функції адміністратора, як інсталяція й ініціалізація;

(2) SCDev використовує сильні криптографічні механізми для генерації пари SCD/SVD і для цифрових підписів;

(3) SCDev забезпечує автентифікацію користувача й керування доступом для використання згенерованої пари SCD/SVD і створення підпису. Дані автентифікації (пароль) підписувача — це таємниця, не збережувана електронно;

(4) SCDev реалізує елементарні заходи самоперевірок для захисту себе від помилок і маніпуляцій;

(5) SCDev покладається на захист операційною системою поділу домену. не IT-середовище має фізично захистити SCD, SCDev та IT-платформу.

Тепер розглянемо випадок використання розширених підписів без SSCD, проілюстрований на рисунку.

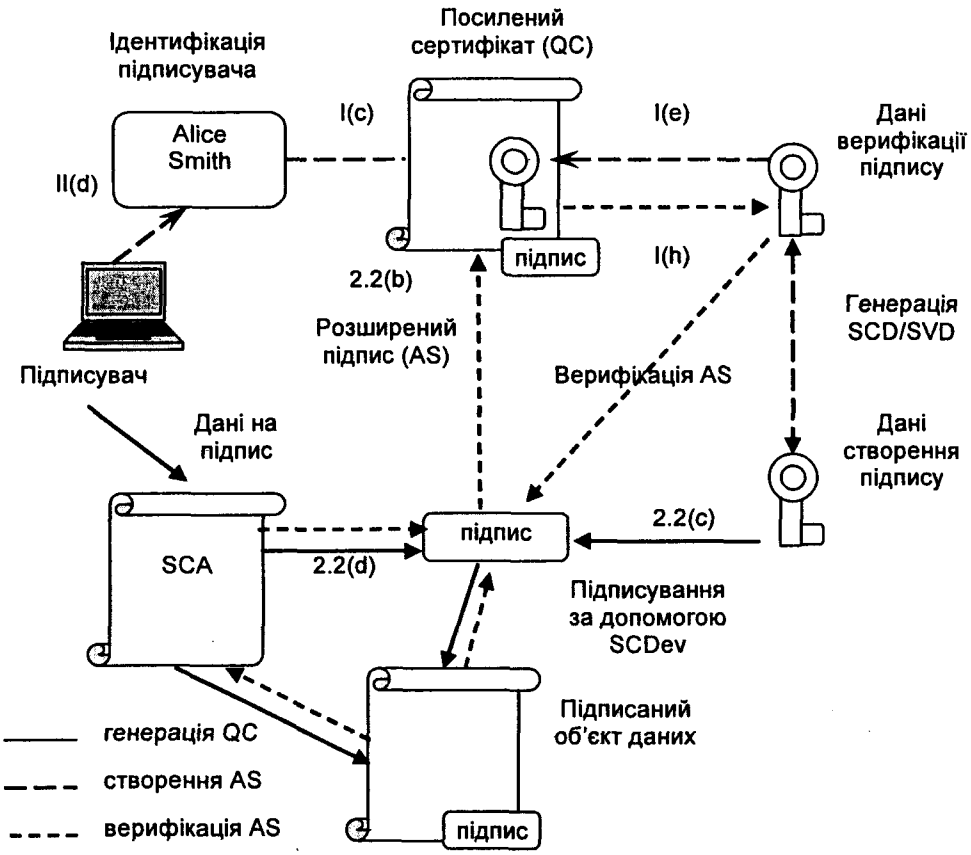


Рисунок 2

У цьому разі відсутнє посилання на механізм захисту, що зміцнює зв'язок QC із SCD. За відсутності цього посилання належного захисту SCD необхідно, щоб верифікатор довіряв підписувачеві. Хоча система у разі використання може забезпечити ще більший захист, ніж SSCD, у Директиві визначено, що це некваліфікований електронний підпис, оскільки не виконано вимоги Додатка III або не оцінено вповноваженим органом влади.

Отже, ця система для належного захисту SCD і доречного використання тільки SCD вимагає, щоб верифікатор довіряв підписувачеві. У цієї системи є потенційно слабше за SSCD посилання на людину-підписувача; оскільки захист SCD не сильний, підписувач може потім стверджувати, що SCD захопив і використав якийсь інший об'єкт.

