ДОДАТОК І

ТЕХНІЧНІ СПЕЦИФІКАЦІЇ ДЛЯ СПІЛЬНОГО ШАБЛОНУ ДОВІРЧИХ СПИСКІВ

ГЛАВА І

ЗАГАЛЬНІ ВИМОГИ

Довірчі списки повинні містити дійсну та всю попередню, починаючи з моменту внесення постачальника довірчих послуг до довірчих списків, інформацію про статус внесених до списку довірчих послуг.

Терміни «затверджений», «акредитований» та/або «піднаглядний» у цих специфікаціях також охоплюють національні схеми затвердження, але додаткову інформацію щодо виду будь-яких таких національних схем буде зазначено державами-членами в їхніх довірчих списках, у тому числі пояснення щодо можливих розбіжностей зі схемами нагляду, що застосовують до кваліфікованих постачальників довірчих послуг та кваліфікованих довірчих послуг, які вони надають.

Інформація, зазначена у довірчому списку, в першу чергу спрямована на підтримку валідації токенів кваліфікованих довірчих послуг, тобто фізичних або бінарних (логічних) об'єктів, згенерованих або випущених у результаті використання кваліфікованої довірчої послуги, наприклад, кваліфіковані електронні підписи/печатки, удосконалені електронні підписи/печатки, що підтримуються кваліфікованим сертифікатом, кваліфіковані позначки часу, відомості щодо кваліфікованих електронних відправлень та ін.

ГЛАВА ІІ

ДЕТАЛЬНІ СПЕЦИФІКАЦІЇ ДЛЯ СПІЛЬНОГО ШАБЛОНУ ДОВІРЧИХ СПИСКІВ

Ці специфікації базуються на специфікаціях та вимогах, встановлених в ETSI TS 119 612 v2.1.1 (далі — ETSI TS 119 612).

Якщо жодних спеціальних вимог у цих специфікаціях не встановлено, вимоги, викладені у положеннях 5 та 6 з ETSI TS 119 612, застосовуються повною мірою. Якщо спеціальні вимоги встановлено у цих специфікаціях, вони мають переважну силу над відповідними вимогами ETSI TS 119 612. Якщо існують розбіжності між цими специфікаціями та специфікаціями ETSI TS 119 612, ці специфікації мають переважну силу.

Назва схеми (положення 5.3.6)

Це поле повинно бути присутнім та повинно відповідати специфікаціям, передбаченим у положенні 5.3.6 TS 119 612, відповідно до яких необхідно використовувати таку назву схеми:

«EN_name_value» = «Довірчий список, який містить інформацію щодо кваліфікованих постачальників довірчих послуг, нагляд за якими здійснює держава-член, що видає список, а також інформацію щодо кваліфікованих довірчих послуг, які такі постачальники надають, згідно з відповідними положеннями, викладеними у Регламенті Європейського Парламенту і Ради (ЄС) № 910/2014 від 23 липня 2014 року про електронну ідентифікацію та довірчі послуги для електронних транзакцій на внутрішньому ринку та про скасування Директиви 1999/93/ЄС».

URI інформаційної схеми (положення 5.3.7)

Це поле повинно бути присутнім та повинно відповідати специфікаціям, передбаченим у положенні 5.3.7 TS 119 612, відповідно до яких «належна інформація щодо схеми» повинна містити щонайменше:

(a) Вступну інформацію, яка є спільною для всіх держав-членів та стосується сфери застосування та контексту довірчого списку, основної схеми нагляду та, у відповідних випадках, національної схеми або національних схем затвердження (наприклад, акредитації). Спільний

текст, який підлягає використанню та у якому рядок символів «(*назва відповідної держави-члена*)» необхідно замінити на назву відповідної держави-члена, викладено нижче:

«Цей довірчий список є довірчим списком, що містить інформацію щодо кваліфікованих постачальників довірчих послуг, нагляд за якими здійснює (*назва відповідної держави-члена*), а також інформацію щодо кваліфікованих довірчих послуг, які такі постачальники надають, згідно з відповідними положеннями, викладеними у Регламенті Європейського Парламенту і Ради (ЄС) № 910/2014 від 23 липня 2014 року про електронну ідентифікацію та довірчі послуги для електронних транзакцій на внутрішньому ринку та про скасування Директиви 1999/93/ЄС.

Транскордонному використанню електронних підписів сприяло Рішення Комісії 2009/767/ЄС від 16 жовтня 2009 року, у якому передбачено зобов'язання для держав-членів створювати, вести та публікувати довірчі списки, які містять інформацію, пов'язану з постачальниками послуг зі сертифікації, які видають кваліфіковані сертифікати населенню відповідно до Директиви Європейського Парламенту і Ради 1999/93/ЄС від 13 грудня 1999 року про рамки Співтовариства для електронних підписів та які знаходяться під наглядом держав-членів і акредитовані ними. Цей довірчий список є продовженням довірчого списку, створеного відповідно до Рішення 2009/767/ЄС».

Довірчі списки є важливими елементами у побудові довіри між операторами, дозволяючи користувачам визначати кваліфікований статус та історію статусу постачальників довірчих послуг та їхніх послуг.

Довірчі списки держав-членів містять щонайменше інформацію, зазначену в статтях 1 та 2 Імплементаційного рішення Комісії (ЄС) 2015/1505.

