НАЦІОНАЛЬНИЙ СТАНДАРТ УКРАЇНИ

НАСТАНОВИ ЩОДО РЕАЛІЗАЦІЇ БЕЗПЕЧНИХ ЗАСОБІВ СТВОРЕННЯ ПІДПИСІВ

(CWA 14355:2004, IDT)

ДСТУ CWA 14355:2009

Видання офіційне

Київ
ДЕРЖСПОЖИВСТАНДАРТ УКРАЇНИ
2011

ПЕРЕДМОВА

1 ВНЕСЕНО: Технічний комітет зі стандартизації «Інформаційні технології» (ТК 20)

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

2 НАДАНО ЧИННОСТІ: наказ Держспоживстандарту України від 15 грудня 2009 р. № 452 з 2011–07–01

3 Національний стандарт відповідає CWA 14355:2004 Guidelines for the implementation of Secure Signature-Creation Devices (Настанови щодо реалізації безпечних засобів створення підписів)

Ступінь відповідності — ідентичний (IDT)
Переклад з англійської (en)

4 УВЕДЕНО ВПЕРШЕ

НАЦІОНАЛЬНИЙ ВСТУП

Цей стандарт є тотожний переклад CWA 14355:2004 Guidelines for the implementation of Secure Signature-Creation Devices (Настанови щодо реалізації безпечних засобів створення підписів).

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

Стандарт містить вимоги, які відповідають чинному законодавству України.

У стандарті описано критерії захисту безпечних засобів створення підпису та наведено результати аналізу порівняння та сумісності цих критерії у серіїї стандартів Europsmart.

У CWA 14170:2004 введено термін «кваліфікований підпис», визначений в Директиві як розширений електронний підпис (*advanced electronic signature*), заснований на посилених сертифікатах (*qualified certificate*), створених безпечними (надійними) засобами накладання електронних підписів (*secure signature creation device*). Згідно з Законом України «Про електронний цифровий підпис» від 22 травня 2003 року №852-IV вважають юридично правомочним (валідним) термін «кваліфікований підпис».

До стандарту внесено такі редакційні зміни:

— слова «CWA 14355» замінено на «цей стандарт»;

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

— у розділі 2 «Нормативні посилання» і «Бібліографії» наведено «Національні пояснення», виділені в тексті рамкою;

— усі рисунки по тексту стандарту подано з підрисунковим надписом на відміну від CWA 14355;

— у «Змісті» подано розділи, підрозділи та пункти на відміну від CWA 14355, де наведено підпункти;

— по тексту стандарту знаки «•» і «–» замінено на тире, а «°» — на «•».

Додаток І — довідковий.

Копії документів, на які є посилання в тексті цього стандарту, можна замовити в Головному фонді нормативних документів.

ПЕРЕДМОВА ДО CWA 14355:2004

Успішна реалізація європейської директиви Dir. 1999/93/EC про публічну структуру для електронних підписів [Dir. 1999/93/EC] вимагає стандартів для служб, процесів, систем і продуктів, пов'язаних з електронними підписами, так само як настанови для оцінки погодженості таких служб, процесів, систем і продуктів.

У 1999 р. Європейська рада стандартів ICT за підтримки Єврокомісії розпочала ініціативу, що поєднує юридичних і фізичних осіб, експертів і інших ринкових гравців, для створення європейської електронної ініціативи зі стандартизації підписів (EESSI).

У межах CEN для системи стандартизації інформаційного співтовариства (CEN/ISSS) Європейському інституту стандартизації телекомунікацій /Електронні підписи й інфраструктури (ETSI/ESI) доручено виконання програм з розробки загальновизнаних стандартів на підтримку реалізації [Dir. 1999/93/EC] і європейської інфраструктури електронного підпису.

Симпозіум CEN/ISSS з електронних підписів (WS/E-SIGN) започаткував ряд документів, угод CEN симпозіуму (CWA), які посприяли цим загальновизнаним стандартам. Цей документ — один із таких CWA.

CWA 14169 визначив загальну конфігурацію захисту критеріїв (PP) для безпечних пристроїв створення підпису (SSCD), назвавши [PP SSCD] у залишку цього документа. PP SSCD засновані на робочому припущенні про загальний нейтральний технологічний підхід, винятково заснований на вимогах, визначених відповідно до Директиви. Доки він враховує швидку й погоджену реалізацію Директиви незалежним від реалізації способом, побічний ефект — загальні

СТР SSCD не можуть підкреслити сили будь-якої конкретної технології, що здатна підтримати електронні підписи, не можуть оцінити використання СС SSCD в областях торгівлі (названі «5.2 підписи»).

Мета CWA 14355 полягає в тому, щоб розширити попередню роботу для визначення настанов для здійснення SSCDs у певних платформах (таких, як мікропроцесорні картки, ПК, кишенькові комп'ютери й мобільні телефони) і в певних середовищах (таких, як публічні термінали чи безпечні середовища).

Цей документ CWA призначено для використання юридичними й технічними експертами у сфері електронних підписів, так само як розробниками систем і продуктів у цій сфері.

Цю версію CWA опубліковано у квітні 2004 р.

Список осіб і організацій, які підтримують технічну угоду, наведено відповідно до цієї угоди CEN симпозіуму і доступний у центральному секретаріаті CEN.

НАЦІОНАЛЬНИЙ СТАНДАРТ УКРАЇНИ

НАСТАНОВИ ЩОДО РЕАЛІЗАЦІЇ БЕЗПЕЧНИХ ЗАСОБІВ СТВОРЕННЯ ПІДПИСІВ

РЕКОМЕНДАЦИИ ПО РЕАЛИЗАЦИИ БЕЗОПАСНЫХ СРЕДСТВ СОЗДАНИЯ ПОДПИСЕЙ

GUIDELINES FOR THE IMPLEMENTATION OF SECURE SIGNATURE-CREATIONDEVICES

Чинний від 2011–07–01

1 СФЕРА ЗАСТОСУВАННЯ

Директива 1999/93/ЕС Європарламенту й Ради від 13 грудня 1999 про суспільне середовище для електронних підписів [Dir.1999/93/EC], названа як «Директива» у передмові цього стандарту, визначає вимоги для безпечних засобів створення підписів SSCD у додатку III. CWA 14169 роз'яснює ці вимоги безпеки SSCD як профілі захисту, які випливають з умов Загальних критеріїв CC [PP SSCD]. Нейтральний технологічний підхід супроводжує ці PP.

Цей стандарт надає посібник із реалізації [PP SSCD] для певних платформ (наприклад старт-картки, персональні помічники даних, мобільні телефони чи ПК) й операцій у конкретних середовищах (наприклад публічні термінали чи безпечні середовища).

Документ призначено для продавців, що готуються записати мету безпеки (ST — Security Target), яка відповідає SSCD PP, і для користувачів, що мають потребу зрозуміти можливості різних технічних рішень для всебічного розуміння SSCD PP.

Ще одна мета цього стандарту полягає в порівняння [SSCD PP] з подібними PP або іншими поширеними стандартами оцінювання. Це має допомогти розробникам і авторам ST в ідентифікації шляхів розробки продуктів, які відповідають іншим стандартам на додаток до SSCD PP, і в такий спосіб допомогти уникнути подвійних процесів оцінювання.

Документ обмежує свою сферу застосування електронними підписами, заснованими на асиметричній криптографії, тобто цифровими підписами, заснованими на парі «особистий ключ — відкритий ключ».

2 ПОСИЛАННЯ

2.1 Нормативні посилання

Ця угода робочої групи CEN використовує датовані чи недатовані посилання й положення з інших публікацій. Ці нормативні посилання зацитовано у відповідних місцях у тексті, а публікації перелічено далі. Для датованих посилань пізніші зміни чи перегляди кожної із цих публікацій стосуються цієї угоди CEN тільки тоді, коли включені в цей стандарт відповідно до зміни чи перегляду. Для недатованих посилань застосовують найновіше видання публікації (включаючи зміни).

[ALGO] ETSI SR 002 176 Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures V1.1.1 (2003-03)

[CWA 14170] CWA 14170: Security Requirements for Signature Creation Applications

[CWA 14167-3] CWA 14167-3: Cryptographic Module for CSP Key Generation Services — Protection Profile (CMCKG-PP)

[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

[ISO 15408] ISO/IEC 15408-1 to 15408-3, 1999: 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

[SSCD PP] CWA 14169: Security Requirements of Secure Signature Creation Devices (SSCD).

НАЦІОНАЛЬНЕ ПОЯСНЕННЯ

[ALGO] ETSI SR 002 176 Електронні підписи й інфраструктури (ESI); Алгоритми й параметри для безпечних електронних підписів V1.1.1 (2003-03)

[CWA 14170] CWA 14170 Вимоги безпеки для застосувань створення підписів

[CWA 14167-3] CWA 14167-3: Криптографічний модуль для CSP служб генерації ключів. Профіль захисту (CMCKG-CTP)

[Dir.1999/93/ЕЄ] Директива 1999/93/ЕС Європарламенту й ради 13 Грудня 1999 про суспільне середовище електронних підписів

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

[PP SSCD] CWA 14169: Вимоги безпеки безпечних засобів створення підпису (SSCD).

2.2 Довідкова інформація

[CMCSO PP] CWA 14167-2: Cryptographic Module for CSP Signing Operations — Protection Profile, CMCSO-PP

[DFA] E. Biham, A. Shamir, Differential Fault Analysis of Secret Key Cryptosystems, Advances in Cryptology Proceedings of CRYPTO'97

[DPA] P. Kocher, J. Jae and B. Jun, Differential Power Analysis, Advances in Cryptology, Proceedings of CRYPTO'99, 1999, pp. 388-397

[FA] D. Boneh, R.A. Demillo, R.J. Lipton, On the importance of Checking Cryptographic Protocols for Faults, Advances in Cryptology, Proceedings of EUROCRYPT'97

[ISO 7816] ISO/IEC 7816: Identification cards — Integrated circuit cards with contacts

[PP 9806] French Certification Body PP/9806: Protection Profile Smart Card Integrated Circuit, Version 2.0, Eurosmart, September 1998

[PP 9911] French Certification Body PP/9911: Protection Profile Smart Card Integrated Circuit with Embedded Software, Version 2.0, Eurosmart, June 1999

[PP 0002] Bundesamt fur Sicherheit in der Informationstechnik BSI-PP-0002: Smartcard IC Platform Protection Profile, Version 1.0, Eurosmart, July 2001

[PP 0010] French Certification Body PP/0010: Protection Profile Smart Card IC with Multi-Application Secure Platform, Version 2.0, Eurosmart, November 2000

[SCSUG] Smart Card Security User Group: Smart Card Protection Profile, version 3.0, September 2001

[TA] P. Kocher, Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems, Advances in Cryptology, Proceedings of CRYPTO'96, pp. 104-113

[TAMPER] R.J. Anderson, M.G. Kuhn: Tamper Resistance — a Cautionary Note, Proceedings of Second USENIX Workshop on Electronic Commerce pp. 1-11, 1996

[TCPA] Trusted Computing Platform Alliance, Main Specification, version 1.1a, November 2001

[TPMPP] Trusted Platform Module Protection Profile (TCPA-TPMPP), version 1.0, December 2001

[TS 101456] ETSI SEC, Policy requirement for certification authorities issuing qualified certificates, Technical Specification ETSI TS 101456

[WAPWIM] WAP Identity Module, WAP-260-WIM, WAP Forum, Ltd.

НАЦІОНАЛЬНЕ ПОЯСНЕННЯ

[CMCSO PP] CWA 14167-2 Криптографічний модуль для операції підписування CSP. Профіль захисту, CMCSO— PP

[DFA] E. Biham, A. Shamir. Диференціальний аналіз помилок криптографічних систем секретного ключа. Просунуті напрямки криптології CRYPTO '97

[DPA] P. Kocher, J.Jae, B.Червень. Диференціальний аналіз споживаної потужності. Просунуті напрямки криптології CRYPTO '99, 1999, с. 388-397

[FA] D. Boneh, R.A. Demillo, R.J. Lipton. Важливість перевірки криптографічних протоколів на помилки. Просунуті напрямки криптології EUROCRYPT '97

[ISO 7816] ISO/IEC 7816 Посвідчення особи. Картки, засновані на інтегральних схемах із контактами

[PP 9806] Французький орган сертифікації PP/9806. Профіль захисту інтегральної схеми мікропроцесорної картки, Версія 2.0, Eurosmart, вересень 1998 р.

[PP 9911] Французький орган сертифікації PP/9911. Профіль захисту інтегральної схеми мікропроцесорної картки з убудованим програмним забезпеченням, Версія 2.0, Eurosmart, червень 1999 р.

[PP 0002] BSI-PP-0002 профіль захисту платформи IC мікропроцесорної картки, Версія 1.0, Eurosmart, липень 2001 р.

[PP 0010] Французький орган сертифікації CTP/0010. Профіль захисту мікропроцесорної картки IC із багатьма застосуваннями безпечної платформи, Версія 2.0, Eurosmart, листопад 2000 р.

[SCSUG] Група користувачів безпечної мікропроцесорної картки. Профіль захисту мікропроцесорної картки, Версія 3.0, вересень 2001 р.

[TA] P. Kocher. Тимчасові атаки на реалізації Diffie-Hellman, RSA, DSS й інших систем. Просунуті напрямки криптології CRYPTO '96, с. 104-113.

[TAMPER] R.J. Андерсон, M.G. Kuhn: Опір втручанню. Застережна примітка. Продовження другої робочої групи USENIX щодо електронної комерції. С. 1-11, 1996 р.

[TCPA] Надійний союз обчислювальних платформ, Основна специфікація, Версії 1.1a, листопад 2001 р.

[TPMPP] Надійний профіль захисту модуля платформи (TCPA-TPMPP), Версія 1.0, грудень 2001 р.

[TS 101456] ETSI SEC Вимога політики для органів сертифікації, які видають посилені сертифікати. Технічна специфікація ETSI TS 101456

[WAPWIM] WAP Модуль ідентичності, WAP-260-WIM, WAP Forum, Ltd.

3 ТЕРМІНИ ТА ВИЗНАЧЕННЯ ПОНЯТЬ, АБРЕВІАТУРИ

3.1 Терміни та визначення понять

кваліфікований підпис (*Qualified signature*)

Електронний підпис, що виконує вимоги, встановлені в Директиві в статті 5(1) [Dir.1999/93/EC], тобто посилений електронний підпис, заснований на посиленому сертифікаті й згенерований безпечним засобом створення підписів

SSCD типу 1 (*Type 1 SSCD*)

Засіб генерації SCD/SVD, відмінний від SSCD, використовуваного підписувачем. Може бути або оцінюваним засобом [SSCD PP, тип 1] проти [CWA 14167-3], або засобом, що виконує відповідні вимоги [Dir.1999/93/EC]

надійний канал (*Trusted channel*)

Канал комунікації, який може ініціювати будь-яка сторона каналу й забезпечує характеристики неспростовності щодо ідентичності сторін каналу [ISO 15408]

надійний шлях (*Trusted path*)

Шлях, який надає засіб користувачам для виконання функції через упевнену пряму взаємодію з TSF. Надійний шлях зазвичай бажаний для таких дій користувача як початкова ідентифікація

й/або автентифікація, але може також бути бажаний в інших випадках під час користувацького сеансу. Обміни, використовуючи надійний шлях, може ініціювати користувач або TSF. Користувацькі відповіді через надійний шлях мають гарантію захищеності від модифікації чи розкриття ненадійними застосуваннями [ISO 15408].

3.2 Абревіатури

APDU	Application Protocol Data Unit	Блок даних прикладного протокола
CAD	Card Acceptor Device	Пристрій прийняття картки
CBC	Cipher Block Chaining	Зчеплення блоків шифру
CC	Common Criteria Version 2.1	Загальні критерії, версія 2.1
CCS	Cryptographic Checksum	Криптографічна контрольна сума
CEN	Comite Europeen de Normalisation (European Committee for Standardization)	(Європейський комітет зі стандартизації)
CEN/ISSS	CEN Information Society Standardization System	Система стандартизації інформаційного суспільства CEN
CGA	Certification Generation Application	Застосування генерації сертифікатів
CSP	Certification Service Provider	Постачальник послуг сертифікації
CWA	CEN Workshop Agreement	Угода робочої групи CEN
DTBS	Data to be Signed	Дані на підпис
DTBSR	Data to be Signed Representation	Подання даних на підпис
DFA	Differential Fault Analysis	Диференціальний аналіз помилки
DPA	Differential Power Analysis	Диференціальний аналіз потужності
EAL	Evaluation Assurance Level	Гарантований рівень оцінювання
EC	European Commission	Європейська комісія
EESSI	European Electronic Signature Standardization Initiative	Європейська ініціатива стандартизації електронного підпису
EFP	Environment Failure Protection	Захист середовища від відмов
EFT	Environment Failure Testing	Тестування відмови середовища
ETSI	European Telecommunications Standards Institute	Європейський інститут стандартизації телекомунікацій
ETSI SEC	ETSI Security Technical Committee	Технічний комітет ETSI
HI	Human Interface	Інтерфейс користувача
HW	Hardware	Апаратні засоби
IC	Integrated Circuit	Інтегральна схема
I/O	Input/Output	Увід-вивід
ISSS	Information Society Standardisation System	Система стандартизації інформаційного суспільства
MAC	Message Authentication Code	Код автентифікації повідомлення
OS	Operating System	Операційна система
PC	Personal Computer	Персональний комп'ютер
PDA	Personal Digital Assistant	Персональний цифровий секретар
PIN	Personal Identification Number	Особистий ідентифікаційний номер
PP	Protection Profile	Профіль захисту
PUK	PIN Unblocking Key	Розблокування ключа PIN
RAD	Reference Authentication Data	Еталонні дані автентифікації
SCA	Signature-Creation Application	Застосування створення підписів

SCD	Signature-Creation Data	Дані створення підпису
SDO	Signed Data Object	Підписаний об'єкт даних
SDP	Signer's Document Presentation Component	Компонент подання документа підписувача
SFP	Security Function Policy	Політика функції безпеки
SFR	Security Functional Requirement	Функціональні вимоги безпеки
SIM	Subscriber Identification Module	Модуль ідентифікації підписувача
SOF	Strength of Function	Сила функції
SPA	Simple Power Analysis	Простий аналіз потужності
SSCD	Secure Signature-Creation Device	Безпечний засіб створення підписів
SVD	Signature-Verification Data	Дані верифікації підпису
S/WIM	SIM-based WIM	WIM, заснований на SIM
TOE	Target of Evaluation	Об'єкт оцінювання
VAD	Verification Authentication Data	Верифіковані дані автентифікації
WAP	Wireless Access Protocol	Протокол бездротового доступу
WIM	WAP Identity Module	Модуль ідентичності WAP
WS/E-SIGN	CEN/ISSS Electronic Signatures workshop	CEN/ISSS робоча група з електронних підписів

3.3 Прийняті в стандарті домовленості

Документ дотримується кількох угод для вказівки цитування, узятого з нормативної довідкової інформації, або виділення виразів, часто згадуваних усюди в тексті стандарту.

Цитати з нормативної довідкової інформації взяті в рамку, як показано в прикладі нижче.

Стаття 3 lit. 5 із Директиви 93/1999/EC

Комісія, відповідно до процедури, установленої в статті 9, може встановити й видати номера посилання загальновизнаних стандартів для продуктів електронного підпису в *офіційному журналі європейського співтовариства*. Держави-члени мають припустити погодженість із вимогами, встановленими в додатку II, пункт (f) і додатку III, коли електронний продукт підпису відповідає цим стандартам.

Щоб виділити положення, часто згадані у пронумерованих виразах документа, їх виділено напівгрубим шрифтом, як у наступному прикладі:

Положення 0. Кілька стандартів, які виконують вимоги, встановлені в додатку III, можуть бути опубліковані в *офіційному журналі європейського співтовариства.*

4 ПОВ'ЯЗАНІ З SSCD УМОВИ ДИРЕКТИВИ

Мета [SSCD PP] — реалізувати умови додатка III Директиви [Dir.1999/93/EC] як загальні критерії PP, тобто в нейтральний до технології спосіб, що покриває вимоги безпеки, але залишає ринку можливість реалізувати SSCD у множині технологій. Оскільки додаток III не можна розглядати відокремлено від Директиви загалом, цей розділ обумовлює частково спірні припущення й інтерпретації Директиви, на якій [SSCD PP] засновано.

4.1 Релевантні визначення понять

Стаття 2 Директиви 93/1999/EC

1. 'електронний підпис' означає дані в електронній формі, які приєднані або логічно пов'язані з іншими електронними даними й служать методом автентифікації;

2. 'розширений електронний підпис' означає електронний підпис, що відповідає наступним вимогам:

(a) він унікально пов'язаний із підписувачем;

(b) він здатний до ідентифікації підписувача;

(c) він створений із використанням засобів, які підписувач може підтримувати під своїм одноосібним керуванням;

(d) він пов'язаний із даними, яких стосується так, що будь-яку наступну зміну даних буде виявлено.

Для цього стандарту тільки розширені підписи мають значимість, оскільки Директива стосується SSCD і додатка III тільки в контексті розширених підписів. Це далі зазначено в **4**.2 щодо докладного опису (15) з Директиви.

Положення 1. Для розширених підписів підписувач має бути здатний підтримати використання SCD під своїм керуванням. Це не має на увазі вимогу перешкоджання тому, щоб підписувач відмовився від такого керування, і прив'язку SCD до біометричних характеристик підписувача.

Основна умова, наведена у визначенні розширених підписів вище й неодноразово згадувана далі в цьому стандарті, полягає в тому, що розширені підписи створені засобами, які підписувач може підтримати під своїм одноосібним керуванням. По суті це означає, що:

(a) жодний об'єкт, крім підписувача, не може одержати засоби створення такого розширеного електронного підпису;

(b) проте підписувач може відмовитися від одноосібного керування.