Проте втрата сторонньої гарантії захисту SCD, можливо, не стає проблемою в деяких середовищах; якщо верифікатор може гарантувати за допомогою яких-небудь інших засобів, що SCD задіяно в захищеному місці, у верифікатора може з'явитися впевненість щодо підпису, як у разі нормального кваліфікованого електронного підпису. Якщо верифікатор не може цього стверджувати, то він не може зіставити SCD з підписувачем.

У цьому разі верифікатор, можливо, не здатен домогтися неспростовності в суді, що діє за нормами загального права, але в закритому середовищі це може не знадобитися. Приклад такого використання — система, у якій SCD задіяно для ідентифікаційних карток компанії. Картку може не оцінити SSCD, але у разі її використання цього вистачить для підписання внутрішніх документів. Якщо використання картки прив'язане до фізичної безпеки, наприклад коли картку використовують лише там, де застосовують й інші міри захисту, це може бути ще сильніше рішення за SSCD.

Технічна якість і безпека SCDev суттєво залежать від визначення якості доказу. Із цієї причини варто розглянути застосування профілю захисту для визначення вимог безпеки SCDevs. Такі CTP, що визначають мінімальні вимоги до забезпечення цілісності й автентифікації джерела підписаних даних, наведено в [SCDEV-CTP]. CTP спроектовано як цілком програмну реалізацію. Іншими критеріями оцінення, застосовними для забезпечення технічної якості SCDev, є [FIPS 140-2] або [ITSEC].

6.3 Розширений електронний підпис без посиленого сертифіката

У системі, відображеній на рисунку, відсутній посилений сертифікат, що зв'язує ідентичність підписувача з парою SCD/SVD. Замість цього, SVD доступний верифікатору в інший спосіб, наприклад за допомогою непосиленого сертифіката або PGP.