Хоча умова (b) здається нечітким тлумаченням того, що електронні підписи за визначенням служать методом автентифікації, важливо підкреслити, що тут просто немає обов'язкових технічних засобів, які зазначені в Директиві й перешкоджали б відмові підписувача від керування. Тому вимогу включення біометричних характеристик неможливо заперечити за визначенням розширених електронних підписів. Для ідентифікації таким знанням, як увід особистого ідентифікаційного коду (PIN), SSCD не може зробити фактично нічого, щоб перешкодити тому, що підписувач передав код іншим.

Стаття 2 Директиви 93/1999/ЕС

3. 'підписувач' має на увазі людину, що тримає засіб створення підписів і діє або від власного імені, або від імені фізичної чи юридичної особи, чи об'єкта, який він представляє;

4. 'дані створення підпису' означають такі унікальні дані, як коди або особисті криптографічні ключі, використовувані підписувачем для створення електронного підпису;

5. 'засіб створення підписів' — це сконфігуровані засоби програмного забезпечення або апаратні засоби, які зазвичай реалізують дані створення підписів;

Положення 2. Реалізація SCD включає генерацію, зберігання, використання й знищення SCD, навіть якщо під час генерації SCD підписувач невідомий.

Відносини між підписувачем і електронним підписом визначено через засіб, що реалізує дані створення підпису (SCD). У контексті цього стандарту вимогу 'реалізувати' інтерпретують як будь-яку взаємодію з SCD усюди під час його життєвого циклу, незалежно від того, чи існує в певний момент часу відповідний сертифікат, чи ні. Отже, це покриває створення SCD, його зберігання, використання й знищення. Таким чином, для таких процесів, як попередня персоналізація смарт-карток застосовують додаток III, навіть якщо підписувач ще невідомий. Основний аргумент цієї інтерпретації полягає в тому, що інакше порушено й визначення розширеного підпису, й умови додатка III. Імовірно, SCD використовувався колись без одноосібного керування підписувача, і тому без підписувача, здатного захистити SCD від такого використання.

4.2 Загальні умови як докладні описи

Докладний опис (15) із Директиви 93/1999/ЕС

Додаток III покриває вимоги для безпечних засобів створення підписів із гарантією функціональності розширених електронних підписів; він не покриває все системне середовище, у якому працюють такі засоби; функціонування внутрішнього ринку вимагає, щоб Єврокомісія й держави-члени стрімко діяли, щоб призначити органи оцінювання відповідності безпечних засобів підпису згідно з Додатком III; щоб задовольнити ринкові потреби, оцінювання відповідності має бути своєчасним і ефективним;

Основний аспект докладного опису (15) впливу [SSCD PP] — область застосування додатка III і, виходить, обмежена SSCD область застосування обов'язкового оцінювання відповідності, виконаного певними органами. Як пояснено пізніше, SSCD — переважно засіб, якому дозволено 'стосуватися' SCD. У контексті цього документа SCD — особистий криптографічний ключ, а 'стосування' цього особистого ключа може відбутися під час створення, зберігання, використання й знищення.

У термінах [ISO 15408] це означає, що об'єкт оцінювання TOE є SSCD, тобто знову засіб 'стосування' SCD. Хоча реалізатор може вирішити включати такі додаткові елементи, як елементи відображення, елементи уводу-виводу або генерацію документа в процесі оцінювання, щоб збільшити впевненість у продукті його клієнтів, це не вимога, яку можна одержати з Директиви. Границя між TOE і його безпосереднім середовищем, тобто інтерфейсом між ними, є однією з основних проблем, до яких звернено ці настанови й далі обговорюється всюди в цьому стандарті.

Докладний опис (18) із Директиви 93/1999/EC

Зберігання й копіювання даних створення підпису може викликати загрозу юридичної валідності електронних підписів.

Положення 3. SCD не можна скопіювати або умовно депонувати. Для кваліфікованих підписів жодні дублікати SCD не можуть існувати навіть за згодою підписувача. Якщо SCD передано, то початкову копію треба надійно знищити.

Виникають дві основні загрози, якщо допустити дублікати SCD. По-перше, електронні підписи можна створити без згоди ідентичності, завіреної відповідним сертифікатом. Це наражає на небезпеку властивість автентифікації, націленої на електронні підписи взагалі. По-друге, властивість неспростовності, яку можна одержати з електронних підписів, перебуває під загрозою, якщо підписувач може стверджувати, що є практична можливість існування копії SCD. Таким чином, незалежно від того, чи створено такі дублікати SCD із або без згоди, або знання підписувача, інтереси й підписувача, і залежної сторони були б піддані небезпеці таким подвійним SCD.

Докладний опис (18) стосується електронних підписів взагалі, не тільки SCD, збереженому в SSCD. Для SSCD дублікати SCD явно виключено згідно з умовами, наведеними в додатку III.

4.3 Технічні аспекти умов, наведених у додатку III

Додаток III Директиви 93/1999/EC

1. Безпечні засоби створення підписів як відповідні технічні й процедурні засоби мають гарантувати принаймні, що:

(а) дані створення підписів, використовувані для генерації підписів, можуть фактично відбутися тільки один раз і їхню таємницю розумно забезпечено.

Положення 5. Генерацію SCD має бути засновано на ймовірнісних процесах, які зберігають імовірність дубліката SCD якомога меншою. Засоби довести одиничність SCD не потрібні.

У додатка III 1(а) є кілька впливів на технічну реалізацію SSCD:

— SCD має залишитися секретним, а SSCD гарантувати секрет технічними засобами;

— не може бути жодних засобів обійти забезпечення секрету, необхідне відповідно до Директиви, навіть за згоди законного підписувача;

— доказ унікальності SCD не потрібен, якщо порівняння SCD:

- вимагає знання SCD, що порушило б умову секрету SCD,
- із іншими SVD (які вказали б дублікати SCD) усе ще тільки буде можливо в межах домена провайдеру SSCD.

Технічний наслідок 1(а) додатка III полягає в тому, що SCD має бути засновано на ймовірнісному процесі з достатньою якістю гарантії, що не існують жодні дублікати SCD, тобто процес має достатню ентропію. Рішення, чи правочинний певний процес генерації SCD, лежить поза областю [SSCD PP], а правочинність процесів генерації ключа визначено в [ALGO]. Оцінювання SSCD забезпечує гарантію, що процеси відповідно реалізовано.

Подальші наслідки для реалізаторів SSCD, які випливають із 1(a) додатка III, — захист секрету SCD необхідно робити *технічними й процедурними* засобами. Як зазначено раніше в положенні 2, послугу генерації SCD потрібно розглядати як частину SSCD, навіть якщо підписувач ще не відомий. Генерація SCD у провайдера послуг сертифікації (CSP), де секрет SCD винятково засновано на процедурних засобах, наприклад, порушило б 1(a) додатка III, оскільки технічний засіб також треба використовувати в межах служби генерації SCD для захисту SCD.

Додаток III Директиви 93/1999/EC

1. Безпечні засоби створення підписів, що відповідають технічним і процедурним засобами, мають гарантувати принаймні, що:

(b) для генерації підписів неможливо одержати з розумною гарантією, а підпис захищено від підробки, яка використовує на цей час доступну технологію.

Положення 6. Необхідний сильний захист, щоб гарантувати секрет SCD.

Положення 7. Сильна криптографія має запобігати підробці електронних підписів.

Положення 8. Для довгострокової валідності, на додаток до положення 7, не обов'язкові для SSCDs жодні заходи, наприклад часові штемпелі чи перепідписування.

Технічні ефекти, які можна одержати з додатка III 1(b):

— жодні засоби одержання SCD не мають бути виконані:
- від реалізації SCD (яка за визначенням є SSCD),
- від процесу генерації підписів безпосередньо,
- із криптографічних протоколів,
- будь-якими іншими засобами

— захист від підробки підписів вимагає відповідної криптографічної сили.

Крім того, підробку підписів явно звернено до доступної на цей час технології. Заходи не виключають того, що підпис можна підробити, використовуючи майбутню технологію. Як наслідок, неможливо одержати жодні додаткові обов'язкові, технічні або процедурні вимоги до SSCD щодо довгострокової валідності електронних підписів.

Оцінка, чи має певний набір програм підписання право запобігти підробці у теоретичній перспективі, лежить поза областю [SSCD PP] і визначено в [ALGO]. Це — реалізація набору програм, які покриває PP.

Додаток III Директиви 93/1999/EC

1. Безпечні засоби створення підписів з відповідними технічними й процедурними засобами мають гарантувати принаймні, що:

(c) дані створення підписів, використовувані для генерації підписів, може надійно захистити законний підписувач від використання іншими.

Визначення розширених електронних підписів включає це, оскільки засоби створення такого підпису можуть перебувати під одноосібним контролем підписувача. Додаток III 1(c) удосконалює цю вимогу в тому, що SSCD має забезпечити засіб, яким підписувач може захистити використання SCD. Технічні наслідки:

— для використання SCD SSCD має бути здатним розрізнити підписувача й інших, тобто має бути засіб ідентифікувати законного підписувача;

— «захищений» указує, що підписувач може відігравати активну роль у цьому захисті, наприклад, активно вибираючи дані, використовувані для ідентифікації знанням;

— для ідентифікації знанням такий секрет, як PIN-код, не є відгадуваним. Тому SSCD має забезпечити технічні засоби для визначення заданої якості, щоб досягти надійного захисту. Приклад настанови визначено для банківських стандартів на касові апарати.

Додаток III Директиви 93/1999/EC

2. Безпечні засоби створення підписів не можуть змінювати дані, які будуть підписані, або перешкоджати тому, щоб такі дані надавали підписувачу до процесу підписання.

Положення 9. Підписувач може вирішувати, чи переглядати "дані, які будуть підписані".

Додаток III 2 гарантує, що підписувач здатний переглянути дані, які будуть підписані, до підписання їх і гарантує, що ці дані не змінив SSCD. Немає жодної отриманої вимоги, щоб SSCD гарантував, що подання DTBS фактично мало місце. В SSCD може, наприклад, бути опція, що підписувач може створити серію підписів для різних DTBS, не переглядаючи їх, також підписувач може переглядати кожний DTBS. З іншого боку, якщо певна реалізація представляє кожний DTBS тому, хто підписався без підписувача, здатного знищити подання, це — також валідний підхід відповідно до додатка III 2.

4.4 Пов'язані з SSCD заходи щодо посилених сертифікатів і CSP

Додаток I Директиви 93/1999/EC

Посилені сертифікати мають містити:

(e) дані верифікації підпису, які відповідають даним створення підпису під керуванням підписувача;

Положення 10. SSCD має бути здатним допомогти в доказі відповідності між SVD і SCD.

Збережений у сертифікаті SVD має відповідати SCD підписувача, використаного для підписання. Тому SSCD має допомогти застосуванню генерації сертифіката (CGA) у доказі цієї відповідності. Важливо, що такий доказ володіння зазвичай вимагає використання SCD і, можливо, не зіштовхується з іншими положеннями Директиви. Наприклад, підхід до підписання випадкових викликів несе загрозу й має виключатись, оскільки в підписувача немає фактично жодного шансу розрізнити цю ситуацію, що був такий випадковий виклик, а підписувач фактично не мав наміру підписатися значенням геш-функції документа. Тому доказ відповідності між SCD і SVD необхідно розглянути окремо від використання SCD для підписання. Наприклад, RFC 2511 вимагає для доказу володіння, що SVD можна використовувати тільки, щоб підписати SVD або заснований на паролі MAC SVD. Це не запобігає ризику шахрайства.

Додаток II Директиви 93/1999/EC

Провайдер послуг сертифікації має:

(g) вжити заходів проти підробки сертифікатів і у випадках, коли провайдер послуг сертифікації генерує дані створення підписів, гарантувати конфіденційність під час процесу генерації таких даних;

(j) не зберігати або копіювати дані створення підписів особи, якій провайдер послуг сертифікації надавав послуги керування ключами.

Наведені вище заходи, хоча безпосередньо не пов'язані з додатком III, підтримують положення 4, що SCD має залишитися секретним. Доказ відповідності між SCD і SVD надано використанням SSCD, коли обговорено вище положення 10.

5 ПОЯСНЕНІ ЗМІНИ ДО CWA 14169

У цьому розділі пояснено [SSCD PP]. По-перше, наведено загальні настанови з реалізації, пояснені щодо [SSCD PP] у 5.1. Детальне обговорення головних проблем, які мають покрити реалізатори, наведено в 5.2.

5.1 Загальні настанови з реалізації

У цьому розділі наведено короткий огляд [SSCD PP] нейтральним безпосередньо до технології чином [SSCD PP]. Це зроблено з двох причин:

— це має зберегти документ модульним, хоча через тісні зв'язки його неможливо розглянути окремо від [SSCD PP];

— короткий огляд дає розширення описових частин [SSCD PP] і цим допомагає конструкторам в одержанні початкового розуміння, як SSCD-вимоги перевели в Загальні критерії [ISO 15408] розробники [SSCD PP].

Тому підрозділ так структуровано. У 5.1.1 наведено подання високого рівня для процесу створення підписів. Наведено короткий огляд залучених компонентів і інтерфейсів. Різні типи SSCD обговорено в 5.1.2, а в 5.1.3 продовжено обговорення розмежування для поділу між TOE та його середовищем.

5.1.1 *Короткий огляд SSCD*

Рисунок 1

Процес створення підписів, що використовує SSCD, спрощено опишемо так:

— генерація пари SCD-SVD (ключів) і відповідного сертифіката, створеного на фазі ініціалізації. Це проілюстровано внизу праворуч на рисунку 1;

— на фазі використання DTBS має вигляд підписаного підписувачем документа. На підтримку одноосібного контролю над властивостями треба використати автентифікацію підписувача, наприклад, уводячи PIN-код.

Навіть на цьому поверхневому рисунку, що поки нехтує різними опціями реалізації SSCD, можна ідентифікувати кілька основних загроз:

— SCD — це первинне майно, захищене (конфіденційне) під час ініціалізації й використання, оскільки атакувальник, одержавши керування над SCD, може створити будь-яке число підписів без згоди підписувача;

— дані автентифікації — первинний актив, оскільки атакувальник, заволодівши SSCD і даними автентифікації, може створити підписи, які виконують роль законного підписувача;

— дані, повідомлені під час ініціалізації, мають бути захищені для перешкоджання одержання атакувальником сертифіката, який ідентифікує підписувача, але містить SVD атакувальника;

— дані, повідомлені на фазі використання, мають бути захищені для перешкоджання розкриття PIN-коду атакувальником або заміни на DTBSR дані, обрані атакувальником.

5.1.2 *Типи SSCD*

Під час розробки [SSCD PP] розходження зроблено залежно від двох основних альтернатив на фазі ініціалізації (генерації ключів):

— пари SCD-SVD можна згенерувати в SSCD, що використовує підписувач для підписування,

— використовують спеціалізований засіб генерації пари SCD/SVD, що передає SCD в SSCD, застосовуване для підписання.

Це призвело до трьох основних типів SSCD, для яких загальні аспекти реалізації обговорено в наступних підрозділах:

- SSCD типу 1 — генерація пари SCD/SVD,
- SSCD типу 2 — створення підписів,
- SSCD типу 3 — генерація пари SCD/SVD і створення підписів.

5.1.2.1 *SSCD типу 1*

Генерація криптографічних ключів — критичний фактор якості криптопродуктів. Однак для цифрових підписів, що використовують криптографію з асиметричними ключами, генерація ключів може бути ресурсномістким процесом із кількох причин:

— генерація ключів і тестування їхньої сили зазвичай витратно в обчислювальному відношенні;

— вимога для достатньої ентропії (див. положення 5) вимагає таких якісних фізичних генераторів випадкових чисел, як якісні джерела шуму.

Системні проектувальники можуть використовувати спеціалізовані засоби генерації пари SCD-SVD, які спеціально спроектовано для витратного процесу генерації ключів і рятують від потреби включати такі функціональні блоки в засіб для створення підписів, який може бути засобом масового виробництва.

Щодо положення 2 засіб генерації SCD, можливо, є SSCD. Тоді в термінах [SSCD PP] SSCD має тип 1. Його основні функціональні блоки проілюстровано на рисунку 2:

— генерація SCD/SVD;

— SCD експорт підписувача у засіб створення підписів, названий SSCD типу 2 у термінах [SSCD PP];

— SVD експорт або безпосередньо в CGA для генерації сертифіката, або в SSCD типу 2, що зв'язує SVD із CGA на пізнішій стадії.

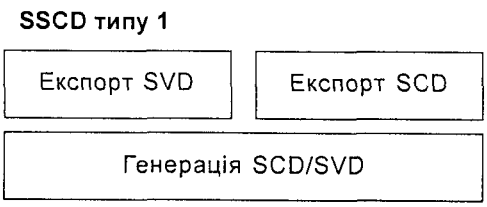


Рисунок 2

5.1.2.2 *SSCD типу 2*

Копія SSCD типу 1 є SSCD типу 2, що є особистим засобом, використовуваним підписувачем для створення підписів. Це індивідуальний засіб, і його основні функціональні блоки проілюстровано на рисунку 3:

— персоналізація як процес застосування конкретних, пов'язаних з підписувачем даних, включаючи:

• такі еталонні дані автентифікації RAD, як особистий PIN-код і PIN-код розблокування ключа (PUK);

• SCD, імпортований із SSCD типу 1;

• SVD відповідний SCD, імпортованому з SSCD типу 1. Зазначимо, що це — опціональна властивість, оскільки SVD не обов'язково міститься в SSCD;

— створення підписів;

— автентифікація користувача, що гарантує забезпечення підписувачеві одноосібного контролю над функцією створення підпису.

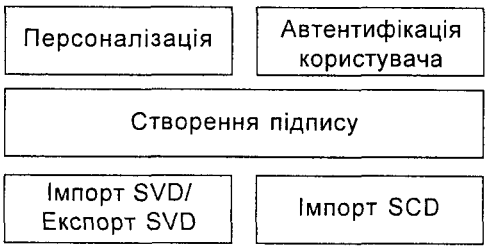


Рисунок 3

5.1.2.3 *SSCD типу 3*

Якщо пару SCD/SVD згенеровано «у межах» SSCD, використовуваного підписувачем для підписування, то результуючим засобом у термінах [SSCD PP] є SSCD типу 3. SSCD типу 3 є повністю виокремлений засіб, який можна розглядати як комбінацію SSCD типу 1 і типу 2.

Основна очевидна розбіжність полягає у тому, що SCD не можна передати за межі SSCD, як показано на рисунку 4. Основні «будівельні» блоки SSCD типу 3:

— генерація SCD/SVD;

— SVD експорт в CGA для генерації сертифіката, а SCD залишається в SSCD;

— персоналізація як процес застосування таких пов'язаних із підписувачем даних, як RAD;

— створення підписів;

— автентифікація користувача, яка гарантує підписувачеві одноосібний контроль над функцією створення підписів.

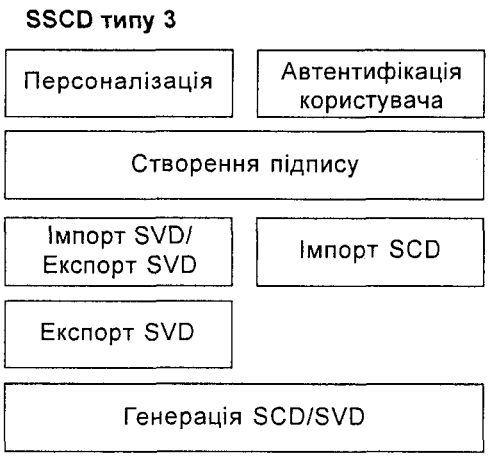


Рисунок 4

5.1.3 ***TOE проти TOE IT-середовища***

З огляду на три різні типи SSCD, описаних вище, три різних PP розроблено в [SSCD PP] — по одному для кожного типу SSCD. Конструктори й автори ST повинні вибрати конкретний PP для відповідності. У цьому розділі обговорено обмеження TOE.

[SSCD PP] одержали компоненти, які є необхідними частинами TOE згідно з додатком III Директиви. Конструктор має право інтегрувати в TOE такі інші компоненти, як засіб перегляду документів, що однак лежить поза описом цього загального розділу, але далі обговорено в цьому стандарті.

Розбіжність між TOE і його середовищем залежить від типу SSCD. Тому далі обговорено це розходження для SSCD типу 1 і SSCD типу 2. Наступний розділ обумовлює межі TOE, загальні для всіх типів SSCD.

5.1.3.1 *SSCD типу 1 і SSCD типу 2*

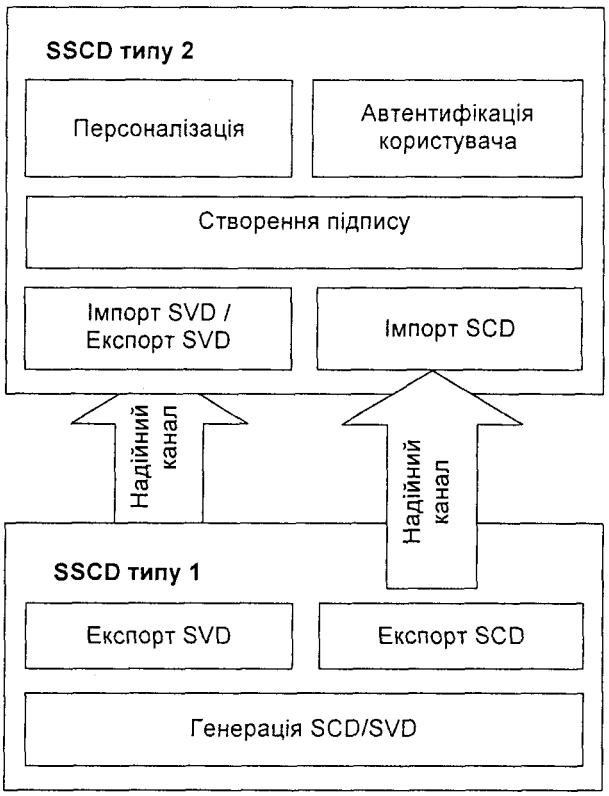


Рисунок 5

Щодо розбіжності між TOE та його середовищем, вочевидь, є взаємозв'язок між SSCD типу 1 і SSCD типу 2.

— У разі SSCD типу 1 TOE експортує SCD у SSCD типу 2, тобто SSCD типу 2 є IT-середовищем TOE. Це стосується SVD, коли SVD передається від TOE в SSCD типу 2.

— З іншого боку, у разі SSCD типу 2, SCD імпортується з SSCD типу 1. Отже, SSCD типу 1 є IT-середовищем TOE. Те саме стосується SVD, коли SVD передається від TOE в SSCD.

Обговорений сценарій проілюстровано на рисунку 5. Щоб виконати вимогу таємності SCD, так званий «надійний канал» визначено в [SSCD PP] між SSCD типу 1 і SSCD типу 2. Мета надійного каналу полягає в тому, щоб підтримати конфіденційність SCD і цілісність SCD протягом передачі. Для опціональної передачі SVD визначено надійний канал, що має підтримати цілісність SVD. Надійні канали обговорено далі в 5.2.1.

Зазначимо, що за визначенням у 3.1 SSCD типу 1 є не обов'язково оцінюваним [SSCD PP] засобом, оскільки можна використовувати інші засоби, які відповідають [Dir.1999/93/EC].

5.1.3.2 *SSCD усіх типів*

Вважаючи, що SSCD типу 3 може бути комбінацією SSCD типу 1 і SSCD типу 2, розбіжність між TOE як конкретний тип SSCD і його середовище проілюстровано на рисунку 6. Зазначимо, що, вочевидь, немає прямого інтерфейсу до SCA і HI для SSCD типу 1. З іншого боку, інтерфейс між SSCD типу 2 і CGA потрібен тільки для випадків, коли SSCD типу 2 містить SVD й експортує його для генерації сертифіката.

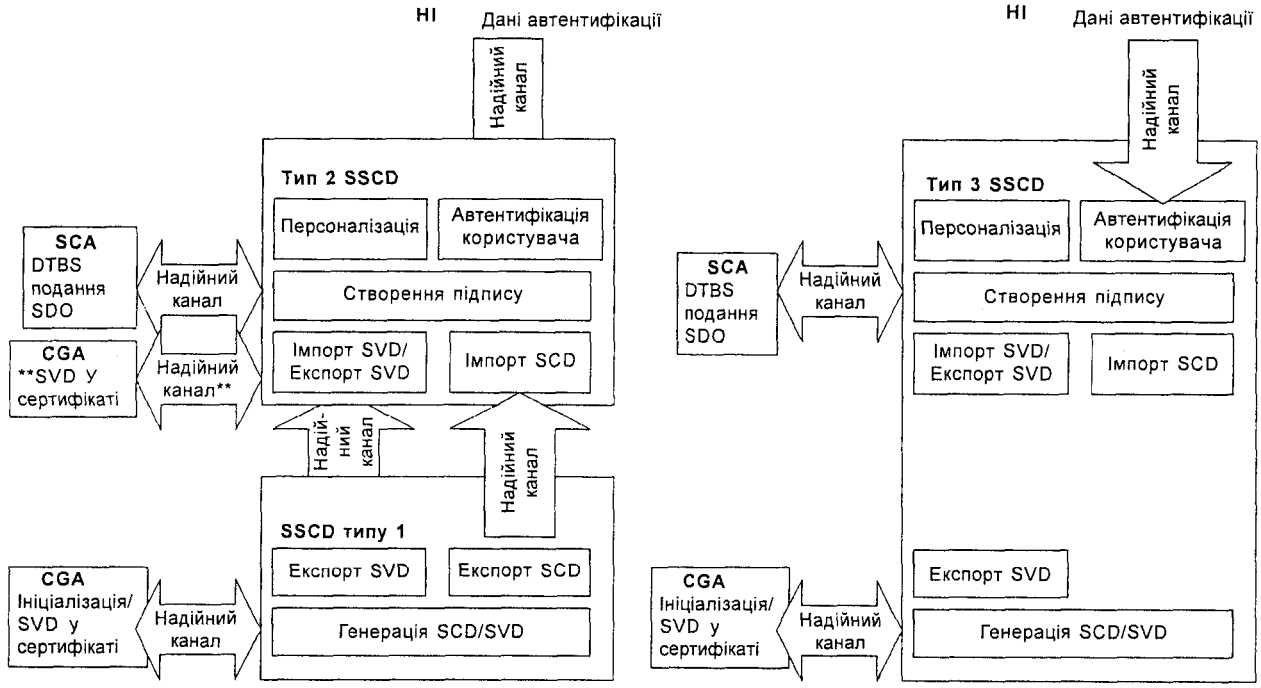


Рисунок 6

На додаток до взаємозв'язку між SSCD типу 1 і SSCD типу 2, TOE спілкується з багатьма застосуваннями, які становлять IT-середовище TOE:

— SVD переданий від SSCD в CGA для генерації сертифіката. Тому надійний канал визначено в [SSCD PP] на підтримку цілісності SVD;

— DTBSR переданий від SCA в SSCD для створення підпису. Тому надійний канал визначено на підтримку цілісності DTBSR;

— технічні засоби для створення можливості підписувачу ініціювати створення підпису під його одноосібним контролем надала автентифікація користувача. Тому так званий «надійний шлях» до інтерфейсу користувача (HI) визначено в [SSCD PP]. Під час розробки [SSCD PP] створені засоби, які інтегрують HI в TOE, тому не потрібен надійний шлях у цій ситуації.

5.2 Настанови з питань, цікавих для конструкторів

У цьому розділі обговорено аспекти, які конструктори вважають особливо цікавими. Ці аспекти викликають підвищену увагу до результатів, які неодноразово цікавили конструкторів чи були джерелом інтенсивного інтересу впродовж розробки SSCD PP.

5.2.1 *Надійний канал (FTP_ITC) між TSF і надійний шлях (FTP_TRP)*

5.2.1.1 *Аргументація для вибору*

SSCD повідомляє такі уразливі дані іншому IT-продукту, як SCD або VAD, переданий між SSCD типу 1 і SSCD типу 2 або користувачами. Тому визначено надійні канали FTP_ITC і надійні шляхи FTP_TRP. Ці надійні канали/шляхи для TOE:

— Експорт FTP_ITC/SCD (SSCD типу 1) й імпорт FTP_ITC/SCD (SSCD типу 2). SCD передано між SSCD типу 1 і SSCD типу 2. Відносно Додатка III 1(a), відповідно до 'положення 4', SSCD має гарантувати секрет SCD.

— Експорт FTP_ITC/SVD, передача SVD (SSCD типів 1,2 і 3). Цілісність SVD має бути захищена протягом передачі CGA для сертифікації.

— Імпорт FTP_ITC/DTBS (SSCD типу 2 і 3). SSCD має запобігти зміні DTBS. DTBS-подання протягом передачі між SCA і SSCD має захистити надійний канал.

— FTP_TRP/TOE, SCA. Для автентифікації підписувача інтерфейс вимагає користувача (HI), наприклад, для вводу PIN-коду. Якщо цьому HI не надають SSCD, уразливі дані (VAD) треба захистити.

5.2.1.2 *Приклади реалізації*

Безпечний обмін повідомленнями, як визначено для смарт-карток в [ISO 7816] частині 4 і в частині 8 для розширених функцій, надає одну опцію для реалізації надійного каналу. Це допускає безпечну передачу пакетів даних протоколу прикладного рівня (APDU) між терміналом і смарт-карткою. Два режими надають потенційних кандидатів, щоб використовувати з SSCD:

— режим authentic. Криптографічна контрольна сума CCS обчислена по APDU, наприклад, ключовий код автентифікації повідомлення MAC або MAC, заснований на симетричному блоковому шифрі в режимі експлуатації ланцюжків блокових шифрів CBC. Це забезпечує цілісність переданих даних, але не забезпечує конфіденційність даних;

— режим combined. У цьому режимі APDU, захищений у режимі Authentic, доповнено і зашифровано. Це забезпечує й цілісність даних, і конфіденційність даних.

Режим combined відповідає вимогам передачі SCD. Для передачі SVD або DTBS-подання, що не несе секретних даних, можна використовувати режими authentic і combined.

Смарт-картки зазвичай використовують симетричні алгоритми, щоб здійснити безпечний обмін повідомленнями, можливі ще й асиметричні алгоритми. Проте у разі потреби криптографічних ключів з'являється проблема захисту цих ключів. У той час як захист ключів, використовуваних для безпечного обміну повідомленнями, не проблематичний для SSCD, оскільки реалізація захисних мір потрібна для SCD щоразу, зберігання криптографічних ключів у середовищі SSCD необхідно розглядати інакше, оскільки розкриття цих ключів критично.

Залежно від фактичної реалізації, обговореної докладно в розділі 7, досягнуто бажану перевагу, якщо SSCD підтверджує справжність середовища, наприклад, безпечного термінала смарт-картки, верифікованим підписувачем способом, і перш ніж буде передано такі уразливі дані, як VAD підписувача (наприклад, PIN-код).

Приклад автентифікації середовища, реалізованої смарт-картками, показує, що секрет, обраний підписувачем, зберігається в SSCD. Тільки після того, як термінал успішно автентифіковано, цей секрет демонструється й відображається підписувачу. За умови, що термінал безпосередньо захищає ці дані автентифікації, щоб уникнути атак на термінал, який передає секрет атакувальнику, підписувач, упевнений у надійності термінала, й може продовжити підписання.

Приклади, наведені вище для надійного шляху/каналу, близько пов'язані, щоб забезпечити обмін повідомленнями, здійснюваний у багатьох старт-картках і засобах прийому карток. Для таких стандартних продуктів, як ПК, досяжні методи, подібні до режимів authentic або combined. Однак такі засоби ще не характерні для ПК. Реалізуючи подібні методи на підтримку безпечного обміну повідомленнями, потрібно розглянути зберігання криптографічних ключів. Розробка в цій області, що може допомогти в здійсненні необхідних функцій, є надійним модулем платформи [TPMPP], розробленої для альянсу надійної обчислювальної платформи [TCPA].

5.2.2 *ТОЕ випромінювання (FPT_EMSEC)*

5.2.2.1 *Аргументація для вибору*

Головні активи, які тримають у секреті SSCD, — це SCD і RAD. Обмеження захисту такими фізичними засобами, як FPT_PHP, уважають недостатнім через такі складні атаки, як аналіз споживаної потужності або часові атаки. Щоб протистояти цим атакам, визначено сімейство FPT_EMSEC для гарантії, що ані ТОЕ не видає інформацію, яка стосується SCD або RAD, ані інтерфейси не можна використовувати для одержання доступу до цих активів.

[SSCD PP]

FPT_EMSEC.1.1 ТОЕ не має видавати [*присвоювання: типи емісії*] понад [*присвоювання: зазначені межі*] наданих прав доступу до RAD і SCD.

FPT_EMSEC.1.2 TSF має гарантувати [*присвоювання: тип користувачів*], що не може використовувати наступний інтерфейс [*присвоювання: тип підключення*], щоб одержати доступ до RAD і SCD

Далі у розділах виділено атаки, які мають врахувати конструктори. Оскільки фактична загроза й контрзаходи суттєво залежать від використаної технології, далі наведено лише загальні твердження, а контрзаходи докладно обговорено в розділах 8—11.

5.2.2.2 *Логічні атаки*

FPT_EMSEC.1.2 приймає логічні атаки через 'звичайні' інтерфейси, які забезпечує SSCD, наприклад, експлуатувати уразливість через канали комунікації, по яких, зазвичай, передаються DTBS-подання (DTBSR), підписаний об'єкт даних (SDO) або VAD.

5.2.2.3 *Витік через випромінювання*

Видача, передбачена для FPT_EMSEC.1.1, є електромагнітним випромінюванням як прямим впливом обробки критичних даних або частин критичних даних. Джерела такого випромінювання може викликати IC через антени або шини, що перебувають у мікросхемі, чи взаємодія критичних елементів між компонентами, установленими на друкованій платі (PCB).

Особливу увагу слід звернути на операції з виконання SCD або RAD, навіть не на безпосередню передачу за рамки компонента, оскільки будь-яке випромінювання може пропустити інформацію. Приклади контрзаходів — екранування, маскування шин, також назване осліпленням або кодуванням даних на шляху.

5.2.2.4 *Витік під час криптографічних операцій, атаки потужності*

Цей клас атак засновано на інформації, що атакувальник збирає на фазах, коли під час атаки компонент виконує криптографічні операції. Атака заснована на витоку інформації через вторинні канали, за якими спостерігають, і які тому іноді згадують як побічні канали. Прикладом такого каналу, що фактично є джерелом кількох уразливостей, є споживана потужність компонентів. Джерело живлення потрібно розглядати як інтерфейс, покритий FPT_EMSEC.1.2, потенційно пропускаючий інформацію.

Атаки потужності засновані на розходженнях у споживаній потужності, зберігаючи '0'-біт у порівнянні з '1'-бітами, тобто перехід від зростаючого краю в порівнянні з переходом на край падіння відповідно.

Приклад такої атаки заснований на прямому контролі розходжень споживаної потужності у виконанні операції, що залежать від ключів. Це згадують як простий аналіз споживаної потужності (SPA — simple power analysis). Наслідок — жодний прямий вплив операцій на SCD не можна виявляти в інтерфейсах.

Диференціальний аналіз споживаної потужності [DPA] є складнішою атакою, що ділить прогресію вимірів у дискретну прогресію, кожний елемент якої розглядають як статистичну функцію розподілу. Обчислюючи розходження прогресії таких розподілів, DPA набуває значного зиску порівняно з SPA від ефекту, що статистичний огляд призводить до нейтралізації ефектів, не потрібних атакувальнику. Атака особливо серйозна як збільшення перекручування, виробленого засобом, їй можна протистояти, збільшуючи число тестових повідомлень, щоб досягти статистичної значимості ефекту, який піддають моніторингу. Наслідок атаки — жодні непрямі впливи, наприклад, статистично значимі ефекти, не можна виявляти.

У подальшому атаки можуть ґрунтуватись на факті, що криптографічні системи можуть вимагати різного часу, щоб обробити різні вводи. Такі часові атаки на криптографічні системи відкритого ключа уведені [TA]. Тому не має відбутися жодна виявлена різниця у синхронізації подій. Це запобігає SCD-залежні операції (RAD-DEPENDENT) із часом виконання, різними щодо витоку інформації відносно SCD (RAD).

5.2.2.5 *Вставка помилок, аналіз помилок*

В атаці апаратного збою [TAMPER] виконання інструкції навмисно збійне. Мета полягає в тому, щоб замінити впорядковане виконання інструкцій довільним.

Криптографічні операції, які створюють апаратні проблеми, можна зробити розв'язними, якщо обробку виконано на навмисно ушкоджених даних. Криптоаналіз можна виконати, вставляючи помилки, начебто втручаючись у середовище компонента. Такий аналіз помилки в криптографічних системах відкритих ключів уведено [FA]. Просування атак помилки дає диференціальний аналіз помилки [DFA]. Загальне правило уникнути таких атак — не робити, передавати або обробляти невдалий результат.

Вставка помилок може випливати зі зміни таких умов навколишнього середовища, як температура, напруга, або таких складних атак, як розкриття компонента іонізуючого випромінювання.

Заслуговує на увагу те, що навантаження на компоненти може також підкреслити ефекти, використовувані для SPA або DPA. Зміна експлуатаційних режимів не має особливо впливати на генератори випадкових чисел, наприклад, заснованих на неоднаковому розподілі нетривалого k DSA.

5.2.3 ***Політики функцій безпеки й ролі (FDP_ACC, FDP_ACF)***

[SSCD PP] вирізняє дві ролі:

(1) адміністратор, який може виконати функції під час ініціалізації й персоналізації;

(2) підписувач, який також може виконати функції створення підпису.

У наступних розділах наведено пояснення політик безпечного функціонування (SFP) для кожного типу SSCD.

5.2.3.1 *SSCD типу 1*

Для SSCD типу 1 атрибут користувача "роль" визначено як "Адміністратор". Атрибут безпеки користувача «керування SCD/SVD» може бути "дозволений (authorised)" або «не дозволений».

Аргументацію наявності єдиної ролі — SSCD типу 1 — призначено винятково для генерації пари SCD-SVD; використання SCD для створення підписів підписувачем не визначено.

Атрибути безпеки для SSCD типу 1 (від [SSCD PP] тип 1, FDP_ACF.1)

Користувач, суб'єкт або об'єкт, із яким асоційовано атрибут	Атрибут	Статус
Користувач	Роль	Адміністратор
Користувач	управління SCD/ SVD	дозволено, не дозволено

[SSCD PP] визначають три SFP, заснованих на призначенні SSCD типу 1 — генерація пари SCD-SVD — таким чином:

— «ініціалізація SFP» покриває генерацію пари SCD-SVD і головним чином використовується, щоб обмежити керування SCD/SVD адміністратором (FDP_ACC.1 керування доступом підмно-

жини й FDP_ACF.1 керування доступом, засноване на атрибуті безпеки), обмежити модифікації атрибута тільки адміністратором (FMT_MSA.1 керування атрибутами безпеки) і визначити обмежувальні значення за промовчанням (FMT_MSA.3 статична ініціалізація атрибута);

— «SCD експорт SFP» покриває експорт SCD в SSCD типу 2. SCD експорт SFP головним чином використовують для обмеження експорту SCD адміністраторові (FDP_ACC.1 керування доступом підмножини) і FDP_ACF.1 (керування доступом, засноване на атрибуті безпеки), FDP_ETC.1 (експорт користувацьких даних без атрибутів безпеки), FDP_UCT.1 (базові дані конфіденційного обміну), щоб обмежити модифікацію атрибута тільки адміністратором (FMT_MSA.1 керування атрибутами безпеки) і визначити обмежувальні значення за промовчанням (FMT_MSA.3 статична ініціалізація атрибута). Крім того, SCD експорт SFP використовує для надійного каналу, що буде наданий (FTP_ITC.1 Надійний канал між TSF);

— «SVD експорт SFP» покриває експорт SVD до CGA (опціонально до SSCD типу 2). SVD експорт SFP головним чином використовують для обмеження експорту SCD тільки адміністратором (FDP_ACC.1 керування доступом підмножини) і FDP_ACF.1 (керування доступом, засноване на атрибуті безпеки), FDP_ETC.1 (експорт користувацьких даних без атрибутів безпеки) і для підтримки цілісності експортованих даних (FDP_UIT.1 цілісність обміну даними). Крім того, SVD експорт SFP використовує для надійного каналу, що буде наданий (FTP_ITC.1 надійний канал між TSF).

5.2.3.2 *SSCD типу 2*

Для SSCD типу 2 адміністратор і підписувач можуть виконати дії, що стосуються фаз ініціалізації й створення підпису. Тому визначено три групи атрибутів безпеки: загальна група атрибутів, яка визначає, що роль користувача може бути «адміністратор» або «підписувач», група атрибутів ініціалізації для керування й імпорту SCD/SVD і група атрибутів створення підпису. Це відображено в наступній таблиці.

Атрибути безпеки для SSCD типу 2 ([SSCD PP] тип 2, FDP_ACF.1)

Користувач, суб'єкт або об'єкт, з яким асоційовано атрибут	Атрибут	Статус
Загальна група атрибутів		
Користувач	Роль	Адміністратор, Підписувач
Група атрибутів ініціалізації		
Користувач	керування SCD / SVD	дозволено, не дозволено
SCD	дозволено безпечний SCD імпорт	ні, так
Група атрибутів створення підпису		
SCD	робочий (експлуатаційний) SCD	ні ,так
DTBS	Відіслано авторизованим SCA	ні, так

[SSCD PP] визначає чотири SFP для SSCD типу 2 у такий спосіб:

— «SVD передача SFP» покриває опціональний імпорт SVD від SSCD типу 1 й експорт в CGA адміністратором або підписувачем як авторизованими користувачами (FDP_ACC.1 керування доступом підмножини й FDP_ACF.1 керування доступом, засноване на атрибуті безпеки). Тому її використовують для експорту SVD в CGA (FDP_ETC.1 експорт користувацьких даних без атрибутів безпеки), для цілісності даних повідомлення (FDP_UIT.1 цілісність обміну даними), щоб обмежити модифікацію атрибутів безпеки й керування SCD/SVD тільки адміністратором (FMT_MSA.1 керування атрибутами безпеки), а також визначити потрібний надійний канал до середовища (FTP_ITC.1 надійний канал між TSF);

— «SCD імпорт SFP» надає копію експорту SCD SSCD типу 1. Тому його використовують, щоб обмежити імпорт SCD авторизированому користувачеві, який може бути адміністратором або підписувачем (FDP_ACC.1 керування доступом підмножини й FDP_ACF.1 керування доступом, засноване на атрибуті безпеки), гарантувати, що SCD імпортовано авторизованим SSCD

(FDP_ITC.1 імпорт користувацьких даних без атрибутів безпеки) зі збереженням конфіденційності переданих даних (FDP_UCT.1 базові дані для конфіденційного обміну), обмежити модифікацію атрибута тільки адміністратором (FMT_MSA.1 керування атрибутами безпеки) і визначити обмежувальні значення за промовчанням (наприклад, робочий SCD перевести в «ні» після імпорту в FMT_MSA.3 статичної ініціалізації атрибута) і для потрібного надійного каналу SSCD типу 1 (FTP_ITC.1 надійний канал між TSF);

— «персоналізація SFP» покриває генерацію RAD адміністратором. Тому її використовують для відповідного керування доступом SFR (FDP_ACC.1 керування доступом підмножини й FDP_ACF.1 керування доступом, засноване на атрибуті безпеки);

— створення підпису SFP визначено для підписування DTBS підписувачем. Відповідні SFR керування доступу — FDP_ACC.1 (керування доступом підмножини), і FDP_ACF.1 (керування доступом, засноване на атрибутах безпеки). Створення підписів SFP також використовують для імпорту DTBSR (FDP_ITC.1 імпорт користувацьких даних без атрибутів безпеки) і підтримки цілісності DTBS (FDP_UIT.1 обмін даними із цілісністю). Модифікацію атрибутів безпеки обмежує тільки підписувач (FMT_MSA.1 керування атрибутами безпеки), а обмежувальні значення визначено за промовчанням (FMT_MSA.3 статична ініціалізація атрибута). Надійний канал до SCA визначено для імпорту DTBSR (FTP_ITC. надійний канал між TSF), як і надійний шлях (FTP_TRP надійний шлях) до HI, якщо HI не надає безпосередньо TOE.