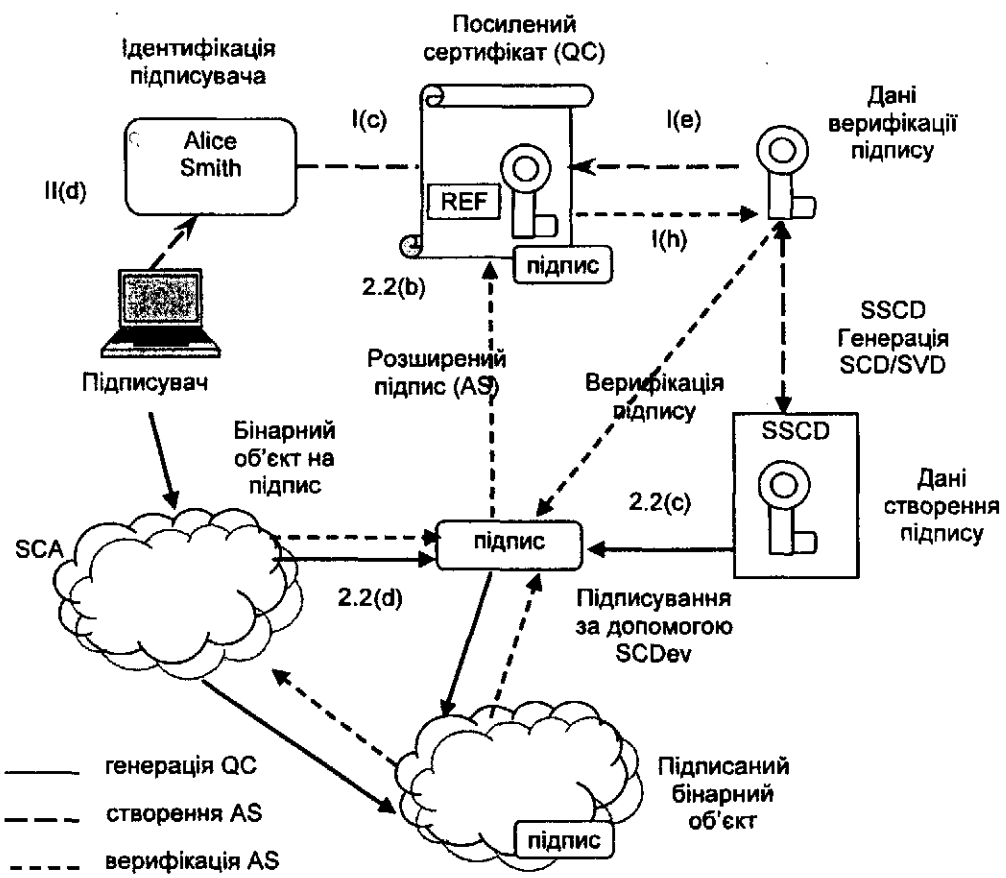


Рисунок 3

У цьому разі система дає змогу верифікатору знати, що підписувач використав SCD від SSCD для створення підпису, але верифікатор може не перевіряти стороннє знання того, ким був підписувач. Верифікатор може також знати, чи інформація належним чином була подана підписувачу. Є кілька випадків використання, що випливають із цієї моделі системи: автентифікація джерела, цілісність даних, анонімність, пряме відношення й підписання групою.

У випадку використання автентифікації джерела SVD міститься в сертифікаті, якому усе ще довіряє верифікатор, хоча це не посилений сертифікат. Підпис усе ще має «юридичну ефективність і допустимість як доказ у процесуальних діях», але він може не мати такого самого юридичного ефекту, як рукописний підпис.

Випадок використання цілісності даних дуже важливий, його не слід пропускати. Підпис під даними, поданими підписувачу, а потім підписаними з використанням SSCD, дає змогу верифікатору згодом виявити незмінність документа. Якщо верифікатору не важливо, хто підписав документ, а важливо тільки, що документ підписаний належним чином, така система працює добре. Проте верифікатор не може стверджувати, що документ підписала конкретна людина.

Випадок використання анонімності дає змогу підписувачу підписуватися з використанням SSCD і залишатися певною мірою анонімним, наприклад у разі використання псевдоніма в сертифікаті. Зазвичай у верифікатора немає прямих доказів того, хто цей підписувач.

Випадок використання «прямого відношення» заснований на припущенні, що підписувач ідентифікує себе, надає відкритий ключ і доказ володіння в прямому контакті з верифікатором. Типовий приклад — церемонія обміну ключами з досить гарною конфіденційністю (PGP).

Тепер верифікатор може, дивлячись на два підписаних об'єкти, довідатися, що їх підписав той самий підписувач. Хоча верифікатор не може юридично довести, що це той самий підписувач, у верифікатора можуть з'явитися серйозні підстави для припущення, що обидва об'єкти підписав той самий підписувач, якщо верифікатор знає про фізичний захист для SCD, особливо якщо використано SSCD. Якщо SSCD перебуває під контролем одного об'єкта, тоді верифікатор може знайти хронологію інформації, що стосується підписувача. Ця інформація дасть можливість верифікатору з високим ступенем точності ідентифікувати підписувача.

Випадок підписання групою — заключний приклад для корпоративного використання. SSCD зберігають в корпоративному сейфі й вилучають за контрольованих обставин. Якщо пізніше об'єкт представляється як підписувач-корпорація, природно, у верифікатора є досить інформації, щоб припустити, що підписувачем є корпорація. Верифікатор не знає, який корпоративний чиновник насправді створив підпис, але верифікатору й не важливо, хто зробив це, а важливо тільки те, що підпис створила компанія.

Який із цих випадків використання фактично застосовний у конкретній ситуації, залежить від того, чи важлива для верифікатора ідентичність підписувача і чи довіряє він необхідному зв'язку між підписувачем і SVD (за допомогою непосиленого сертифіката або PGP).

6.4 Цифровий підпис без подання даних

У цьому разі систему використовують для підписання в цифровій формі й перевірки бінарних даних, складених з випадкового числа, «nonce». Зазначимо, що цей цифровий підпис також не є «електронним підписом», оскільки не пов'язаний з жодними даними.

У кількох державах — членах ЄС у законах про підпис заборонено використовувати SSCDs з метою, відмінною від створення кваліфікованих електронних підписів, і у жодному разі від застосування різних ключів для кваліфікованих електронних підписів на документах, а для підписання «nonce» уважають «гарною практикою». Проте «SCDev, використовуваний для підписання в цифровій формі nonce» може дотепер входити в аналогічний SSCD фізичний пристрій, а SCDev — оцінювати щодо вимог SSCD і тому мати високий рівень безпеки. Проте формально SCDev, що містить SCD для підписання «nonce», не є SSCD, а створюваний цифровий підпис не є електронним підписом.

Цей випадок використання описано тут лише для завершеності.