5.2.3.3 *SSCD типу 3*

SSCD типу 3 визначає ролі адміністратора й підписувача аналогічно SSCD типу 2, див. 5.2.3.2. Атрибути безпеки, визначені в [SSCD PP], перелічено в наступній таблиці. Знову визначено різні групи атрибутів: користувацька група атрибутів, загальна група атрибутів і група атрибутів створення підпису.

Атрибути безпеки для SSCD типу 3 ([SSCD PP] тип 3, FDP_ACF.1)

Користувач, суб'єкт або об'єкт, із яким асоційовано атрибут	Атрибут	Стан
Користувацька група атрибутів		
Користувач	Роль	Адміністратор, Підписувач
Загальна група атрибутів		
Користувач	Керування SCD / SVD	дозволено, не дозволено
Група атрибутів створення підписів		
SCD	робочий SCD	ні, так
DTBS	Відіслано авторизованим SCA	ні, так

Як комбінація SSCD типу 1 і SSCD типу 2, визначено чотири SFP для SSCD типу 3 у [SSCD PP] у такий спосіб:

— «ініціалізація SFP» покриває генерацію пари SCD-SVD і головним чином використовується, щоб обмежити «керування SCD/SVD» тільки користувачем, який може бути адміністратором або підписувачем (FDP_ACC.1 керування доступом підмножини й FDP_ACF.1 керування доступом, засноване на атрибутах безпеки). Модифікацію атрибута безпеки «керування SCD/SVD» обмежує тільки адміністратор (FMT_MSA.1 керування атрибутами безпеки), а обмежувальні значення визначено за промовчанням (FMT_MSA.3 статична ініціалізація атрибута);

— «персоналізація SFP» покриває генерацію RAD адміністратором. Тому її використовують відповідним керуванням доступом SFR (FDP_ACC.1 керування доступом підмножини й FDP_ACF.1 керування доступом, засноване на атрибутах безпеки);

— «SVD передача SFP» покриває експорт SVD в CGA адміністратором або підписувачем (FDP_ACC.1 керування доступом підмножини, FDP_ACF.1 керування доступом, засноване на атрибуті безпеки й FDP_ETC.1 експорт користувацьких даних без атрибутів безпеки) для цілісності даних повідомлення (FDP_UIT.1 цілісність обміну даними) і для потрібного надійного каналу до CGA (FTP_ITC.1 надійний канал між TSF);

— «створення підпису SFP» визначено для підписання DTBS підписувачем. Відповідні SFR керування доступом — FDP_ACC.1 (керування доступом підмножини) і FDP_ACF.1 (керування доступом, засноване на атрибутах безпеки). Створення підпису SFP також використовують для імпорту DTBSR (FDP_ITC.1 імпорт користувацьких даних без атрибутів безпеки) і підтримки цілісності DTBS (FDP_UIT.1 обмін даними із цілісністю). Модифікацію атрибута безпеки «робочий SCD» обмежує тільки підписувач (FMT_MSA.1 керування атрибутами безпеки), а обмежувальні значення визначено за промовчанням (наприклад, «робочий SCD» установлено в «ні» після створення) (FMT_MSA.3 статична ініціалізація атрибута). Надійний канал до SCA визначено для імпорту DTBSR (FTP_ITC.1 надійний канал між TSF), як і надійний шлях (FTP_TRP надійний шлях) до HI, якщо HI не надає безпосередньо TOE.

5.2.4 ***Перехід у робочий стан***

Для персоніфікованих засобів, тобто SSCD типу 2 і SSCD типу 3, атрибут «робочий SCD» визначено, щоб ідентифікувати, чи є SCD робочим для створення підпису, чи ні. Мета полягає в тому, щоб здійснити єдине керування підписувачем, як визначено для розширених електронних підписів у статті 2 [Dir.1999/93/EC] і Додатку III. Не може бути жодної можливості використовувати SCD для створення підпису, перш ніж підписувач досяг такого одноосібного керування.

Можливі численні організаційні й технічні засоби, що реалізують цю особливість. Дві можливості — наступні:

— початковий PIN-код. SSCD можна постачати з «початковим PIN-кодом» (I-PIN), що недвозначно відрізняється від VAD (PIN-коду), використовуваного для створення підпису. Цього можна досягти, визначивши довжину I-PIN коду коротшою за мінімальну довжину PIN-коду, наприклад, п'ять символів I-PIN коду проти мінімум шести символів для PIN-коду. Коли підписувач спочатку вибирає PIN-код, I-PIN код не валідний і SCD установлено у робочий. Тоді підписувач може виявити, якщо SCD використовували до постачання SSCD, оскільки валідний I-PIN указує, що SCD не був робочим;

— імпорт сертифікатів. Оскільки кваліфіковані підписи вимагають SSCD і посиленого сертифіката, SSCD може надавати функції, які дозволяють підписувачу імпортувати посилений сертифікат. Якщо SSCD перевіряє валідність сертифіката, а передачу між SVD у сертифікаті й SCD реалізує SSCD, то факт, що підписувачу призначено посилений сертифікат, можна використати для установки SCD у робочий стан.

5.2.5 ***Знищення ключа (FCS_CKM.4)***

Для SSCD типу 1 SCD треба знищити після експорту в SSCD типу 2.

Для SSCD типу 2 або SSCD типу 3 SCD треба знищити на вимогу адміністратора або підписувача. Крім того, SCD треба знищити, перш ніж SCD повторно згенерований (SSDC типу 3) або повторно імпортований (SSCD типу 2).

Взагалі конструктори мають гарантувати, що знищення є постійним у тому сенсі, що відсутній будь-який засіб відновлення SCD або частини його на більш пізній стадії. Це означає, що конструктори мають відзначити, що:

— недостатньо тільки відключити доступ до SCD із даними SCD, що залишаються в пам'яті;

— необхідно розглянути дегенеративні ефекти, які випливають із тривалого зберігання даних. Приклад — «гарячі електрони» або окислювання, які можна виміряти після видалення даних;

— такі методики, як E^2PROM, які періодично поширюють дані між результатом сторінок у ситуаціях, коли дані можна видалити в активній сторінці, але контент залишається в неактивних сторінках.

Незважаючи на зазначені вище проблеми, фізично знищення SSCD бажано з погляду підписувача. Залежно від використовуваної технології, конструктор повинен дати подання про те, який "знешкоджувач" необхідно використовувати для певної реалізації SSCD. Як яскравий приклад, для широкої публіки, можливо, не очевидно, що поломка пластмаси в «схожій на кредитну картку» мікропроцесорній картці зазвичай не руйнує SSCD.

5.2.6 ***Оброблення невдач автентифікації (FIA_AFL)***

[SSCD PP] визначають для обробки невдалих автентифікацій (FIA_AFL.1), оскільки після невдалого числа спроб автентифікації RAD необхідно блокувати й у такий спосіб забороняти автентифікацію підписувача, що вимагає створити підпис.

Була несуттєва невизначеність про те, що мали на увазі автори PP щодо розблокування RAD, оскільки FMT_MTD.1 (керування даними TSF) визначає, що тільки одна роль може змінити RAD, це — підписувач, який у разі заблокованого RAD більше не може автентифікувати себе.

Фактично персоналізація SFP визначає для FDP_ACC.1/Персоналізація SFP (керування доступом підмножини) і FDP_ACF.1/Персоналізація SFP (керування доступом, засноване на атрибутах безпеки), що адміністратор може створити новий RAD. Цю звичайну практику використовують, наприклад, із банківськими картками.

5.3 Запити про роз'яснення

Цей розділ дає відповіді на «запити про роз'яснення про SSCD PP». Такі запити отримано під час зростаючого інтересу до стандартів. Запити згруповано за їх основними твердженнями і обговорено далі способом питання/відповідь.

5.3.1 *Статус SSCD PP*

Питання	Зараз видані SSCD PP — це єдині «стандарти безпеки» для всього SSCD?
Відповідь	Можливість кількох стандартів, які виконують вимоги SSCD, неявно подано в Директиві. Процедура, визначена в статтях 3 (5), 9 і 10, забезпечує, що Комісія може видати (будь-яке число) таких еталонів в офіційному європейському журналі.
Співтовариство	Коли продукт відповідає одному такому стандарту, зазначеному в офіційному журналі, це означає тільки, що продукт, як автоматично припускають, відповідає вимогам у додатку III Директиви. Однак продукт можна також безпосередньо визначити, як відповідний додатку III (не використовуючи такий стандарт), «відповідним суспільним або приватним органом, уповноваженим державою-членом. Таке визначення відповідності мають також визнати всі інші держави-члени.
Питання	Чи реєструють PP у реєстрі, як визначено в статті 3 (5) Директиви?
Відповідь	Так, CWA 14169, що містить PP, уведено до реєстру Єврокомісією в офіційному журналі 15 липня 2003 року.
Питання	Кожний із SSCD PP (Тип 1-3; EAL 4, EAL4 +) оцінено?
Відповідь	Усі три SSCD PP (Типи 1, Тип 2 і Тип 3) оцінено, а EAL 4+ дипломовано.

5.3.2 *Генерація ключа в CSP*

Питання	Є засіб SSCD PP для генерації SCD типу 1. Через те, що генерацію ключа зазвичай виконує CSP у фізично захищеному середовищі, хіба це не занадто високі вимоги для відповідності Додатка III?
Відповідь	Це було джерелом спірного обговорення під час розробки SSCD PP. Щодо положення 1 у цьому документі генерацію SCD за визначенням виконує SSCD. Проте оскільки SSCD PP дотримує загального підходу, який не розглядає середовища, надані в засобах CSP, зазвичай можуть бути інші стандарти генерації ключа й більше запобіжних заходів для засобів підписувача.

5.3.3 *Використання для підписання CSP*

Питання	Можна [SSCD PP] використовувати для того, щоб підписати засіб, використовуваний в CSP для штемпелювання часу або підписання посилених сертифікатів?
Відповідь	Це не було метою розробки [SSCD PP]. Проте область застосування CWA указує, що стандарт застосовний й у таких цілях. PP для криптографічного модуля конкретно звертається до вимог CSP засобу підписання, розроблених EESSI в області D2 [CMCSO PP] і зазначених Єврокомісією в офіційному журналі 15 липня 2003 року, як визначено в додатку II (f) Директиви [Dir.1999/93/EC].

5.3.4 *Відновлення та депонування ключів, спільне використання секретів SSCD*

Питання	Чи можна засіб з SCD, спільно використовуваний кількома особами, оцінити як SSCD PP?

Відповідь — Такі сценарії не підтримує SSCD PP, заснований на визначенні *підписувача,* наведеному в Директиві (стаття 2(3): підписувач — особа, яка підтримує засіб створення підписів) і визначення *розширеного підпису* (стаття 2(2): розширений підпис створюється з використанням засобу, які підписувач може підтримувати під своїм одноосібним контролем). Це не передбачає множини осіб, при цьому єдине керування не можна взяти на себе, якщо кілька людей спільно використовують SCD.

Питання — Чи може CSP забезпечити функції резервування для SCD?

Відповідь — Резервну копію SCD не підтримує SSCD PP, як обговорено у «положенні 3» у цьому стандарті.

Питання — Спільні секрети можуть бути корисними для CSP, наприклад, для резервування ключів із посиланням на застосування PP також для CSP.

Відповідь — Доки сфера застосування стверджує, що PP застосовно, коли первинна сфера застосування є SSCD підписувача. Тому SSCD PP обмежили сферу застосування визначенням підписувача як єдиного об'єкта. Жодні спільні секрети не передбачено.

5.3.5 *Надання послуги підписування*

Питання — SSCD PP застосовно до такого надання послуги підписування, як провайдер послуг, що підтримує SCD дистанційно, наприклад, через Інтернет?

Відповідь — Такі сценарії не розглянуто в [SSCD PP]. Однак вони важливі для розгляду й тому обговорені докладно в розділі 12.

5.3.6 *SVD експорт-імпорт для типу 2*

Питання — Чому на рисунку 3 немає блоків для імпорту й експорту SVD?

Відповідь — Ці блоки дійсно не відображено. Усе ще імпорт і експорт SVD надано SVD передачею SFP. Зазначимо, що зміст SVD або відповідного сертифіката не обов'язковий ані для типу 2, ані для типу 3 SSCD. Для типу 3 його треба експортувати в CGA для сертифікації й можна вилучити згодом. Для типу 2 або відповідного SSCD типу 1, що згенерував SCD, SVD може надати CGA або SVD може бути імпортований із SCD для подання в CGA. У кожному разі SSCD має бути здатним довести, чи відповідає SVD наданий SSCD SCD.

5.3.7 *Криптографічні атаки*

Питання — Як розкривають атаки, засновані на основних криптографічних операціях, як атаки на геш-функції чи протоколи підписування? Зокрема оскільки SCA може обчислити значення геш-функції, можуть бути атаки на схеми доповнення тощо.

Відповідь — Набори програм підписування, що підходять для кваліфікованих підписів, визначено в [ALGO]. З тих пір є набори програм, стійкі проти атак доповнення, тому можна гешувати поза SSCD.

5.3.8 *Автентифікація й ідентифікація*

Питання — SSCD-CTP обговорює автентифікацію підписувача (опис TOE або OE.HI_VAD), поки Директива говорить про розширені підписи як ідентифікацію підписувача.

Відповідь — Автентифікацію підписувача, використовувану SSCD PP, застосовують для втілення додатка III, конкретно 1(c) з вимогою, щоб SSCD гарантував, що SCD може надійно захистити підписувач від використання інших осіб.

Питання — Здається недостатнім, що CGA в OE.SVD_Auth_CGA верифікує SSCD відправник SVD щодо атак "людина усередині".

Відповідь — Крім того, потрібно в OE.SVD_Auth_CGA, щоб CGA верифікував передачу між SVD і SCD в SSCD підписувача, відповідно OE.CGA_QCert, вказуючий на SVD, відповідає SCD, реалізованому в TOE під одноосібним контролем підписувача. Таким чином, дане чітке посилання на підписувача.

5.3.9 *Розумна впевненість*

Питання — OT.SCD_Secrecy стверджує «розумна впевненість», а де "розумна" — неясно. OT.SCD_Secrecy заявляє «розумно впевнений», а де "розумно" — неясно.

Відповідь — Це формулювання взято з додатка III 1(a) Директиви. У його фактичному використанні в OT.SCD_Secrecy, "розумна" означає, що мета полягає в забезпеченні засобу, що достатньо забезпечує секрет SCD як первинне майно, навіть розглядаючи атакувальника з високим потенціалом атаки.

5.3.10 *Керування поведінкою функції безпеки (FMT_MOF.1)*

Питання — Стан відображення FMT_MOF.1 на OT.Sigy_SigF та OT.SCD_Secrecy є мало-з'ясований.

Відповідь — Функції керування доступом гарантують, що тільки законний підписувач може використовувати SCD для створення підпису, як задано в OT.Sigy_Sig, визначеному в додатку III Директиви, конкретно 1(c) («SSCD гарантує, що SCD може надійно захистити законний підписувач проти інших користувачів»). Відображення OT.SCD_Secrecy має запобігти таким атакам на SCD, заснованих на процесі створення підпису, який може бути початий як атака апаратного збою чи [DFA].

5.3.11 *Безпека випромінювання про неможливість спостереження (FPR_UNO)*

Питання — [SSCD PP] задають певне сімейство FPT_EMSEC, щоб покрити загрози, які випливають із спостереження за інтерфейсом або складовими випромінювання. Це розширення [ISO 15408]. Чому неможливість спостереження (FPR_UNO) недостатня для покриття таких загроз?

Відповідь — FPT_EMSEC уведено, щоб покрити загрози, які випливають із витоку під час обробки або передачі даних. Такий витік можна помітити через електромагнітне випромінювання SSCD, інтерфейси даних, явища споживаної потужності тощо. Зв'язані атаки, наприклад, SPA, [DPA], [DFA] тощо, обговорено докладно в 5.2.2.

FPR_UNO — сімейство, що покриває захист приватності, щоб уникнути спостереження за використанням послуги користувачем. У контексті SSCD це було б, наприклад, спостереженням за ситуацією, коли підписувач створює підпис, що лежить поза сферою застосування [SSCD PP]. На противагу атакам, до яких звертається FPT_EMSEC і які засновані на спостереженні за такими побічними ефектами, як фізичні явища, що показують конфіденційні дані під час використання SSCD, не є фактом використання безпосередньо SSCD. Тому FPR_UNO вважають недостатнім, щоб покрити ці загрози.

6 ВІДНОШЕННЯ SSCD PP ДО ІНШИХ СТАНДАРТІВ

У цьому розділі наведено настанову конструкторам, які прагнуть відповідати іншим зв'язаним профілям захисту. В 6.1 наведено короткий огляд різних стандартів, розширений детальним обговоренням у додатку I цього документа.

У 6.2 обговорено оцінювання SSCD як комбінації апаратних засобів і програмного забезпечення, використовуючи різні pro.

6.1 Короткий огляд пов'язаних профілів захисту

SSCD PP порівнювали з такими пов'язаними профілями захисту.

— Eurosmart PP-документи [PP 9806] [PP 9911] [PP 0002] і [PP 0010];

— PP-документ SC-групи користувачів NIST [SCSUG].

Повне порівняння SSCD PP та інших має в ідеалі містити такі теми порівняння:

— Який TOE може задовольнити різні PP?

— Які загрози взято до уваги?

— Які SFR враховано та які основні розбіжності є в концепції?

6.1.1 *SSCD PP*

Рівнем оцінювання CWA 14169 є EAL4, аргументований

— AVA_VLA.4,

— AVA_MSU.3.

Необхідна сила функції — «SOF— HIGH»

6.1.2 *Eurosmart PP9911 (програмне забезпечення й обладнання), що покладається на апаратні засоби PP9806*

Рівнем оцінювання [PP 9911] є також EAL4 +, але аргументований концепціями:

— ADV_IMP.2,

— ALC_DVS.2,

— AVA_VLA.4.

Ці PP ураховують етап розробки й фазу використання продукту. Отже, покрито активи:

— специфікації IC, дизайн, інструментальні засоби розробки й технологія,

— програмне забезпечення для IC;

— убудоване програмне забезпечення в смарт-картку, включаючи специфікації, реалізацію й зв'язану документацію;

— прикладні дані TOE (IC, дані конкретної системні, дані ініціалізації, вимоги попередньої персоналізації IC і дані персоналізації).

Розбіжності зроблені в описі TOE між модулем обробки, блоками пам'яті й уводом-виводом.

Активи треба захищати в термінах конфіденційності й цілісності.

Загрози відрізняються між фазами.

Як в [SSCD PP], немає жодного визначення організаційної політики безпеки, тому що її вважають занадто залежною від контексту використання TOE (тобто застосування).

Цілі безпеки включають мету для TOE, що має працювати завжди, навіть якщо змінюється середовище.

Цей PP включає вимогу FPR_UNO безпеки замість SSCD PP як специфічної функціональної вимоги безпеки FPT_EMSEC.1.

6.1.3 *Eurosmart PP0002 "Профіль захисту платформи мікропроцесорної картки IC"*

Рівнем оцінювання [PP 0002] є також EAL4 +, але аргументований концепціями:

— ADV_IMP.2 (Реалізація TSF);

— ALC_DVS.2 (Достатність заходів безпеки);

— AVA_MSU.3 (Аналіз і тестування на небезпечні стани);

— AVA_VLA.4 (Дуже стійкий).

[PP 0002] головним чином націлений на смарт-картки IC. [PP 0002] також покриває таке програмне забезпечення, як убудоване програмне забезпечення IC, яке постачають зі смарт-картками виготовники IC.

Єдина організаційна політика безпеки — P.Process-TOE, що покриває захист під час розробки й виготовлення.

6.1.4 *Eurosmart PP0010 "Смарт-картка IC з безпечною платформою для багатьох застосувань"*

Рівень оцінювання — також EAL4+, але аргументований концепціями:

— ADV_IMP.2 (Реалізація TSF);

— ALC_DVS.2 (Достатність заходів безпеки);

— AVA_VLA.4 (Дуже стійкий).

Що стосується [PP 9911], то [PP 0010] має сильну залежність від [PP 9806]. Фактично TOE має впливати на апаратну платформу, сумісну з [PP 9806].

Як у [SSCD PP], немає жодного визначення організаційної політики безпеки, тому що її вважають занадто залежною від контексту використання TOE (тобто застосування).

6.1.5 *PP-документ SC-групи користувачів NIST (версія 3.0)*

Рівень оцінювання — також EAL4+, але аргументований концепціями:

— AVA_VLA.3 (Оцінка уразливості — Аналіз уразливості — Помірковано стійкий);

— ADV_INT.1 (Розробка — внутрішня організація TSF — модульність).

[SCSUG] включає коментар про надійний канал. "TOE складається з достатніх апаратних і програмних елементів, щоб бути здатним до встановлення надійного каналу до надійного джерела для завантаження застосування або для інших потенційно привілейованих команд." ([SCSUG], підрозділ 2.2, параграф 5).

PP покривають користувача й застосування TOE, таким чином, активи складені з даних користувача, а також коду застосування.

PP включає організаційну політику безпеки:

— P.Audit;
— P.Crypt_Std — Криптографічні стандарти;
— P.Data_Acc — Доступ до даних;
— P.File_Str — Структура файлу;
— P.Ident — Ідентифікація;
— P.Sec_Com — Безпечний зв'язок.