У цьому випадку використання верифікатор знає, що «nonce» не змінено, що підписувач підписав «nonce» і що SCD належним чином захищений в SCDev. Однак верифікатор не знає, чи має «nonce» даних яке-небудь значення для підписувача.

Для захисту верифікатора від подальшої вимоги, що інформація представляє якийсь контракт або іншу інформацію, підписувач повинен мати однозначний індикатор того, що він у цифровій формі підписує «nonce», а не документ. Цей однозначний індикатор може постачати SCA у форматі підпису або

з використанням окремого ключа з відповідним сертифікатом, що вказує, як ключ застосовують тільки для підписання великих бінарних об'єктів/BLOBs. Один із прикладів такого індикатора використання ключа — це «використання ключа digitalSignature» в X.509 для автентифікації.

Рисунок 4

Зазначимо, що використання SCD для інших засобів, крім підписання документів, може обійти таємність SCD. Наприклад якщо алгоритми підпису в SCD уразливі для окремих атак на відкритий текст, застосовуючи такі варіанти використання, варто пам'ятати про це. Їх можна запобігти, наприклад забезпечивши гешування «nonce» до використання SCD.

Типове використання цієї системи — схема доказу володіння або автентифікації підписувача. Тоді «nonce» — це просто випадкове число. У разі перевірки виробленого цифрового підпису «nonce» верифікатор знає, що підписувач контролював SCDev і авторизував підписання «nonce». Цього досить, щоб довести верифікатору, що підписувач брав участь у процесі підписання; отже, верифікатор може підтвердити ідентичність, оголошену в сертифікаті.

Приклад такого використання — це ID-картка компанії, що є SSCD, а також містить належним чином створений SCDev з SCD і SVD. Якщо застосування автентифікації надсилає SCDev для підписання «nonce», належним чином підписаний «nonce» доводить, що підписувач має картку й що він лише авторизував використання SCDev. Це забезпечує зовсім безпечну автентифікацію користувача.

Крім того, у підписувача пізніше можуть виникнути ускладнення у разі спростування того, що він створив підпис; те, що він може спростувати, є потенційним поданням даних. Із цієї причини за такого використання системи не можна довіряти контенту «nonce» або його поданню для підписувача. Якщо сертифікат містить індикатор використання ключа та заявляє, що ключ дозволено використовувати тільки для підписання «nonce» у цифровій формі, не виникне небезпеки неправильного вживання цього ключа.

7 ДОКАЗ ДЛЯ ЕЛЕКТРОННИХ ПІДПИСІВ

Як показано раніше, «електронний підпис» — це досить широке поняття, що слугує багатьом цілям.

У разі суперечки про підпис на електронному повідомленні варто врахувати всі доступні докази для валідації підпису й урегулювання спорів. При цьому можуть виникати, наприклад проблеми, коли підписувач:

- взагалі заперечує виконання підпису;
- визнає виконання підпису, але для іншого повідомлення.

Як описано далі, більшість необхідних для різних типів електронних підписів технічних доказів аналогічні й їх можна знайти в підписаному повідомленні й у таких документах, на яких воно посилається, як сертифікат, CPS і політика підписання. Проте зазначимо, що:

- підпис як волевиявлення/оголошення про наміри вимагає доказу контексту, у якому підпис створено. Це описано в останньому підрозділі цього розділу.

7.1 Докази, наявні у підписаних даних

Підписані дані самі по собі містять такі основні елементи доказу, потрібні для встановлення законності підпису:

- документ підписувача: електронні дані, до яких приєднано чи з якими логічно пов'язано електронний підпис;
- підпис: рядок битів, отриманий у процесі підписання з використанням SSCD або SCDev;
- ознака застосування алгоритмів для гешування документа й підписання значення геш-функції;
- однозначне посилання на сертифікат підписувача, який обрав підписувач, наприклад який задовольняє самому собі або посиланню на нього, можливо, разом зі значенням геш-функції із сертифіката.