Детальне обговорення цих стандартів порівняно з [SSCD PP] наведено в додатку I цього стандарту. Наступний розділ звернено до аспектів, які конструктори розглядають, прагнучи відповідати різним PP.

6.2 Аспекти оцінювання SSCD як комбінації HW-SW

У цьому підрозділі розглянуто оцінку SSCD як комбінації апаратних засобів і програмного забезпечення. Тому 6.2.1 звертається до тих аспектів, коли бажана апаратна реалізація. У 6.2.2 зазначено програмні аспекти. Нарешті в 6.2.3 обговорено, як можна виконати комбіновані оцінки.

6.2.1 *Вимоги до компонентів апаратури*

SSCD складається з комбінації апаратних і програмних компонентів, здійснюючи певні функції безпеки TOE (TSF) для функціональних вимог, визначених в PP. Для деяких із цих вимог необхідна підтримка апаратних засобів, як описано нижче.

SSCD має здійснити заходи безпеки, щоб виконати функціональні вимоги безпеки FPT_PHP.1 (пасивне виявлення фізичної атаки) і FPT_PHP.3 (опір фізичній атаці). TSF, необхідний FPT_PHP.1, має виявити фізичне втручання, що може поставити під загрозу TSF, і забезпечити доказ втручання. Це зазвичай здійснюють покриттями, блокуваннями, ізоляціями й/або інкапсуляцією апаратури непрозорим герметичним матеріалом. Крім того, SSCD згідно з FPT_PHP.3 має пручатися фізичним атакам втручання, відповідаючи автоматично у такий спосіб, що TSF не порушено. Цього можна досягти датчиками виявлення втручання й властивостями занулення SCD та інших секретів, захистом від відмови середовища (EFP) або запуском перевірки захисту EFT від відмови середовища. Ці TSF можна здійснити повністю апаратними засобами, але їх також можна реалізувати програмним забезпеченням (наприклад, активні екрани чипа мікропроцесорної картки, які перевіряє операційна система). Засіб створення підпису, повністю реалізований програмно, не може в такий спосіб окремо захистити SCD від фізичної атаки втручання. Для SSCD, реалізованого на мікропроцесорній картці, де є тільки доступна напруга, коли картка вставлена в засіб читання карток, опір втручанню й занулення SCD могли, наприклад, відбутися як частина початкової процедури самотестування разом із вмиканням живлення.

Функціональну вимогу безпеки FDP_EMSEC.1 (випромінювання TOE) часто здійснюють комбінацією апаратних і програмних засобів (заходів) безпеки. Апаратні співпроцесори використовують не тільки для прискорення криптоалгоритмів, але й для забезпечення властивостей безпеки, щоб захистити SCC від простого й диференціального аналізу споживаної потужності, часових атак і інших атак, заснованих на поведінці фізичної реалізації. Програмна реалізація TSF згідно з FCS_CKM.1 (генерація криптографічного ключа) і FCS_COP.1 (криптографічна операція) має використовувати ці властивості безпеки для процесу створення підпису.

TSF генерації пари SCD/SVD, як вимагає FCS_CKM.1 для SSCD типу 1 і типу 3, має використовувати фізичний генератор випадкових чисел. Програмне забезпечення має здійснити криптоалгоритм, який створює пару SCD/SVD, і виконати тести фізичного генератора випадкових чисел згідно з FPT_TST.1 (тестування TSF).

Усі інші функціональні вимоги безпеки в PP взагалі може здійснити програмне забезпечення, незалежне від апаратних засобів.

6.2.2 *Поділ SSCD на різні компоненти*

Як описано в попередньому розділі, SSCD складається з апаратних і програмних компонентів. TSF здійснено комбінацією властивостей безпеки, наданих апаратними засобами, програмним забезпеченням і прикладними даними. Можливі різні рішення композиції цих властивостей безпеки, але загалом їх характеризують так само, як апаратні засоби й операційну систему або прикладні функції, як обговорено далі.

6.2.2.1 *Апаратна платформа*

Апаратні засоби SSCD реалізують TSF з вимогами:

(a) відповідь апаратних засобів на виявлені FPT_TST.1 апаратні відмови згідно з FPT_FLS.1 (відмова зі збереженням безпечного статусу),

(b) FPT_PHP.1 (пасивне виявлення фізичної атаки) і FPT_PHP.3 (опір фізичній атаці),

(c) самоперевірка апаратних ресурсів, як вимагає FPT_TST.1 (самоперевірка TSF).

Крім того, апаратні засоби, як передбачено, забезпечують функції, що підтримують FCS_CKM.1 (генерація криптоключа), FCS_COP.1 (криптооперація) і FPT_EMSEC.1 (випромінювання TOE). Для FCS_CKM.1 необхідний такий генератор випадкових чисел, як апаратне джерело шуму, що відповідає умовам [ALGO].

Для функцій можна використовувати криптографічний співпроцесор, стандартний для смарт-карток, або універсальний процесор, що виконує криптооброблення. Крім аспектів продуктивності, конструктор може використати спеціалізований криптосопроцесор для розробки SSCD, стійкий проти таких атак, як [DPA] щодо FPT_EMSEC.

6.2.2.2 *Операційна система*

Програмне забезпечення операційної системи управляє апаратними ресурсами й надає послуги застосуванням. Програмне забезпечення операційної системи реалізує:

(a) криптоалгоритми для FCS_CKM.1 і FCS_COP.1, у той час як параметри визначають дані TSF застосування. Ці TSF виконують FPT_EMSEC.1, використовуючи криптографічний співпроцесор і генератор випадкових чисел апаратної платформи;

(b) керування доступом до файлів, ключів і еталонних даних автентифікації, заснованих на даних TSF застосування;

(c) ідентифікація згідно з FIA_UID.1 (синхронізація ідентифікації), автентифікація згідно з FIA_UAU.1 (синхронізація автентифікації) і керування еталонними даними автентифікації згідно з FIA_AFL.1 (обробка невдалої автентифікації) і FIA_ATD.1 (визначення користувацьких атрибутів);

(d) автоматична перевірка цілісності збережених даних згідно з FDP_SDI.1 (моніторинг цілісності збережених даних);

(e) повторне використанню об'єкта для криптографічних особистих і секретних ключів і даних автентифікації згідно з FDP_RIP.1 (захист підмножини залишкової інформації);

(f) відповідь операційної системи на виявлені FPT_TST.1 (самоперевірка TSF) апаратні або програмні відмови згідно з FPT_FLS.1 (відмова зі збереженням безпечного статусу);

(g) самотестування згідно з FPT_TST.1 (самотестування TSF) для реалізації криптоалгоритмів, генератора випадкових чисел і властивостей керування доступом;

(h) кодування й криптографічні механізми контрольних сум для даних уводу-виводу на підтримку FDP_UIT.1 (цілісність обміну даними), FTP_ITC.1 (надійний канал між TSF) і FTP_TRP.1 (надійний шлях) залежно від даних TSF (ключів) застосування.

6.2.2.3 *SSCD застосування*

Застосування SSCD складається з певних даних SSCD (користувацьких даних й даних TSF) і, можливо, певного програмного забезпечення для підписання.

Для мікропроцесорних карток застосування SSCD, зазвичай, складається тільки з користувацьких даних (ключів) і даних TSF у формі каталогів, простих файлів із їхніми правами доступу. Здійсненний код не є частиною застосування SSCD, тому що операційна система забезпечує всі необхідні функції.

Застосування SSCD реалізує:

(a) FDP_ACC.1 функціональні вимоги безпеки керування доступом (політика керування доступом) і FDP_ACF.1 (керування доступом, засноване на атрибутах безпеки) за визначенням SSCD PP SFP через атрибути безпеки (наприклад, права доступу до файлу для смарт-карток), засновані на властивостях безпеки операційної системи;

(b) SFP для імпорту й експорту даних згідно з FDP_ETC.1 (експорт користувацьких даних без атрибутів безпеки) і FDP_ITC.1 (імпорт ззовні TSF керування);

(c) функції FMT_MOF.1 керування безпекою (керування поведінкою функцій безпеки), FMT_MSA.1 (керування атрибутами безпеки), FMT_MSA.2 (безпечні атрибути безпеки), FMT_MSA.3 (статична ініціалізація атрибута), FMT_MTD.1 (керування даними TSF) і FMT_SMR.1 (безпечні ролі), засновані на властивостях безпеки операційної системи

(d) визначене абстрактне машинне тестування FPT_AMT.1 (абстрактне машинне тестування), засноване на властивостях безпеки операційної системи, можливо, удосконаленої згідно з [SSCD PP] політикою функціональної безпеки з використанням атрибутів безпеки.

6.2.3 *Оцінювання SSCD як складеного засобу*

Апаратні засоби, програмне забезпечення й застосування зазвичай надають різні продавці. Це визначає оцінювання складеного продукту, заснованого на оцінених компонентах. Далі обговорено загальні підходи до оцінювання (рисунок 7). Мета всіх цих оцінювань полягає в тому, щоб одержати сертифікат для SSCD, що відповідає SSCD PP.

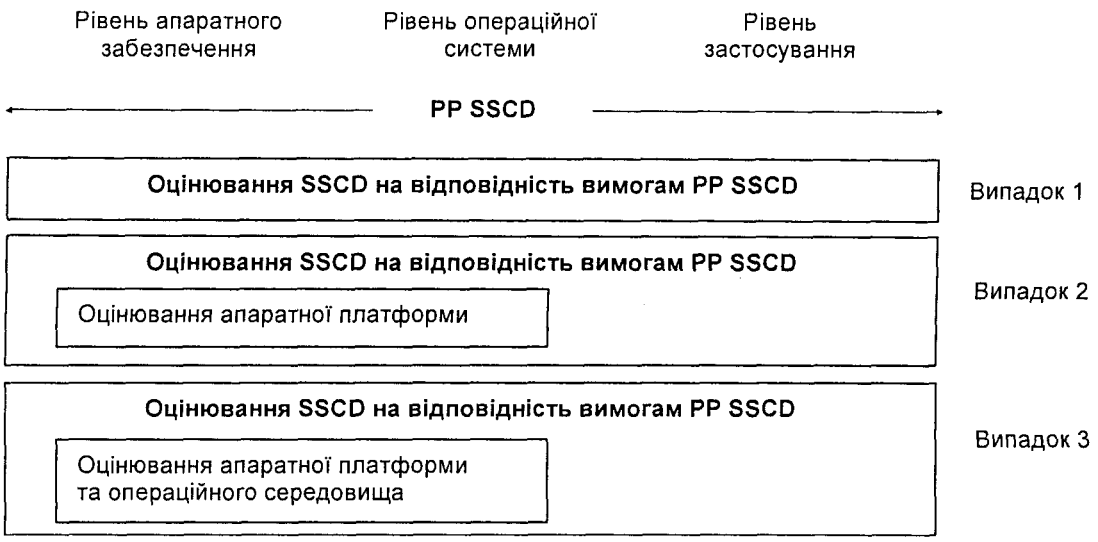


Рисунок 7

6.2.3.1 *Випадок 1 — Оцінювання SSCD як інтегрального продукту*

TOE — закінчений SSCD, а цілі безпеки вимагають відповідності з SSCD PP. Жоден із компонентів TOE не оцінюють окремо. Спонсор оцінювання SSCD гарантує, що розробники різних компонентів забезпечують необхідне оцінювання вузлів і їхніх компонентів.

6.2.3.2 *Випадок 2 — Оцінювання SSCD із використанням оцінок апаратної складової*

TOE і ціль безпеки — ті самі, що й у випадку 1, але апаратну платформу TOE раніше оцінено й сертифіковано. Оцінювання SSCD може використовувати результати сертифікації апаратної платформи із гарантією, що:

— ST апаратної платформи включає відповідні цілі безпеки й вимоги безпеки SSCD PP;

— операційна система й прикладні компоненти TOE використовують апаратну платформу гарантованим способом, тобто як вимагає настанова з апаратної платформи.

Якщо ці умови виконано, оцінювання SSCD може прийняти задані сертифіковані властивості безпеки. Оцінювання SSCD зосередиться на:

— наданий TSF, що комбінує апаратну платформу й операційну систему, тобто TSF, що реалізує FPT_EMSEC.1,

— коректність і ефективність TSF, наданого операційною системою й застосуванням,

— продукт у цілому, виконуючий SSCD PP.

Зазначимо, що останнє завдання оцінювання, можливо, має потребу в подальшій інформації про результати оцінювання апаратної платформи. Ці проблеми залежать від реалізації й технології SSCD, сертифіката апаратної платформи й інших факторів.

Описаний підхід до оцінювання широко використовують для смарт-карток. Приклади конфігурацій захисту, які можна розглянути як підставу для оцінок апаратури:

— профіль захисту інтегральної схеми смарт-картки [PP 9806];

— профіль захисту платформи смарт-картки IC [PP 0002].

Але зазначимо, що SSCD PP, із одного боку, PP [PP 9806] і [PP 0002], з іншого боку, не відповідають повністю один одному. Більш детально див. додаток I цього стандарту.

Оцінювання смарт-карток як комбінації чипа, з одного боку, і операційної системи й застосування, з іншого, — обговорено в чартерній ініціативі по смарт-картках eEurope, ТВ3, включаючи органи сертифікації, засоби оцінювання й продавців смарт-картки.

6.2.3.3 *Випадок 3 — Оцінювання SSCD, що використовує оцінки апаратної складової й операційної системи*

TOE і ціль безпеки — ті самі, що й у випадку 1, але об'єднану апаратну платформу й операційну систему TOE раніше оцінено й сертифіковано. Оцінювання SSCD може використовувати результати сертифікації з гарантією, що

(i) ST продукт включає відповідні цілі безпеки й вимоги безпеки SSCD PP;

(ii) прикладний компонент TOE використовує сертифікований продукт сертифікованим способом, тобто як вимагає настанова.

Якщо ці умови виконано, оцінювання SSCD може прийняти задані сертифіковані властивості безпеки. Оцінювання SSCD зосередиться на:

(iii) застосування використовує властивості безпеки, надані сертифікованим продуктом для реалізації TSF, необхідного SSCD PP, тобто використовує керування доступом для ключів, наданих операційною системою, щоб реалізувати SVD передачу SFP, ініціалізацію SFP, персоналізацію SFP і створення підпису SFP;

(iv) продукт у цілому виконує SSCD PP.

Зазначимо, що завдання оцінювання (iii), можливо, має потребу в подальшій інформації про оцінки апаратної платформи й операційної системи. Ці проблеми залежать від реалізації й технології SSCD, сертифіката оцінювання й інших факторів.

Описаний підхід до оцінювання також можна використовувати для смарт-карток. Приклади профілів захисту, які можна розглянути як підставу для оцінювання:

— профіль захисту інтегральної схеми смарт-картки з убудованим програмним забезпеченням [PP 9911];

— група користувачів безпечної смарт-картки: профіль захисту смарт-картки [SCSUG].

Проте зазначимо, що SSCD PP, з одного боку, PP [PP 9911] і [SCSUG], з іншого боку, не відповідають один одному повністю. Детальніше див. додаток I цього стандарту.

7 ЗАГАЛЬНІ НАСТАНОВИ З РЕАЛІЗАЦІЇ ПЛАТФОРМИ

Процес створення підпису, описаний в [CWA 14170], визначає систему створення підписів (SCS) як складену із застосування накладання підпису (SCA) і безпечного засобу створення підпису (SSCD). Універсальний процес накладання електронного підпису такий (див. рисунок 8):

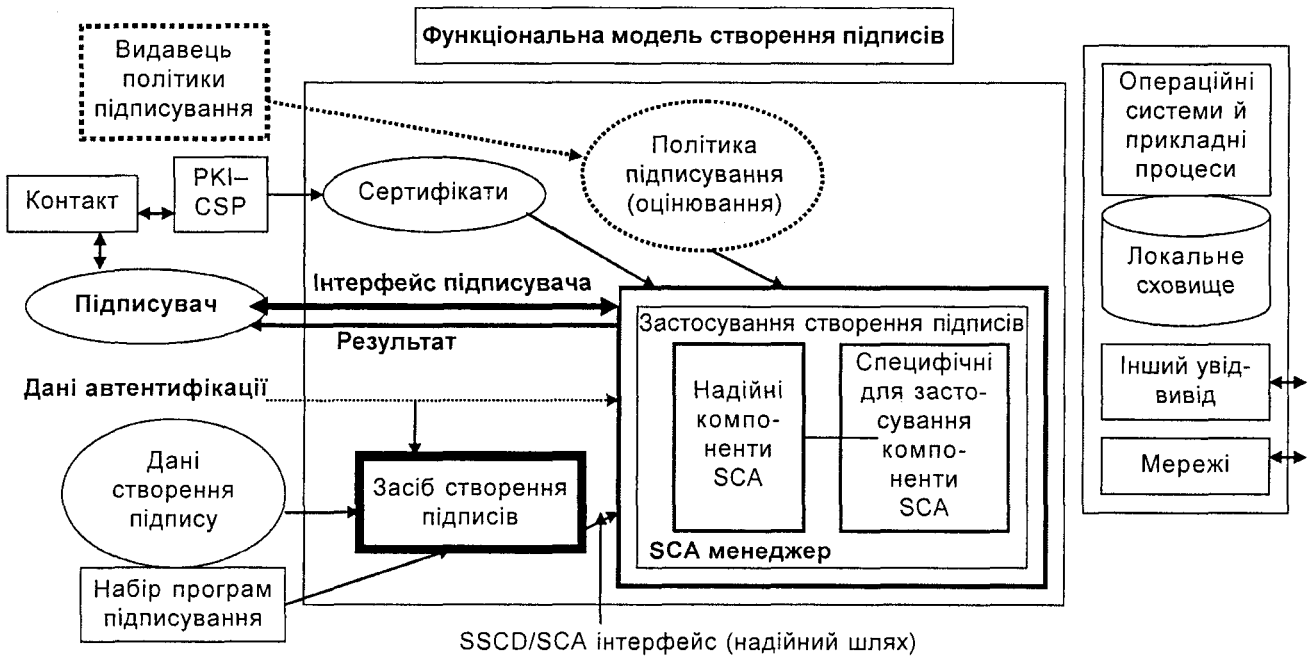


Рисунок 8

— компонент подання документа особи, що підписує (SDP), використовує SCA, щоб зробити огляд документа;

— SCA одержує дозвіл підписати повідомлення через інтерфейс користувача (HI);

— із даних гешування компонента (DHC) SCA створює подання (геш) DTBS, згадуване як DTBSR;

— SCA посилає DTBSR у SSCD;

— SSCD створює підпис, використовуючи SCD;

— виведено підписані формати (SDOC) композитора об'єкта даних SDO.

7.1 SSCD і посилений сертифікат

7.1.1 *SSCD-індикатор у сертифікаті*

Кваліфікований електронний підпис визначено як розширений електронний підпис, заснований на посиленому сертифікаті й створений SSCD. ETSI QCP [TS 101456] визначає два ідентифікатори політики сертифікації, один із яких «публічний QCP + SSCD» гарантує, що посилений сертифікат, випущений для SVD (відкритий ключ), а відповідний SCD (особистий ключ) постійно перебуває в SSCD. Для залежних сторін одержання підписаного повідомлення, яке посилається на такий сертифікат, завіряє їх, що підпис фактично є кваліфікований підпис.

Якщо замість цього посилений сертифікат тільки містить ідентифікатор політики «публічний QCP», то залежна сторона має через інші засоби одержати гарантію, що використано SSCD. Хоча цього можна досягти технічними або процедурними засобами, зазвичай це буде набагато складніше, ніж якщо цю довіру надає CA, наприклад, визначаючи OID QCP у сертифікаті.

7.1.2 *Надійний канал до CGA*

Щоб спростити потреби залежних сторін, можна чекати, що більшість CA захоче гарантувати й гарантує, що використано SSCD для зберігання SCD, навіть якщо SSCD не надано CA. У такому сценарії підписувач одержить свій SSCD із іншого джерела й потім на більш пізній стадії запросить сертифікат свого SVD. Це вже передбачено в [SSCD PP], який для експорту вимагає FTP_ITC.1/SVD, щоб SSCD забезпечив надійний канал експорту SVD у застосування генерації сертифіката CGA. Проте не наведено подробиць реалізації для такого каналу й немає вимог для CGA з використання цього надійного каналу. Відомі такі рекомендації реалізації для надійних каналів:

— реалізація SSCD має ретельно розглянути цю функцію й забезпечити механізм, який може легко використовувати CGA для гарантії, що SVD виходить зі справжнього SSCD, і верифікувати цілісність SVD;

— потенційний механізм для цього може, наприклад, надати всім SSCD як спеціалізований особистий ключ, використовуваний для підписання експортованого SVD. Тоді CGA може верифікувати SVD, використовуючи відповідний відкритий ключ постачальника, що поширюється в сертифікаті;

— більш надійний механізм зберігає залежний від засобів секретний ключ на всіх SSCD разом із сертифікатом засобу, підписаним продавцем. Тоді CGA може також верифікувати дійсність SSCD.

Крім того, [SSCD PP] допомагає CGA, пропонуючи доказ передачі між SCD і SVD як криптографічну операцію (FCS_COP).

7.1.3 *Поширення сертифікатів*

Під час генерації сертифіката SSCD спілкується з CGA. Взагалі існують дві альтернативи залежно від часу доставки SSCD підписувачу:

— сертифікат створено CSP разом із генерацією ключа й персоналізацією SSCD, до доставки SSCD підписувачу;

— сертифікат створив у пізніший час й ініціював підписувач.

Які потреби треба розглянути? Що включає визначення посиленого сертифіката, що SCD перебуває під контролем підписувача ([Dir.1999/93/EC], Додаток 1(e))? Таким чином, у першому випадку заходи мають гарантувати, що сертифікат «не зроблено доступним» до фактичного одержання SSCD підписувачем, який має контроль над SCD.

В обох випадках експорт SVD через надійний канал необхідний, якщо генерація SCD/SVD виконана в SSCD або вона виконана на SSCD типу 1 і пізніше експортована в SSCD підписувача.

7.2 Реалізація SCA та SSCD

Якщо SCA і SSCD реалізовано на певній платформі, є дві можливості:

— SCA і SSCD спільно використовують обчислювальний механізм (клас 1 SCS),

— SCA і SSCD використовують два окремих обчислювальних механізми (клас 2 SCS).

Обидві можливості обговорено далі.

7.2.1 *Клас 1 SCS — SCA і SSCD спільно використовують обчислювальний механізм*

Для класу 1 SCS, SCA і SSCD спільно використовують обчислювальний механізм. Це розташування вимагає рішення таких проблем:

— поділ домена. SCA і SSCD мають бути окремими від всіх інших обчислювальних процесів. Якщо єдина мета засобу — створення підпису, це — не проблема. Якщо засіб ураховує інші операції, тоді підключення між SCA і SSCD вимагає надійного каналу;

— захист SCD. Оскільки засіб діє як SSCD, треба забезпечити всі функції SSCD;

— захист DTBSR. Створення й передача DTBSR (тобто значення геш-функції) вимагають надійного каналу між SCA і SSCD. Надійний канал у засобі з єдиною метою може бути апаратним каналом на захищеній платформі;

— безпечний увід-вивід. SCA здатний відобразити належним чином повідомлення, щоб підписати (DTBS) і дістати однозначну згоду користувача створити один або більше підписів.

Головні моменти атаки для реалізації класу 1 SCS пов'язані з відділенням SCA і SSCD від інших компонентів і захистом SCD. У засобах із єдиною метою не існує більшості цих проблем; однак у користувача є засіб, який виконує тільки одну операцію. Із загальнодоступними обчислювальними машинними й множинними процесами захист SCD і належна передача DTBSR стали важко розв'язуваними проблемами.

7.2.2 *Клас 2 SCS — SCA і SSCD на окремих обчислювальних механізмах*

Для класу 2 SCS використовують окремі обчислювальні механізми SCA і SSCD. Окремі компоненти можна реалізувати на тій же фізичній платформі, але процеси спільно не використовують один обчислювальний механізм. Це розташування вимагає вирішення наступних проблем:

— надійний канал. SCA і SSCD вимагають, щоб надійний канал повідомив команди й DTBSR. Команди включають вибір користувача SCD і однозначної згоди виконати один або більше підписів;

— ідентифікація SCA і SSCD. Належне створення надійного каналу вимагає ідентифікації й автентифікації двох кінцевих крапок;

— SCA належить мати безпечний шлях уводу-виводу, щоб належним чином відобразити повідомлення для підписання й дістати згоду користувача підписатися через надійний шлях;

— SSCD має повторно перевірити валідність згоди користувача виконати підпис.

Головні моменти атаки для реалізації класу 2 — надійний канал між SCA і SSCD. Тому що SSCD відповідає вимогам SSCD PP і колись DTBSR досягає SSCD, то виконано вимоги безпеки. Проблема — створення DTBSR і його передача.

7.3 Обмеження відображення

У багатьох засобів є доступ до обмеженої кількості екранних засобів відображення. Це обмеження створює потребу мати два типи засобів підпису. Ці два типи відомі як «Відображення повідомлення» і «Відображення геша».

7.3.1 *Засіб відображення повідомлень DM*

Засіб DM може відобразити всі повідомлення, що містять закінчений SCA. Всі повідомлення, включно текст, відформатовану інформацію, графіку, колір і іншу інформацію.

Повідомлення подають на екрані засобу SDP (компонент відображення документа підписувача) SCA, що постійно перебуває на засобі.

7.3.2 *Засіб відображення геша (DH)*

Якщо засіб підписання може відобразити тільки обмежену кількість даних, SCA фактично складена із двох частин: одна — на засобі, а інша — на віддаленому терміналі. Віддалена термінальна частина SCA містить SDP так само, як компонент гешування даних (DHC — Data Hashing Component), що подасть дані, виконає гешування, відобразить результуюче значення геш-функції й також надішле значення геш-функції в засіб. Значення геш-функції буде відображено також на засобі для гарантії цілісності DTBSR, відісланого з віддаленого термінала на засіб.

7.4 Випадки використання

Відомі такі випадки використання

	Засіб відображення повідомлення	Засіб відображення геша
Клас 1: спільний обчислювальний механізм	Система класу 1DM Ex: Спеціалізований засіб підписування, безпечний ПК із надійним уводом-виводом, безпечний кишеньковий комп'ютер з інтегрованим SSCD, SIM карта з SSCD	Система класу 1DH Ex: смарт-картка з дисплеєм, мобільний телефон з інтегрованим WIM, спеціальний термінал підписування
Клас 2: окремий обчислювальний механізм	Система класу 2DM Ex: ПК зі смарт-карткою, кишеньковий комп'ютер зі смарт-карткою, мобільний телефон з S/WIM	Система класу 2DH Ex: мобільний телефон з S/WIM

7.4.1 *Система класу 1DM*

Ця система є повністю модульною, має тільки один процесор і завжди забезпечує закінчений захист SSCD і SCA. Система забезпечує внутрішній надійний канал між SSCD і SCA.

Блок відображення повідомлень може однозначно відобразити повідомлення користувачеві й одержати його згоду виконати підпис.

Прикладом цього типу системи є спеціалізований продукт засобу підписання або ПК, що має безпечну операційну систему з надійним уводом-виводом для всіх засобів уводу й виводу. Інший приклад — SIM-карта, що містить SSCD і SCA, що тільки використовує мобільний телефон як засіб надійного вводу-виводу.

Система класу 1DM може також виконати ті самі функції, що й система класу 1DH, тобто відобразити геш замість закінченого повідомлення.

7.4.2 *Система класу 2DM*

У цієї системи є два обчислювальних модулі: основний процесор і SSCD. Система забезпечує надійний шлях між SCA основної системи й SSCD.

Блок відображення повідомлення підключено до процесора SCA і може відобразити повідомлення однозначно користувачеві. Згоду користувача виконати підпис можна одержати через надійний шлях до SCA або безпосередньо до SSCD (наприклад, пристрій, що зчитує, смарт-картки з убудованою клавіатурою для PIN-коду).

Прикладом цієї системи є ПК або кишеньковий комп'ютер з SSCD, прикріпленим як смарт-картка чи засіб USB, або мобільний телефон з S/WIM, у якому повідомлення — досить коротке, щоб відобразити його на телефоні.

7.4.3 *Система класу 1DH*

У цієї системи є SSCD і частина SCA на тому самому процесорі, система завжди забезпечує закінчений захист SSCD і локальної частини SCA.

Однак блок відображення не здатний відобразити все повідомлення й відображає тільки геш повідомлення. Тому потрібен надійний канал між віддаленою частиною SCA (відображає повідомлення й виконує гешування) і локальною частиною SCA.

7.4.4 *Система класу 2DH*

У цієї системи є окремі процесори для SSCD і SCA. Блок відображення не здатний відобразити все повідомлення й відображає тільки геш повідомлення. Використовуючи надійний канал, підключено SSCD і частину SCA, яка постійно перебуває на засобі, що відображає значення геш-функції.

SCA також містить віддалений компонент SDP і DHC. Система забезпечує надійний канал між DHC і SSCD.

Прикладом цього типу системи є мобільний телефон з SSCD в S/WIM (заснований на SIM WIM), що застосовують для підписання повідомлень, які неможливо відобразити безпосередньо на телефоні. Частина локального SCA постійно перебуває на S/WIM, використовуючи процесор мобільного телефону тільки, щоб відобразити значення геш-функції. Основна частина SDP і DHC утримується у віддаленому кінцевому застосуванні, наприклад, відображаючи повідомлення, що буде підписано в web-браузері.

8 НАСТАНОВИ З РЕАЛІЗАЦІЇ СМАРТ-КАРТОК

Смарт-картки зараз є очевидними SSCD. Вони безпечні, належать особі й дають користувачеві мобільність. Смарт-картки доступні як SSCD типу 2 і типу 3 (без і з убудованою генерацією ключів).

Смарт-картки — природний компонент системи створення підписів класу 2, оскільки смарт-картки не містять SCA.

8.1 Функції платформи SSCD

8.1.1 *Персоналізація*

Персоналізація охоплює генерацію SCD/SVD і імпорт SCD або експорт SVD за потреби. Є дві можливості для генерації ключів:

— генерація ключа, виконана поза карткою. Це означає, що SSCD типу 2 згідно [SSCD PP], з вимогою до надійного каналу для імпорту SCD. У цьому випадку генерацію ключа зазвичай виконує виготовник смарт-картки або CSP, що пропонує послуги постачання SSCD. Тоді смарт-картку постачають користувачеві з попередньо згенерованими ключами;

— генерація ключа безпосередньо в смарт-картці, «убудована генерація ключа». Смарт-картка з убудованою генерацією ключа є SSCD типу 3 згідно з [SSCD PP]. Генерацію ключа може ініціювати виготовник, CSP або користувач безпосередньо після одержання смарт-картки.

Другий крок персоналізації — генерація сертифіката — розглянуто в 7.1.3.

8.1.2 *Автентифікація користувача*

Для смарт-картки автентифікація користувача виконана протягом уводу алфавітно-цифрового значення PIN-коду через інтерфейс користувача. Інтерфейс користувача може бути клавіатурою, якою управляє SCA (наприклад, ПК або клавіатура кишенькового комп'ютера), або клавіатурою PIN-коду безпосередньо на терміналі смарт-картки.

Надійний шлях установлюють між інтерфейсом користувача й смарт-карткою, гарантуючи конфіденційність коду. Природно, це легко зробити на клавіатурі PIN-коду термінала смарт-картки.

Після визначеного числа помилкових спроб картку буде блоковано. Її можна відкрити після вводу PIN-коду розблокування ключа (PUK — PIN Unblocking Key).

8.1.3 *Надійні канали й надійний шлях*

У класі 2 SCS важливе припущення для SSCD — надійний канал до SCA. Для смарт-карток це спричиняє автентифікацію SCA і механізм, що підтримує надійний канал. Наведені далі механізми для установки надійного каналу можна використовувати для смарт-карток:

— безпечний обмін повідомленнями, як визначено в [ISO 7816]; детальніше див. 5.2.1.2;

— зовнішня автентифікація, як визначено в [ISO 7816].

Надійні канали й шляхи також установлюють у таких цілях:

— надійний канал необхідний для імпорту SCD у смарт-картку від SSCD типу 1, коли виконано генерацію ключа поза смарт-карткою;

— надійний канал необхідний для експорту SVD зі смарт-картки в CGA, коли виконано генерацію ключа в смарт-картці;

— надійний шлях потрібен для вводу користувачем даних автентифікації (PIN-код) у смарт-картку.

8.2 Середовище SSCD

Процес підписування може бути у двох чітко різних типах фізичних середовищ, де SCA управляють різні організації.

Типове середовище для першого випадку — будинок або офіс, де в людини або компанії є пряме керування SCA. Тоді вимоги безпеки підписувач може виконати за допомогою організаційних заходів, а технічними засобами гарантувати, що досягнення вимог безпеки можна послабити. Наприклад, у крайньому випадку підписувач може використовувати ізольований ПК, збережений у сейфі, який може відкрити тільки підписувач.

У другому випадку типове середовище таке, що SCA розташовано в такому публічному місці, як залізнична станція, банк або будь-який інший SCA, яким управляє провайдер послуг, не обов'язково пов'язаний з або під керуванням підписувача.

Без подальших технічних заходів безпеки цей тип середовища може перенести багато інших видів атак, наприклад, заміна SCA помилковим SCA. Тому будуть суворіші технічні вимоги SCA, яким управляють у такому публічному середовищі.

9 НАСТАНОВИ З РЕАЛІЗАЦІЇ МОБІЛЬНИХ ТЕЛЕФОНІВ

Мобільний телефон — чудовий засіб створення підписів. У нього є можливість містити SSCD і частини SCA. Мобільний телефон — особистий засіб, зазвичай захищений від неправильного вживання його власником.

Далі «мобільний телефон» використовують, щоб позначити закінчений кишеньковий засіб, складений із мобільного обладнання (ME) безпосередньо й з будь-яких SIM-карток, чипів або інших смарт-карток, вставлених у нього.

Теоретично мобільний телефон може бути класом 1 або класом 2 SCS. Хоча можна використовувати телефон безпосередньо, щоб здійснити SSCD, очікується, що він зазвичай буде класу 2 SCS із SSCD, здійснюваним на SIM-карті, можливо, відповідно до стандарту WIM (картка S/WIM). Інша цікава можливість полягає в тому, що сама SIM-карта становить клас 1 SCS, використовуючи ME також як надійний засіб уводу-виводу для уводу PIN-коду й відображення.

Також можна здійснити SSCD на окремому чипі, відмінному від SIM-карти. Це рішення вимагає телефона з "двома слотами" або "двома чіпами", куди окрема смарт-картка або чип (що використовує WIM або інший стандарт) вставлено у телефон. Однак під час розробки цього документа таке рішення, здається, не мало інтересу й тому далі не обговорено.

9.1 Міркування про використання

Мобільний телефон має обмежену кількість наявного простору відображення, щоб відобразити повідомлення. Як передбачається, його будуть використовувати для підписання в одному із трьох випадків:

— як клас 1DM, де повідомлення досить мале для подання на дисплеї телефону. Тоді закінчені SCA, включаючи SDP і DHC, постійно перебувають на SIM-карті разом із SSCD;

— як клас 2DM, де повідомлення досить мале для подання на дисплеї телефону. Однак тоді SDP і DHC постійно перебувають на мобільному обладнанні, а SSCD — на SIM;

— як система класу 2DH, де повідомлення занадто велике для подання по телефону, тільки значення геш-функції подано й підписано.

9.1.1 *Відображення закінченого повідомлення по телефону*

Повідомлення, що буде підписано, посилають у мобільний телефон, використовуючи команду WMLScript **signText** або подібну функцію. Мобільний телефон подає повідомлення на екрані, гешує повідомлення й підписує його, використовуючи особистий ключ, збережений у мобільному телефоні.

У цьому разі фактично є два способи реалізації SCA:

— SCA на ME. Тоді SCA постійно перебуває на мобільному обладнанні й тільки передає значення геш-функції SIM-карті, яка має встановити надійний канал з SCA, щоб одержати DTBSR і передати назад SDO (підписаний об'єкт даних). Також необхідний надійний канал для уводу даних автентифікації з клавіатури ME;

— SCA на SIM безпосередньо. Тоді SCA постійно перебуває на SIM разом з SSCD, спільно використовуючи обчислювальний механізм SIM. Через API SIM Toolkit телефону SCA використовує тільки дисплей телефону як SDP (засіб перегляду), а клавіатуру як засіб уводу даних для автентифікації (PIN-код). Тоді SIM-карта фактично здійснює тип 1DM системи.

9.1.2 *Відображення телефоном тільки значення геш-функції*

Повідомлення, що буде підписано, є занадто великим для подання на екрані ME. Замість цього повідомлення подане, наприклад, в Web-браузері, що постійно перебуває на ПК. Застосування підписання тоді гешує повідомлення й посилає геш у телефон для підписання. Щоб гарантувати, що в значення геш-функції не втрутилися по шляху, частину значення геш-функції подано як шістнадцятковий рядок у браузері/засобі перегляду й на екрані телефону.

Коли тільки значення геш-функції посилають на телефон для підписання, SCA фактично складається із двох частин: одна — у мобільному телефоні, а інша — у віддаленому терміналі, кожна містить SDP, як і DHC. Разом дві частини SCA гарантують цілісність DTBSR (значення геш-функції), надіслане з віддаленого термінала на телефон. Це можна зробити, порівнюючи значення геш-функції, подані в обох частинах SCA, таким чином дозволяючи користувачеві верифікувати їхню коректність.

9.2 Функції платформи SSCD

9.2.1 *Персоналізація*

Персоналізація охоплює генерацію SCD/SVD і імпорт SCD або експорт SVD за потреби. Є дві можливості виконати генерацію ключів:

— генерація ключа, виконана поза карткою. Це означає, що SSCD має тип 2 згідно [SSCD PP] із вимогою до надійного каналу для імпорту SCD. У цьому випадку генерацію ключа зазвичай виконує виготовник SIM-карти або оператор мобільного зв'язку. А SIM постачають користувачеві з попередньо згенерованими ключами;

— генерація ключа в смарт-картці безпосередньо, «убудована генерація ключа». SIM-карта з убудованою генерацією ключа є SSCD типу 3 згідно з [SSCD PP]. Генерацію ключа може тоді ініціювати виготовник, оператор або користувач безпосередньо після одержання SIM.

Другий крок персоналізації — генерація сертифіката — розглянуто в 7.1.3.

9.2.2 *Автентифікація користувача*

Мобільний телефон забезпечує чудовий механізм для одержання користувацького наміру. Екран і увід (клавіатура) підключено й захищено від втручання. Це дуже просто зробити так, щоб користувач увів послідовність чисел, відображених на екрані, і перевірити намір замість того, щоб тільки натиснути мишею або вибрати єдину кнопку.

Автентифікація користувача охоплює увід даних верифікації автентифікації підписувача (SVAD — Signatory's verification authentication data), тобто даних автентифікації, наданих користувачем для автентифікації як підписувача. Для мобільного телефона це означає числовий PIN-код, уведений користувачем на клавіатурі мобільного телефона. Рекомендовано, щоб PIN-код не відображався під час набору. Так SSCD має підтримувати надійний шлях до PIN-клавіатури.

На відміну від звичного PIN-коду для SIM-карти, автентифікація користувача для функції підпису має бути для кожної операції підписання.

Після визначеного числа помилкових спроб SIM-карта буде блокована. Її можна відкрити тільки після вводу PIN-коду PUK розблокування ключа.

9.2.3 *Надійні канали і шляхи*

Наступні надійні канали й шляхи можна пророкувати для платформи мобільного телефона:

— надійний канал потрібен для імпорту SCD в SSCD від SSCD типу 1, після виконання генерації ключа поза SIM-картою;

— надійний канал потрібен для експорту SVD від SSCD до CGA, після виконання генерації ключа в SIM-карті;

— надійний канал потрібен для імпорту DTBSR в SSCD від SCA. Цього легко досягти в системі класу 1, коли й SSCD і SCA постійно перебувають на SIM-карті. Коли SCA постійно перебуває на мобільному обладнанні, вимоги до надійного каналу залежать від операційної системи ME;

— надійний шлях потрібен для вводу користувачем даних автентификации (PIN-код) із клавіатури телефону в SSCD.

9.3 Середовище SSCD

У всіх випадках використання зазначених вище, SSCD здійснено на SIM-карті. Мобільний телефон включає "безпосереднє середовище", з екраном, клавіатурою й SCA (крім того, SCA реалізовано на SIM разом із SSCD).

Доки користувач використовує власний мобільний телефон, він розцінює його як надійне середовище.

Однак, якщо він у певний момент поміщає свою SIM-карту в інший мобільний телефон, він захоче гарантії того, що цьому новому мобільному телефону можна довіряти й він не є керованим мобільним телефоном, ставлячи під загрозу функцію підписування.

10 НАСТАНОВИ З РЕАЛІЗАЦІЇ ДЛЯ КИШЕНЬКОВОГО КОМП'ЮТЕРА

Персональний цифровий секретар PDA швидко став особистим інструментом для всіх. З появою служб комунікації для кишенькового комп'ютера є потреба у використанні кишенькового комп'ютера як системи створення підписів.

Кишеньковий комп'ютер можна спроектувати як систему всіх класів: 1DH, 1DM, 2DH і 2DM.

10.1 Вибір обчислювальних механізмів

10.1.1 *Єдиний обчислювальний механізм*

Головна проблема з єдиним обчислювальним механізмом — вимога поділу домена. Апаратні засоби кишенькового комп'ютера й ОС мають врахувати створення й обмеження окремих доменів. Поточні апаратні засоби кишенькового комп'ютера й розробка ОС утруднюють відповідність цим вимогам. Це не перешкоджає кишеньковому комп'ютеру забезпечити такі функціональні можливості в майбутньому.

Після поділу домена кишеньковий комп'ютер має також забезпечити надійний канал між SSCD і SCA. Цей канал може включати апаратний канал, заснований на архітектурі кишенькового комп'ютера, або може бути логічним каналом, використовуючи захист, наданий ОС кишенькового комп'ютера.

Кінцева головна вимога передбачає тривале зберігання SCD. Механізм зберігання має пройти оцінювання [SSCD PP].

10.1.2 *Роздільні обчислювальні механізми*

Поділ SSCD і SCD можна зробити за наявності внутрішнього SSCD або використовуючи змінний SSCD.

Кишеньковий комп'ютер має забезпечити надійний шлях між SSCD і SCA. Це можна зробити із чистим апаратним підключенням, коли SSCD є завжди частиною кишенькового комп'ютера. Коли SSCD — змінна частина кишенькового комп'ютера, це можна зробити логічно, використовуючи шифрування.

Використовуючи змінний SSCD, важливо встановити надійний шлях між SSCD і SCA. Обидві сторони мають перевірити валідність шляху й всіх параметрів установки.

10.2 Міркування про відображення

У кишеньковий комп'ютер інтегровано дисплей, тому він здатен мати застосування SCA, що працює на засобі.

10.2.1 *Засіб відображення повідомлення*

У кишенькового комп'ютера може бути здатність відобразити закінчене повідомлення, щоб підписатися. Відображаючи закінчений документ, SCA є застосування на кишеньковому комп'ютері. Після створення DTBS передачу DTBSR на механізм підписання роблять надійним шляхом або через канал залежно від підключення SCD до кишенькового комп'ютера.

Необхідно забезпечити, щоб застосування SCA могло вирішити, що кишеньковий комп'ютер здатний відображати й повідомляти підписувачу інформацію відповідним чином. Наприклад, якщо в SCA бракує ресурсів, щоб відобразити документ у правильній розрізнювальній здатності або з достатнім кольором, SCA має запобігти операції підписування.

Кишеньковий комп'ютер має створити надійний шлях/канал до SSCD залежно від вибору обчислювальних механізмів.