Підписані дані можуть також містити такі додаткові докази:

- ознака використання SSCD для створення підпису. Хоча нині його застосовують не так широко, цього можна досягти, наприклад за допомогою додаткового підпису, створеного залежним від конкретного засобу ключем у SSCD. У загальному випадку політика сертифікації, на яку посилається сертифікат підписувача або інші специфікатори у сертифікаті, може вказувати на використання SSCD;
- штемпель часу, застосований у цифровому підписі, випущено надійним Органом штемпелювання часу (TSA), що вказує час, до якого створено підпис;
- інформація про шлях сертифіката до одного надійного вказівника, як визначено політикою підписання;
- інформація про статус сертифіката, яке доводить, що він був дійсний у потрібний час створення підпису. Проте зазначимо, що цю інформацію верифікатор збирає і зберігає впродовж перевірки підпису після певного «пільгового періоду» для гарантії, що сертифікат не було скасовано (заблоковано) під час створення підпису;
- тип фіксації транзакції, що відображає семантику підпису. Тип фіксації транзакції можна вказувати в електронному підписі неявно або явно, використавши «ознаки типу фіксації транзакції» у форматі електронного підпису, або явно — у семантиці підписаних даних;
- індикатор місця розташування, що задає конкретне місце розташування підписувача під час, коли він або вона наклав підпис;
- індикатор часу підписувача, що задає конкретний час застосування підпису;
- роль, під якою застосовано підпис;
- посилання на політику підписання, під якою затверджено підпис (див. далі).

7.2 Наявні у сертифікаті докази

Сертифікат, випущений органом сертифікації, на який посилається або який міститься в підписаному повідомленні, включає такі додаткові елементи доказу:

- ознака того, чи випущено сертифікат як посилений, чи ні (додаток I);
- позначення органу, що випустив сертифікат, наприклад провайдер послуг сертифікації й держава, у якому він діє (додаток I);
- посилання на політику сертифікації й/або припис практики сертифікації, які виконує CA у разі випуску сертифіката;
- ім'я підписувача або псевдонім, які ідентифікують підписувача як такого (додаток I);
- дані верифікації підпису, що відповідають даним створення підпису під керуванням підписувача (додаток I);

• вказівка початку й кінця терміну дії сертифіката (додаток I);
• неявне або явне посилання на інформацію про статус сертифіката (listCRL скасування сертифіката або мережний протокол статусу сертифікатів OCSP);
• код ідентичності сертифіката (додаток I);
• розширений електронний підпис випускального провайдера послуг сертифікації (додаток I).

Опціонально сертифікат може також містити:
• обмеження на сферу використання сертифіката, якщо вони застосовні (додаток I);
• границі значень транзакцій, у яких використовують сертифікат, якщо вони застосовні (додаток I).

7.3 Докази, наявні у політиці сертифікації та/або CPS

Політика сертифікації та/або CPS видана CA містить значну інформацію про виконані вимоги та/або процедури, використовувані для випуску сертифіката, тим самим засвідчує про достовірність/довіру сертифіката. Найважливішими елементами доказу, пов'язаними із законністю підпису, є такі:
• вказівка, чи випущено сертифікат як посилений чи ні;
• опис процедур для встановлення ідентичності власника сертифіката;
• вказівка, чи підтверджує CA, що секретний ключ (SCD) зберігається в SSCD чи ні;
• опис процедур безпеки для CA, наприклад пов'язаних із захистом ключа CA.

7.4 Доказ щодо статусу сертифіката

Під час перевірки підписаного повідомлення варто встановити статус сертифіката (скасований або чинний) на момент **створення підпису**. Цей тип доказу можна надати двома способами:

• Після одержання повідомлення одержувач підписаного повідомлення перевіряє статус сертифіката (використовуючи CRL або OCSP) і зберігає цю інформацію разом з повідомленням (можливо, також штемпелем часу; див. також 7.1, де описано штемпелі часу як додатковий доказ). Зазначимо, що одержувачеві може знадобитися інформація про статус у два різних моменти часу: один раз — безпосередньо після одержання підписаного повідомлення, а другий — після певного пільгового періоду, що допускає будь-яке можливе скасування для передачі службі інформації про статус сертифіката. Потім одержувач переконується в одержанні доступу до відповідної інформації про статус, у разі виникнення подальших суперечок.

• CA зберігає «історичну» інформацію про статус сертифіката й за запитом надає таку інформацію. CRL має містити таку історичну інформацію протягом періоду чинності сертифіката, але її можна видалити з CRL після закінчення періоду чинності сертифіката.