10.2.2 *Засіб відображення геша*

Як у всіх інших засобах, якщо SCA перебуває в режимі розбивки й відображає повідомлення, виконане на несумісному засобі, SCA має відобразити значення геш-функції на обох дисплеях. Підписувач перевіряє його валідність, обидва засоби відображають те саме значення геш-функції й потім підписувач указує, що підписання може відбутися.

Кишеньковий комп'ютер має створити надійний шлях/канал до SSCD залежно від вибору обчислювальних механізмів.

10.3 Наміри користувача

Кишеньковий комп'ютер забезпечує чудовий механізм, щоб одержати користувацький намір. Екран і засіб уводу даних підключено й можуть бути захищені від втручання. Це дуже просто зробити так, щоб користувач увів послідовність чисел, відображених на екрані, щоб перевірити намір замість того, щоб тільки натиснути мишею або вибрати єдину кнопку.

Автентифікація користувача охоплює ввід даних автентифікації для верифікації підписувача (SVAD), тобто даних автентифікації, наданих користувачем для автентифікації як підписувача.

У дизайні кишенькового комп'ютера розглянуто ефекти приєднання кишенькового комп'ютера. Коли закріплений кишеньковий комп'ютер ураховує ввід інформації від засобів, крім засо-

бу вводу даних кишенькового комп'ютера, він також передбачає відображення інформації щодо певного засобу виводу, крім дисплея кишенькового комп'ютера. Обидва ці випадки не мають допустити руйнування користувацького наміру або неналежне його відображення. Якщо немає гарантії, що властивості безпеки закріплено в розширених засобах, як і у внутрішніх засобах, кишеньковий комп'ютер не допускає їхнє використання в операціях створення підпису.

10.4 Функції платформи SSCD

10.4.1 *Персоналізація*

Персоналізація охоплює генерацію SCD/SVD і імпорт SCD або експорт SVD за потреби. Є дві можливості виконати генерацію ключів:

— генерація ключа, виконана поза SSCD. Це означає, що SSCD має тип 2, з вимогою надійного каналу для імпорту SCD. Тоді генерацію ключа зазвичай виконує виготовник SSCD або кишенькового комп'ютера. Кишеньковий комп'ютер тоді постачають користувачеві з попередньо згенерованими ключами;

— генерація ключа в SSCD безпосередньо. Кишеньковий комп'ютер з убудованою генерацією ключа має SSCD типу 3 згідно [SSCD PP]. Виготовник SSCD, виготовник кишенькового комп'ютера чи користувач безпосередньо після одержання кишенькового комп'ютера може ініціювати генерацію ключа.

Другий крок персоналізації — генерація сертифіката — розглянуто в 7.1.3.

10.4.2 *Автентифікація користувача*

У кишенькового комп'ютера є повноцінний увід й засоби відображення, тому користувацька автентифікація використовує у своїх інтересах ці засоби. Користувацька автентифікація має використовувати фрази допуску принаймні і можливе використання другого фактора автентифікації.

Надійний шлях/канал між засобом уводу даних і SSCD має гарантувати конфіденційність фрази допуску або іншої інформації автентифікації.

У разі множинних невдач автентифікації здійснюють політику блокування SSCD.

10.4.3 *Надійні шляхи і канали*

Усі системи вимагають принаймні:

— для SSCD типу 2 надійний канал для імпорту SCD в SSCD;

— для SSCD типу 3 надійний канал для експорту SVD в CGA;

— для окремих обчислювальних засобів надійний шлях між засобом уводу даних і SSCD;

— для єдиного обчислювального засобу надійну лінію зв'язку між засобом уводу даних і SSCD. Тип лінії зв'язку (шлях або канал) залежить від конструкції кишенькового комп'ютера й того, як засіб уводу даних підключено до системи.

Система класу 1DH вимагає принаймні:

— надійний канал між віддаленими частинами застосування SCA. Цей шлях — точка входу DTBSR у систему;

— надійний канал між SCA, що відображає геш засобу й SSCD.

Система класу 2DH вимагає принаймні:

— надійний канал між віддаленими частинами застосування SCA. Цей шлях — точка входу DTBSR у систему;

— надійний канал між SCA, що відображає геш засобу й SSCD.

Система класу 1DM вимагає принаймні:

— надійний канал між SCA і SSCD.

Система класу 2DM вимагає принаймні:

— надійний шлях між SCA і SSCD.

11 НАСТАНОВИ З РЕАЛІЗАЦІЇ ДЛЯ ПК

Протягом довгого часу ПК був найбільш використовуваним засобом для електронної комерції. Уже сьогодні багато застосувань створюють підписані повідомлення в середовищі ПК: поштові програми, доповнення до браузерів і застосування форм. Потужність ПК забезпечує швидкі обчислення й різноманітний набір засобів.

ПК можна використовувати, щоб створити всі чотири класи SCS.

11.1 Вибір обчислювального механізму

11.1.1 *Єдиний обчислювальний механізм*

Головна проблема з єдиним обчислювальним механізмом — вимога поділу домена. Апаратні засоби ПК і ОС мають врахувати створення й обмеження окремих доменов. Поточні апаратні засоби ПК і розробка ОС ускладнюють відповідність цим вимогам. Це не перешкоджає ПК надати ці функціональні можливості в майбутньому.

Після поділу домена ПК має також забезпечити надійний канал між SSCD і SCA. Цей канал може включати апаратний канал, заснований на архітектурі ПК, або може бути логічним каналом, використовуючи засоби захисту, надані ОС ПК.

Кінцева головна вимога має передбачити тривале зберігання SCD. Механізм зберігання має пройти оцінювання [SSCD PP].

11.1.2 *Роздільні обчислювальні механізми*

Поділ SSCD і SCD можна зробити за наявності внутрішнього SSCD або вставляючи змінний SSCD у слот.

ПК має забезпечити надійний шлях між SSCD і SCA. Це може зробити чисте апаратне підключення, коли SSCD є завжди частина ПК. Коли SSCD — змінна частина ПК, його можна реалізувати логічно, використовуючи шифрування.

Використовуючи змінний SSCD, важлива установка надійного шляху між SSCD і SCA. Обидві сторони мають бути здатні перевірити валідність шляху й всіх параметрів установки.

11.2 Міркування про відображення

У ПК інтегровано дисплей, тому він здатен мати застосування SCA, що працює на засобі.

11.2.1 *Засіб відображення повідомлення*

ПК здатний відобразити закінчене повідомлення для підписання. Відображаючи закінчене повідомлення, SCA є застосування ПК. Після створення DTBS передачу DTBSR на механізм підписання роблять надійним шляхом або через канал залежно від підключення SCD до ПК.

Необхідно забезпечити, щоб застосування SCA вирішувало, що ПК може відобразити й повідомити інформацію підписувачу відповідним чином. Наприклад, якщо в SCA бракує ресурсів для відображення документа в правильній роздільній здатності або в прийнятному кольорі, SCA має запобігти операції підписання.

ПК має створити надійний шлях/канал до SSCD залежно від вибору обчислювальних засобів.

11.2.2 *Засіб відображення геша*

Як у всіх інших засобах, якщо SCA перебуває в режимі розбивки й відображає повідомлення, відображене на певному несумісному засобі, SCA має відобразити значення геш-функції на обох дисплеях. Підписувач перевіряє валідність цього, обидва засоби відображають одне значення геш-функції й потім підписувач дає вказівку, що підписання може відбутися. ПК має створити надійний шлях/канал до SSCD залежно від вибору обчислювальних засобів.

11.3 Наміри користувача

ПК забезпечує чудовий механізм для одержання наміру користувача. Екран і засіб уводу даних підключені й можуть бути захищені від втручання. Дуже просто зробити так, щоб користувач увів послідовність чисел, відображених на екрані, щоб верифікувати намір замість того, щоб тільки натиснути мишею або вибрати єдину кнопку.

Автентифікація користувача охоплює ввід даних автентифікації верифікації підписувача, тобто даних автентифікації, наданих користувачем для автентифікації як підписувача.

11.4 Функції платформи SSCD

11.4.1 *Персоналізація*

Персоналізація охоплює генерацію SCD/SVD і імпорт SCD або експорт SVD за потреби. Є дві можливості виконати генерацію ключів:

— генерація ключа, виконана поза SSCD. Це означає, що SSCD має тип 2, з вимогою надійного каналу для імпорту SCD. Тоді генерацію ключа зазвичай виконує виготовник SSCD або ПК. ПК тоді постачають користувачеві з попередньо згенерованими ключами;

— генерація ключа в SSCD безпосередньо. ПК із убудованою генерацією ключа має тип 3 SSCD згідно [SSCD PP]. Виготовник SSCD, виготовник ПК або користувач безпосередньо після одержання ПК можуть ініціювати генерацію ключа.

Другий крок персоналізації — генерація сертифіката — описано в 7.1.3.

11.4.2 *Автентифікація користувача*

У ПК є повноцінні ввід й засоби відображення, тому автентифікація користувача використовує у своїх інтересах ці засоби. Ця автентифікація має використовувати фрази доступу принаймні і, якщо можливо, — другий фактор автентифікації. Здатність ПК підключати додаткові засоби збільшує гарантію під час автентифікації користувача. Наприклад, до ПК можна прикріпити зчитувач відбитків пальців так, щоб фразу доступу перевіряти з відповідною контрольною сумою файлу для користувача.

Надійний шлях/канал між засобом уводу даних і SSCD гарантує конфіденційність фрази проходу або іншої інформації автентифікації.

У разі множинних невдач автентифікації здійснюють політику блокування SSCD.

11.4.3 *Надійний шлях і канали*

Усі системи вимагають принаймні:

— для SSCD типу 2 надійний канал для імпорту SCD у SSCD;

— для SSCD типу 3 надійний канал для експорту SVD у CGA;

— для окремих обчислювальних засобів надійний шлях між засобом уводу даних і SSCD;

— для єдиного обчислювального засобу надійна лінія зв'язку між засобом уводу даних і SSCD. Тип лінії зв'язку (шлях або канал) залежить від конструкції ПК і того, як засіб уводу даних підключено до системи;

— надійний канал між обчислювальним механізмом і засобом виводу.

Система класу 1DH вимагає принаймні:

— надійний канал між відділеними частинами застосування SCA. Цей шлях — точка входу DTBSR у систему;

— надійний канал між SCA, що відображає геш засобу й SSCD.

Система класу 2DH вимагає принаймні:

— надійний шлях між відділеними частинами застосування SCA. Цей шлях — точка входу DTBSR у систему;

— надійний шлях між SCA, що відображає геш засобу й SSCD.

Система класу 1DM вимагає принаймні:

— надійний канал між SCA і SSCD.

Система класу 2DM вимагає принаймні:

— надійний шлях між SCA і SSCD.

12 ПОСЛУГИ ПІДПИСУВАННЯ

Можна спроектувати систему послуг підписання, де SCD всіх користувачів містить велике SSCD, з яким можуть з'єднатися багато користувачів. Одним екземпляром класу є вузол мережі, що підписує повідомлення для підписувача, коли надходить повідомлення й належна автентифікація користувача.

Цей проект не заборонено згідно з Директивою й є технічно можливий. Однак висновок поточної робочої групи не фіксує серйозні технічні проблеми, які має цей проект.

По-перше, [SSCD PP] не відповідає SSCD, що використовував би послугу підписання. Нові PP зобов'язані звертатися до проблем належного поділу інформації SCD, користувацької автентифікації, користувацьких намірів і відображення повідомлень.

Іншою головною проблемою, що має вирішити послуга підписання, є створення надійного шляху між користувачем і SCA і надійного шляху між SCA і SSCD. Для послуги підписання надійний шлях, імовірно, доведеться встановити по відкритому Інтернету. Крім того, здатність належним чином дістати згоду користувача використовувати SCD зажадала б надійного шляху між SSCD і поточною платформою, де користувач постійно перебуває.

Ці проблеми технічно здійсненні; однак вибір обмежено з поточного покоління апаратних засобів і програмного забезпечення.

ДОДАТОК І
(довідковий)

ПОРІВНЯННЯ ПРОФІЛІВ ЗАХИСТУ

У 6.2 ідентифіковано багато зв'язаних профілів захисту, яким конструктор хотів би відповідати на додаток до [SSCD PP]. Кілька випадків, які можна було б розглянути щодо комбінації оцінювання цих PP, обговорено в 6.2. У цьому додатку наведено деталі зв'язаних PP. Тому в AI.1 наведено порівняння об'єктів безпеки, які накладають різні PP. В AI.2 описано вибір SFR у різних PP_S.

AI.1 Порівняння об'єктів безпеки

Цей розділ проводить порівняння між об'єктами безпеки [SSCD PP] та Eurosmart PP [PP 0010] і [PP 0002] (відповідно PP [SCSUG]), відповідаючи на запитання: «Якщо потрібно було написати об'єкти безпеки, вимагаючи відповідності з [SSCD PP] і Eurosmart [PP 0010] (resp. [PP 0002] або [SCSUG]) PP, які об'єкти безпеки кожного допомогли б гарантувати об'єкти безпеки один одного?».

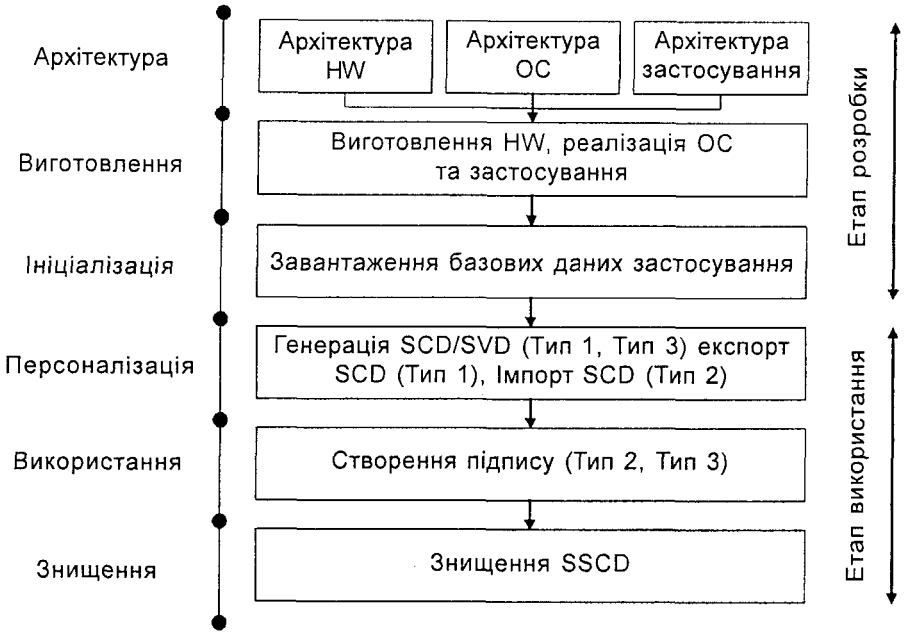
Для кожного об'єкта безпеки відповіді на це питання можуть бути досить прямими або, що частіше, залежати від додаткових припущень або тверджень про розробку або наявність властивостей SSCD. У контенті цього розділу виділено питання, на які потрібно відповісти, намагаючись скласти ST, що відповідає обом Eurosmart [PP 0010] (resp. [PP 0002] або [SCSUG]) PP_S.

У випадках, розглянутих у цьому розділі, необхідні загальні припущення, щоб окреслити сценарії композиції. Додаткові припущення заявлені нижче для кожного випадку, як відповідні.

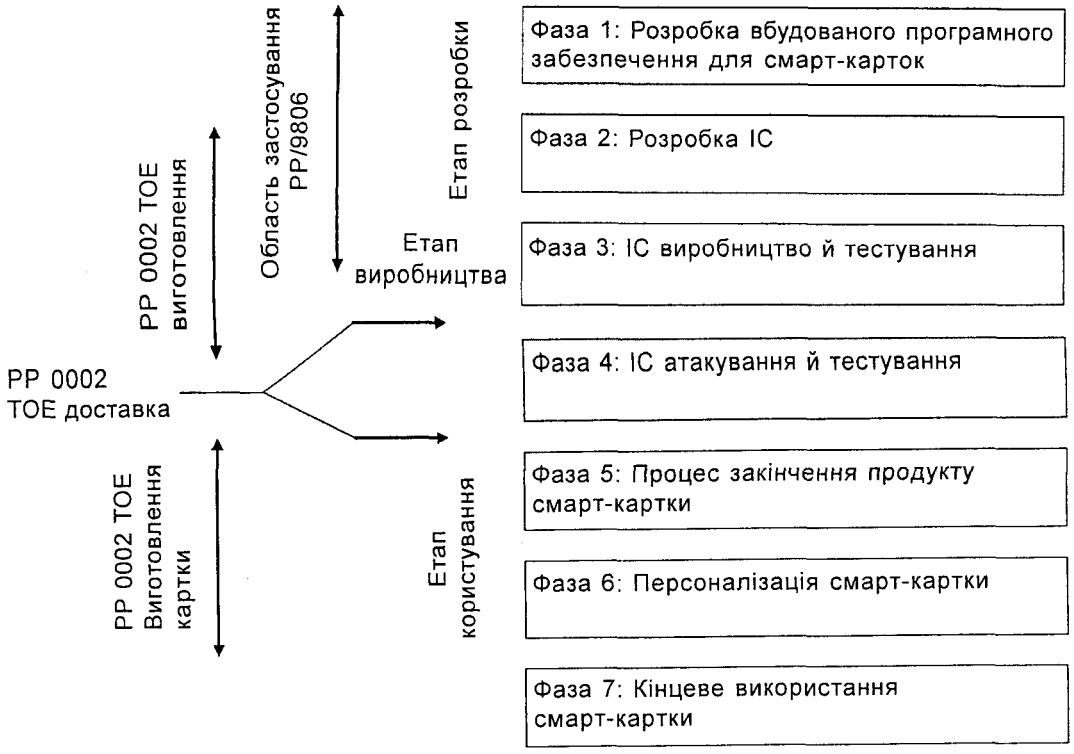
Розглянутий SSCD (його тип немає значення) здійснено на смарт-картці й призначено для вставлення й використання в терміналі (наприклад, пристрій прийняття карток CAD). Отже, фаза персоналізації SSCD відповідає фазі персоналізації смарт-картки, а фаза використання й знищення SSCD — закінченню використання смарт-картки. Автентифікацію підписувача виконує зовнішній засіб, підключений (можливо, як частина) до термінала.

Оскільки певне застереження треба надати щодо цих різних моделей життєвого циклу, поданих у різних PP і розглянутих у цьому розділі, рисунок AI.1 ілюструє різні моделі життєвого циклу [PP] і Eurosmart PP ([PP 9806] і [PP 0010], resp. [PP 0002]).

Програмне забезпечення, що встановлює та готує SSCD застосування, можна спроектувати разом із убудованим програмним забезпеченням або розробити у незалежному життєвому циклі з подальшою інтеграцією у смарт-картку.



[SSCD PP] Модель життєвого циклу



Eurosmart PP Модель життєвого циклу (спрощена) [PP 9806]/ [PP 0010], resp. [PP 0002]

Рисунок AI.1

AI.1.1 *SSCD проти Eurosmart PP0010*

AI.1.1.1 *Сфера застосування TOE*

Профіль захисту Eurosmart [PP 0010] визначає вимоги для мультиприкладної платформи смарт-картки, вбудованої в інтегральну схему, так само як для її життєвого циклу, визначаючи фази, пронумеровані від 1 (впроваджена розробка програмного забезпечення) до 7 (закінчен-

ня використання). Платформа включає операційну систему, завантажуваний інтерфейс прикладної системи, IC спеціалізованого програмного забезпечення (поза TOE, але підлеглий вимогам [PP 9806]) і, можливо, рідні застосування.

Операційна система платформи підтримує завантаження застосування протягом персоналізації або на фазах кінцевого використання (фази 6 і 7 відповідно). Розробку й включення рідних застосувань можна пророкувати; вони вже виконані як фаза 1 і включені у фазу 3 (виробництво IC), 6 (персоналізація) або 7 (кінцеве використання).

Взаємодію застосувань з операційною системою обмежено за допомогою інтерфейсу завантаженої прикладної системи, а в рідних застосуваннях може бути прямий доступ до операційної системи.

Проблеми безпеки мають справу з об'єктами безпеки, заявленими в цьому PP, їх можна одержати в підсумку:

— підробка або пасивне прослуховування функцій безпеки TOE, даних TSF і користувацьких (завантажених і рідних застосувань) даних,

— захист від імітації,

— безпека розробки, усунення недоліків,

— мультиприкладне керування:

- відмовостійке завантаження,
- керування доступом у завантаженні застосування й операціях видалення,
- керування конфіденційністю, цілісністю, дійсністю завантажених застосувань,
- видалення залишкової інформації, асоційованої з вилученими застосуваннями,
- сегрегація й стримування ресурсів між застосуваннями.

Питання, на які потрібно відповісти:

— чи дійсно SSCD — рідне або завантажене застосування? На якій фазі воно вставлено? (життєвий цикл на рис. 5 в CWA, на рис. 3 в SSCD PP відповідно швидше вказує рідне застосування, завантажене виробником картки);

— SSCD середовище функціонування (у значенні CC) починається з фази 6, а Eurosmart проектує його на фази 4-7. Потрібно бути обережним у контексті (SSCD або Eurosmart), читаючи такі терміни як «розробка», «операція» чи «життєвий цикл»;

— тут є додаткові застосування (завантажені чи рідні), яким дозволено перебувати разом із SSCD? Дозволено завантаження застосувань на фазі кінцевого використання?

— чи залежить знищення SSCD від операцій видалення застосування, передбачуваних Eurosmart PP, або це фізичне знищення (SSCD PP не погоджується із цим пунктом, однак знищення SCD обговорено докладно в 5.2.4 цього стандарту)?

— чи допускає автентифікацію користувача безпечний протокол комунікації з терміналом картки? Інші контрольні точки ідентифіковано нижче як умови для відповідності об'єктам безпеки.

AI.1.1.2 *Порівняння об'єктів безпеки*

Немає відповідності між двома наборами об'єктів безпеки. Загальна підмножина має справу з фізичним і електронним захистом, вимогами життєвого циклу й безпечною комунікацією з терміналом. Є проблема із цілями безпеки, які мають справу із втручанням.

Деякі цілі безпеки для середовища Eurosmart PP частково відповідають об'єктам безпеки для TOE від SSCD PP. Це означає, що відповідність із SSCD PP допомагає виконувати вимоги/припущення до середовища з позицій Eurosmart PP. Щоб зазначити об'єкти безпеки для середовища, їхні префікси змінено з 'O.' на 'OE.'; для цілей TOE [SSCD PP] використано префікс 'OT'.

Об'єкт OT.EMSEC_Design (від SSCD PP) повністю відповідає об'єкту O.SIDE (від Eurosmart PP).

Об'єкт OT.Init може відповідати OE.INIT_ACS за умови, що область видимості останнього об'єкта («дані ініціалізації мають бути доступні тільки авторизованим особам (фізичними, персональними, організаційними, технічними процедурами).») ефективно відповідають примітці SCD/SVD, що SCD не можна постачати жодній особі й також SCD не можна вважати даними ініціалізації, як визначено в [PP 9911]. Об'єкт OT.Lifecycle_Security відповідає O.FLAW за умови усунення помилок.

Об'єкт OT.SCD_Secrecy може відповідати O.DIS_MECHANISM2 за умови, що область застосування останнього об'єкта («захист механізмів безпеки ES від несанкціонованого розкриття») має на увазі нерозголошення SSCD.

Об'єкт OT.Tamper_ID перебуває в прямому протиріччі з O.TAMPER_ES, а O.Tamper_Resistance повністю відповідає йому. Протиріччя є між 'запобіганням' і 'виявленням' втручання. Певною мірою розходження відбувається через [SSCD PP], визначеного як нейтральний до технології, а Eurosmart PP строго стосуються смарт-карток.

Об'єкт OT.DTBS_Integrity_TOE відповідає O.MOD_MEMORY (наскільки допускає захист DTBS-подань, збережених у межах TOE) і може відповідати OE.USE_DIAG (наскільки допускає захист DTBS-подань між SCA і SSCD). Потрібно розглянути вимоги [SSCD PP], щоб TOE зберіг цілісність DTBS-подання, а O.USE_DIAG — об'єкт вимоги.

Об'єкт OT.Sigy_Sig може відповідати OE.USE_DIAG за умови, що «безпечні протоколи комунікації між смарт-карткою й терміналом», до якого звертається цей останній об'єкт, мають на увазі автентифікацію користувача. Зазначимо, що автентифікація користувача не є настільки явною в Eurosmart PP, як у [SSCD PP].

Об'єкт OE.HI_VAD може відповідати OE.USE_DIAG за умови, що «безпечні протоколи комунікації між смарт-карткою й терміналом», до якого звертається цей останній об'єкт, мають на увазі автентифікацію користувача й відповідний захист (конфіденційність і цілісність) даних автентифікації VAD для передачі між терміналом і смарт-карткою.

AI.1.2 *SSCD проти Eurosmart PP0002*

AI.1.2.1 *Сфера застосування TOE*

Профілі захисту [PP 0002] визначають вимоги для платформи смарт-картки IC, що складається із процесора, компонентів безпеки, портів уводу-виводу й пам'яті (енергозалежної й такої, що не руйнується). Програмне забезпечення покрите як „спеціалізоване програмне забезпечення» (убудоване програмне забезпечення) для розширення, оскільки воно існує внаслідок постачання виготовника IC. Також PP головним чином зацікавлені в апаратному дизайні й стадіях розробки.

[PP 0002] стосуються Eurosmart PP у деякому розумінні, визначаючи ті самі «сім фаз» моделі життєвого циклу, обговореної в AI.1.1.1.

PP визначають користувацькі дані як первинний актив, захищений (крім таких інших, як убудоване програмне забезпечення, дані ініціалізації, дані попередньої персоналізації). Тому витік користувацької інформації підкреслено як загрозу, яку необхідно запобігти. Крім того, враховано якість генераторів випадкових чисел. Вторинні активи також покривають дизайн IC і інформацію фізичної реалізації.

[PP 0002] визначають три мети безпеки високого рівня:

— SG1: підтримати цілісність користувацьких даних і убудованого програмного забезпечення;

— SG2: підтримати конфіденційність користувацьких даних і убудованого програмного забезпечення;

— SG3: забезпечити випадкові числа.

AI.1.2.2 *Порівняння об'єктів безпеки*

Порівнюючи об'єкти [SSCD PP] і [PP 0002], маємо певну відповідність, де користувацькі дані, насамперед SCD, мають бути захищені. Також [PP 0002] надає апаратну платформу для SSCD (подібно [PP 9806]).

Об'єкт OT.EMSEC_Design [SSCD PP] відповідає об'єкту O.Leak_Inherent і O.Leak_Forced в [PP 0002].

OT.SCD_Secrecy [SSCD PP] відповідає O.Leak_Inherent і O.Phys-Probing.

OT.Tamper_ID і OT.Tamper_Resistance [SSCD PP] стосуються O.Phys-Probing і O.Phys-Manipulation [PP 0002].

OT.Init для [SSCD PP] частково відповідає O.Identification за допомогою підтримки попередньої персоналізації через дані ініціалізації для ідентифікації TOE.

AI.1.3 *SSCD проти SCSUG*

AI.1.3.1 *Область застосування TOE*

Профіль захисту [SCSUG] визначає вимоги для платформи смарт-картки, убудованої в інтегральну схему, включаючи операційну систему, на якій додаткові застосування можна завантажити на фазі кінцевого використання.

На противагу Eurosmart 0010 PP [PP 0010], життєвий цикл смарт-карток не враховано у поясненні тверджень об'єктів безпеки (хоча довідковий додаток B.2 надає багато інформації про це). Отже, точно не зазначено в об'єктах безпеки факт розробки (рідних) застосувань і вставлення перед кінцевим використанням і набором відповідних вимог безпеки.

Середовище функціонування відповідає фазі кінцевого використання. Об'єкти безпеки для TOE звертаються винятково до цієї фази.

Проблеми безпеки мають справу з об'єктами безпеки, заявленими в цьому PP, і можна їх підсумувати:

— підробка чи пасивне прослуховування функцій безпеки TOE, даних TSF і користувацьких даних,

— дотримання стандартів криптографії й інструкцій,

— відмовостійкість,

— керування доступом до користувацьких даних і даних TSF,

— керування доступом до функцій життєвого циклу,

— сегрегація між застосуваннями,

— ревізія можливостей,

— захист від методів грубої сили,

— захист від повторюваних атак,

— безпечна комунікація з CAD.

Контрольні точки ідентифіковано нижче як умови для відповідності цілей безпеки.

AI.1.3.2 *Порівняння об'єктів безпеки*

Є суттєва відповідність між PP SCSUG і SSCD PP, ніж з Eurosmart PP, тому що пристосування фаз життєвого циклу смарт-карток перебуває в кращій відповідності. Природно, SCSUG не звертається до SSCD-визначених об'єктів, але є зв'язок щодо загальних мотивів як доказ втручання, логічний захист, опір «атакам грубої сили», керування відкритими ключами або користувацькою автентифікацією.

Один привід для занепокоєння, проте є фактом, що пакет гарантій PP SCSUG включає тільки складовий AVA_VLA.3, а SSCD PP включає AVA_VLA.4. Пояснення для вибору AVA_VLA.3 ([SCSUG]) розглянуто як спірне. Крім того, PP SCSUG передають під мандат SOF-високий рівень для всіх «статистичних або імовірнісних механізмів в TOE», але не нормативним способом [SCSUG]:

Компонент AVA_VLA.4 вибирають, щоб вимагати відповідності з [SSCD PP]. Сила функціональних вимог до відповідних механізмів безпеки має бути високою, відповідно до розглянутої вище вдалої практики.

Об'єктивно OT.EMSEC_Design відповідає O.I_Leak і O.Env_Strs.

Об'єктивно OT.Init може відповідати O.Life_Cycle через генерацію SCD/SVD, що є командою, залежною від життєвого циклу в термінах [SCSUG]. У рамках цього об'єкта безпеки єдині команди, доступні для SCD і операцій генерації SVD, явно пов'язані з фазою персоналізації застосування SSCD. Також OT.Init може відповідати O.Set_Up.

Об'єктивно OT.SCD_Secrecy може відповідати O.Brute-Force настільки, наскільки SCD відповідає меті цього об'єкта безпеки, який відкидає SCD у пошуку атаки грубої сили.

Об'єктивно OT.Tamper_ID відповідає OE.Tamper, але цей об'єкт безпеки середовища TOE також надає політику підтримки організаційної безпеки, мета якої є перевірка носіїв відповідним персоналом.

Об'єктивно OT.DTBS_Integrity_TOE відповідає O.Log_Prot (наскільки захист подано DTBS, збереженого в межах TOE) і може відповідати O.Sec_Com (наскільки захист подано DTBS між SCA і SSCD.

Об'єктивно OT.Sigy_Sig може відповідати O.Sec_Com, де надійний шлях надано [SCSUG], а необхідний опір атакам забезпечує O.Brute-Force.

Об'єктивно OT.Sig_Secure може відповідати O.Crypt, O.Brute— Force або O.Unlink.

Об'єктивно OE.CGA_QCert може відповідати OE.Key_Supp.

Об'єктивно OE.SVD_Auth_CGA може відповідати OE.CAD_Sec-Com і/або OE.Key_Supp, залежно від деталей політики керування SVD/сертифіката.

Об'єктивно OE.HI_VAD може відповідати O.Sec_Com, коли надано надійний шлях [SCSUG].

AI.2 Порівняння функціональних вимог безпеки

AI.2.1 *Атрибут безпеки FAU*

Коментарі

[SSCD PP] і [PP 9806] не покривають функціональні можливості аудиту, а інші PP роблять це. Більш точно, Eurosmart PP (у термінах [PP 9806], [PP 9911] і [PP 0010]) інтегрує вимоги безпеки для генерації тривог безпеки й аналізу потенційного порушення безпеки.

[PP 0002] визначає сімейство для можливості зберігання даних аудиту.

Функціональні вимоги безпеки		PP SSCD			PP9806	PP0002	PP9911	PP0010	PP SCUG
		T1	T2	T3					
Тривоги безпеки	FAU_ARP.1.1							X	X
Генерація списку аудиту списку (PP UG)	FAU_LST.1.1								X
	FAU_LST.1.2								X
Аналіз потенційного порушення	FAU_SAA.1.1				X		X		X
	FAU_SAA.1.2				X		X		X
] Зберігання даних аудиту [PP 0002]	FAU_SAS.1.1					X			
Вибірковий аудит	FAU_SEL.1.1								X
Захищене зберігання аудиторського сліду	FAU_STG.1.1								X
	FAU_STG.1.2								X
Дія у разі можливої втрати даних аудиту	FAU_STG.3.1								X

AI.2.2 *Криптографічна підтримка FCS*

Функціональні вимоги безпеки		PP SSCD			PP9806	PP0002	PP9911	PP0010	PP SCUG
		T1	T2	T3					
Генерація криптоключа	FCS_CKM.1.1	X		X					X
Розподіл криптоключа	FCS_CKM.2.1	E	E	E					
Доступ до криптоключа	FCS_CKM.3.1	E	E	E			X	X	X
Знищення криптоключа	FCS_CKM.4.1	X	X	X			X	X	
Криптооперація	FCS_COP.1.1	X	X	X			X	X	X
Якісні показники випадкових чисел [PP 0002]						X			

Коментарі

Вимога безпеки про доступ до криптоключа перебуває під відповідальністю IT-середовища TOE (CGA для генерації сертифіката).

[PP 0002] визначає конкретне сімейство для якісних показників генераторів випадкових чисел.

AI.2.3 *Користувацький захист даних FDP*

Функціональні вимоги безпеки		PP SSCD			PP9806	PP0002	PP9911	PP0010	PP SCUG
Керування доступом підмножини	FDP_ACC.1.1	X	X	X					X

Функціональні вимоги безпеки		PP SSCD			PP9806	PP0002	PP9911	PP0010	PP SCUG
Повне керування доступом	FDP_ACC.2.1				X		X	X	
	FDP_ACC.2.2				X		X	X	
Керування доступом, засноване на атрибутах безпеки	FDP_ACF.1.1	X	X	X	X		X	X	X
	FDP_ACF.1.2	X	X	X	X		X	X	X
	FDP_ACF.1.3	X	X	X	X		X	X	X
	FDP_ACF.1.4	X	X	X	X		X	X	X
Базова автентифікація даних	FDP_DAU.1.1						X	X	
	FDP_DAU.1.2						X	X	
Експорт користувацьких даних без атрибутів безпеки	FDP_ETC.1.1	X	X	X			X	X	X
	FDP_ETC.1.2	X	X	X			X	X	X
інформаційних даних підмножини	FDP_IFC.1.1				X	X			X
Прості атрибути безпеки	FDP_IFF.1.1				X				X
	FDP_IFF.1.2				X				X
	FDP_IFF.1.3				X				X
	FDP_IFF.1.4				X				X
	FDP_IFF.1.5				X				X
	FDP_IFF.1.6				X				X
Імпорт користувацьких даних без атрибутів безпеки	FDP_ITC.1.1		X	X			X	X	X
	FDP_ITC.1.2		X	X			X	X	X
	FDP_ITC.1.3		X	X			X	X	X
Основний внутрішній захист передачі	FDP_ITT.1.1					X			
Захист підмножини залишкової інформації	FDP_RIP.1.1	X	X	X			X	X	X
Основне відкочування	FDP_ROL.1.1							X	
	FDP_ROL.1.2							X	
Моніторинг цілісності збережених даних	FDP_SDI.1.1				X				
Моніторинг цілісності збережених даних і дій	FDP_SDI.2.1		X	X			X	X	
	FDP_SDI.2.2		X	X			X	X	
Конфіденційність базових даних обміну	FDP_UCT.1.1	X	X						
Цілісність обміну даними	FDP_UIT.1.1	X	X	X					X
	FDP_UIT.1.2	X	X	X					X

Коментарі

[SSCD PP] враховує цілісність даних, коли відбувається обмін з іншими засобами.

[SSCD PP] не покриває відкочування функцій у разі помилки, але управляє цілісністю даних.

[SSCD PP] і [SCSUG] обидва вимагають тільки керування доступом підмножини до користувацьким даних, а Eurosmart PP вимагає закінченого керування доступом.

AI.2.4 *Ідентифікація FIA та автентифікація*

Функціональні вимоги безпеки		PP SSCD			PP9806	PP0002	PP9911	PP0010	PP SCUG
Обробка невдач автентифікації	FIA_AFL.1.1	X	X	X			X	X	X
	FIA_AFL.1.2	X	X	X			X	X	X
Користувацьке визначення атрибутів	FIA_ATD.1.1	X	X	X	X		X	X	X
Синхронізація автентифікації	FIA_UAU.1.1	X	X	X			X	X	X
	FIA_UAU.1.2	X	X	X			X	X	X
Користувацька автентифікація перед будь-якою дією	FIA_UAU.2.1				X				
Незабута автентифікація	FIA_UAU.3.1						X		
	FIA_UAU.3.2						X		
Механізми автентифікації єдиного використання	FIA_UAU.4.1						X	X	
Захищений розпізнавальний зворотний зв'язок	FIA_UAU.7.1								X
Синхронізація ідентифікації	FIA_UID.1.1	X	X	X			X	X	X
	FIA_UID.1.2	X	X	X			X	X	X
Користувацька ідентифікація перед будь-якою дією	FIA_UID.2.1				X				
Зв'язування з користувацьким об'єктом	FIA_USB.1.1						X	X	

Коментарі

Без коментарів.

AI.2.5 *Керування безпекою FMT*

Функціональні вимоги безпеки		PP SSCD			PP9806	PP0002	PP9911	PP0010	PP SCUG
Обмежені можливості [PP 0002]	FMT_LIM.1.1					X			
Обмеження придатності [PP 0002]	FMT_LIM.2.1					X			
Керування поведінкою функцій безпеки	FMT_MOF.1.1		X	X	X		X	X	X
Керування атрибутами безпеки	FMT_MSA.1.1	X	X	X	X		X	X	X
Безпечні атрибути безпеки	FMT_MSA.2.1	X	X	X			X	X	X

Функціональні вимоги безпеки		PP SSCD			PP9806	PP0002	PP9911	PP0010	PP SCUG
Статична ініціалізація атрибутів	FMT_MSA.3.1	X	X	X	X		X	X	X
	FMT_MSA.3.2	X	X	X	X		X	X	X
Керування даними TSF	FMT_MTD.1.1		X	X			X	X	X
Керування обмеженнями даних TSF	FMT_MTD.2.1							X	X
	FMT_MTD.2.2							X	X
Скасування	FMT_REV.1.1								X
	FMT_REV.1.2								X
Ролі безпеки	FMT_SMR.1.1	X	X	X	X		X	X	
	FMT_SMR.1.2	X	X	X	X		X	X	

Коментарі

[SSCD PP] покриває ті самі вимоги, що й Eurosmart PP [PP 9911] [PP 0010]. [PP 9806] покриває ті самі вимоги, що й [SSCD PP], за винятком FMT_MTD.1 (керування даними TSF).

[PP 0002] задають конкретне сімейство, обмежуючи можливість і придатність TSF власній меті. Це фактично — єдина необхідна функція керування безпекою [PP 0002].

Є розбіжність із PP SCUG, що стосується скасування атрибутів безпеки будь-яких даних, покритих тільки TOE.

AI 2.6 *Приватність FPR*

Функціональні вимоги безпеки		PP SSCD			PP9806	PP0002	PP9911	PP0010	PP SCUG
		T1	T2	T3					
Неспостережуваність	FPR_UNO.1.1				X		X	X	

Коментарі

Див. коментар про FPT_EMSEC в AI.2.7.

AI 2.7 *FPT-захист TSF*

Функціональні вимоги безпеки		PP SSCD			PP9806	PP0002	PP9911	PP0010	PP SCUG
		T1	T2	T3					
Абстрактне машинне тестування	FPT_AMT.1.1	X	X	X					
Випускання TOE [SSCD PP]	FPT_EMSEC.1.1	X	X	X					
	FPT_EMSEC.1.2	X	X	X					
Відмова зі збереженням безпечного стану	FPT_FLS.1.1	X	X	X		X	X	X	X
Виявлення Inter-TSF модифікації	FPT_ITI.1.1								X
	FPT_ITI.1.2								X
Основний внутрішній захист передачі даних TSF	FPT_ITT.1.1					X			
Пасивне виявлення фізичної атаки	FPT_PHP.1.1	X	X	X					
	FPT_PHP.1.2	X	X	X					

Функціональні вимоги безпеки		PP SSCD			PP9806	PP0002	PP9911	PP0010	PP SCUG
		T1	T2	T3					
Повідомлення про фізичну атаку	FPT_PHP.2.1				X				
	FPT_PHP.2.2				X				
	FPT_PHP.2.3				X				
Опір фізичній атаці	FPT_PHP.3.1	X	X	X	X	X	X	X	X
Автоматизоване відновлення без недоречної втрати	FPT_RCV.3.1								X
	FPT_RCV.3.2								X
	FPT_RCV.3.3								X
	FPT_RCV.3.4								X
Функціональне відновлення	FPT_RCV.4.1							X	X
Виявлення перегравання	FPT_RPL.1.1								X
	FPT_RPL.1.2								X
Non-bypassability TSP	FPT_RVM.1.1							X	X
	FPT_SEP.1.1					X	X	X	X
	FPT_SEP.1.2					X	X	X	X
Послідовність даних Inter-TSF	FPT_TDC.1.1						X	X	
	FPT_TDC.1.2						X	X	
Тестування TSF	FPT_TST.1.1	X	X	X			X	X	X
	FPT_TST.1.2	X					X	X[1)]	X
	FPT_TST.1.3	X	X	X			X	X[2)]	X

[1)] Ці дві вимоги відсутні в [PP 0010], але здається, це — помилка PP.
[2)] Ці дві вимоги відсутні в [PP 0010], але здається, це — помилка PP.

Коментарі
SFR FPT_EMSEC створено для [SSCD PP].
[SSCD PP] не враховує функції відновлення.
[SSCD PP] тільки один вимагає пасивного виявлення фізичної атаки.

AI.2.8 *Використання ресурсу FRU*

Функціональні вимоги безпеки		PP SSCD			PP9806	PP0002	PP9911	PP0010	PP SCUG
		T1	T2	T3					
Обмежена відмовостійкість	FRU_FLT.2.1					X			
Максимальні квоти	FRU_RSA.1.1							X	

Коментарі
Відмовостійкість вимагає тільки [PP 0002].
[PP 0010] стосуються мультизастосування, а FRU_RSA проілюстровано.

AI.2.9 *FTP надійні шляхи/канали*

Функціональні вимоги безпеки		PP SSCD			PP9806	PP0002	PP9911	PP0010	PP SCUG
		T1	T2	T3					
Inter-TSF довіра каналу	FTP_ITC.1.1	X	X	X					X
	FTP_ITC.1.2	X	X	X					X
	FTP_ITC.1.3	X	X	X					X
Надійний шлях, якому довіряють	FTP_TRP.1.1		X	X					
	FTP_TRP.1.2		X	X					
	FTP_TRP.1.3		X	X					

Коментарі

Важливість надійних каналів обумовлено тим, що шлях — основне розходження з іншими PPs, як зазначено в таблицях. Для детального обговорення надійних шляхів/каналу, яким довіряють, див. 5.2.1.

Код УКНД 03.160; 35.040; 35.100.05

Ключові слова: безпечний засіб створення підпису (SSCD), верифікатор, загальні настанови з реалізації платформи, застосування створення підписів (SCA), надійний канал, мета оцінювання (TOE), підписувач, розширений електронний підпис.