7.5 Докази, наявні у політиці підписання

Політика підписання — це низка правил, що стосується створення й перевірки електронного підпису, за яких підпис визначають як достовірний. У цьому юридичному/договірному контексті можна визнати, що конкретна політика підписання задовольняє вимоги. Політику підписання може випускати, наприклад сторона, що покладається на електронні підписи, й вибирати підписувача для використання цією стороною. Альтернативно, політику підписання можна встановлювати через співтовариство електронної торгівлі для використання серед його учасників. Підписувач і верифікатор використовують одну й ту саму політику підписання.

Політика підписання може бути неявною або явною. Політику підписання можна надавати як частину підписаного документа, поза передачею або іншими способами. Політику підписання можна явно ідентифікувати або передбачати семантикою підписуваних даних і/або інших зовнішніх даних, як за контрактом, на який посилаються і який сам посилається на політику підписання, так і за допомогою контексту підписання. У явної політики підписання для відкритого використання є глобально унікальне посилання, яке підписувач зв'язав з електронним підписом як частину обчислення підпису.

Політика підписання може включати таке:
• правила побудови/перевірки шляху сертифіката (включаючи вказівку використовуваних довірених кореневих сертифікатів);
• правила використання інформації про статус скасування (наприклад CRL або відповіді OCSP);
• правила використання синхронізації інформації, маркування часу й/або штемпелів часу;
• дані перевірки підпису, надані підписувачем;
• дані перевірки підпису, зібрані верифікатором.

Політика підписання також може включати:
• період, протягом якого можна виконувати підписи з цією політикою;

- список розпізнаних типів фіксації транзакції;
- правила використання ролей підписувача;
- будь-які обмеження на алгоритми підпису й довжину ключа;
- інші правила політики підписання, яким має задовольняти мета підпису.

7.6 Доказ в органі реєстрації

Мінімальних елементів, яких вимагає додаток I Директиви, не досить, щоб чітко й однозначно ідентифікувати власника сертифіката.

Орган реєстрації (RA),який діє від імені CSP, може зберігати реєстраційну інформацію, надану під час реєстрації. Наявного в сертифікаті імені підписувача не завжди вистачає для його однозначної ідентифікації.

У такому разі спочатку надана частина інформації може (або має відповідно до національного законодавства) однозначно ідентифікувати особу. Це також потрібно для використання псевдоніма.

Отже, навіть ідентичність підписувача є інформацією, не обов'язково надаваною підписом (навіть некваліфікованим електронним підписом), це потрібно, щоб можна було послатися на джерела інформації, що не обов'язково містяться в підписаних даних.

7.7 Доказ недоступності через підписане повідомлення

Наступний «нетехнічний» доказ потрібен для встановлення контексту створення підпису, і таким чином, становить необхідний доказ для електронного підпису, аналогічно оголошенню схвалення через навмисну дію:

- документ підписаний як навмисна дія. Незалежно від технічних доказів підписувача однаково могли обдурити або змусити підписатися під примусом;
- підписувач читав і зрозумів завершений документ. Хоча технічне середовище створення підпису дає можливість йому читати завершений документ, воно не може змусити його зробити це. Крім того, необхідно встановити, що документ написаний мовою, зрозумілою підписувачу.

Можуть знадобитися такі додаткові докази:

- місце підписання. Для деяких договірних ситуацій це суттєво і це треба доводити;
- юридична система, застосовувана для підписаного документа.

Для документів, підписаних кількома підписувачами, може також знадобитися встановити порядок підписання й присутність усіх підписувачів у тому самому місці на момент підписання.

Код УКНД 03.160; 35.040; 35.240.60

Ключові слова: автентифікація, відкритий ключ, Директива Європарламенту 1999/93/ЕС, електронний цифровий підпис, кваліфікований електронний підпис, неспростовність, посилений сертифікат, послуги сертифікації.

Редактор **О. Перевозчикова**
Технічний редактор **О. Касіч**
Коректор **Т. Нагорна**
Верстальник **С. Павленко**

Підписано до друку 17.08.2009. Формат 60 × 84 1/8.
Ум. друк. арк. 2,79. Зам. 1936 Ціна договірна.

Виконавець
Державне підприємство «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» (ДП «УкрНДНЦ»)
вул. Святошинська, 2, м. Київ, 03115

Свідоцтво про внесення видавця видавничої продукції до Державного реєстру видавців, виготівників і розповсюджувачів видавничої продукції від 14.01.2006 р., серія ДК, № 1647