Держави-члени можуть вносити до довірчих списків інформацію щодо некваліфікованих постачальників довірчих послуг разом з інформацією щодо некваліфікованих довірчих послуг, які такі постачальники надають. Необхідно чітко вказувати, що вони не є кваліфікованими відповідно до Регламенту (ЄС) № 910/2014.

Держави-члени можуть вносити до довірчих списків інформацію щодо видів національно визначених довірчих послуг, відмінних від тих, що визначено у статті 3(16) Регламенту (ЄС) № 910/2014. Необхідно чітко вказувати, що вони не є кваліфікованими відповідно до Регламенту (ЄС) № 910/2014.

(b) Конкретну інформацію щодо основної схеми нагляду та, у відповідних випадках, національної схеми або національних схем затвердження (наприклад, акредитації), зокрема ([4]):

(1) Інформацію щодо національної системи нагляду, застосовної до кваліфікованих та некваліфіковних постачальників довірчих послуг і кваліфікованих та некваліфікованих довірчих послуг, які вони надають, як передбачено Регламентом (ЄС) № 910/2014;

(2) Інформацію, у відповідних випадках, щодо національних добровільних схем акредитації, застосовних до постачальників послуг зі сертифікації, що видали кваліфіковані сертифікати відповідно до Директиви 1999/93/ЄС;

Ця конкретна інформація містить для кожної базової схеми, зазначеної вище, щонайменше:

(1) Загальний опис;

(2) Інформацію щодо процесу, передбаченого для національної системи нагляду та, у відповідних випадках, для затвердження за національною схемою затвердження.

(3) Інформацію щодо критеріїв, відповідно до яких здійснюється нагляд за постачальниками довірчих послуг або, у відповідних випадках, затвердження таких.

(4) Інформацію щодо критеріїв та правил, що використовуються для вибору наглядачів/аудиторів та визначення способу оцінки ними постачальників довірчих послуг і довірчих послуги, які такі постачальники надають.

(5) У відповідних випадках, іншу контактну та загальну інформацію, що застосовується для функціонування схеми.

Вид/спільнота/правила схеми (положення 5.3.9)

Це поле повинно бути присутнім та повинно відповідати специфікаціям, викладеним у положенні 5.3.9 TS 119 612.

Вона повинна містити тільки URI у британському варіанті англійської мови.

Вона повинна містити щонайменше два URI:

(1) Такий URI, що є спільним для довірчих списків усіх держава-членів та вказує на описовий текст, який застосовується до усіх довірчих списків:

URI: http://uri.etsi.org/TrstSvc/TrustedList/schemerules/EUcommon

Описовий текст:

«Участь у схемі

Кожна держава-член повинна створити довірчий список, який містить інформацію щодо кваліфікованих постачальників довірчих послуг, за якими здійснюється нагляд, а також інформацію щодо кваліфікованих довірчих послуг, які такі постачальники надають відповідно до Регламенту Європейського Парламенту і Ради (ЄС) № 910/2014 від 23 липня 2014 року про електронну ідентифікацію та довірчі послуги для електронних транзакцій на внутрішньому ринку та про скасування Директиви 1999/93/ЄС.

Покликання на цю імплементацію таких довірчих списків також необхідно вказувати у списку посилань (покажчиків) на довірчі списки кожної держави-члена, скомпільованого Європейською Комісією.

Політика/правила оцінки зазначених у списку послуг

Держави-члени повинні здійснювати нагляд за кваліфікованими постачальниками довірчих послуг, заснованими на території держави-члена, яка призначила наглядовий орган, як передбачено в главі III Регламенту (ЄС) № 910/2014, щоб забезпечити, що такі кваліфіковані постачальники довірчих послуг та кваліфіковані довірчі послуги, які вони надають, відповідають вимогам, що встановлені у цьому Регламенті.

Довірчі списки держав-членів містять щонайменше інформацію, зазначену в статтях 1 та 2 Імплементаційного рішення Комісії (ЄС) 2015/1505.

Довірчі списки повинні містити дійсну та всю попередню інформацію про статус внесених до списку довірчих послуг.

Довірчий список кожної держави-члена повинен містити інформацію про національну схему нагляду і, у відповідних випадках, національну схему або національні схеми затвердження (наприклад, акредитації), відповідно до яких внесено до списку постачальників довірчих послуг та довірчі послуги, які вони надають.

Інтерпретація довірчого списку

Загальні настанови для користувача щодо програм, послуг та продуктів на основі довірчого списку, опублікованого відповідно до Регламенту (ЄС) № 910/2014, є такими:

Кваліфікований статус довірчої послуги позначається комбінацією значення «Service type identifier» («Ідентифікатор виду послуги», «Sti») у записі про послугу та статусу відповідно до значення поля «Service current status» («Поточний статус послуги»), актуального з дня, вказаного у «Current status starting date and time» («Дата і час встановлення поточного статусу»). Попередня інформація щодо такого кваліфікованого статусу надається таким самим чином у відповідних випадках.

Щодо кваліфікованих постачальників довірчих послуг, що видають кваліфіковані сертифікати для електронних підписів, для електронних печаток та/або для автентифікації веб-сайту:

Запис «CA/QC» «Service type identifier» («Sti») (що може бути пізніше кваліфікований як «RootCA-QC» шляхом використання відповідного додаткового розширення інформації про

послуги «Service information extension» («Розширення інформації про послуги», «Sie»))

— вказує на те, що сертифікат кінцевого користувача, виданий центром сертифікації (CA), представленим відкритим ключем та назвою CA з «Service digital identifier» («Цифровий ідентифікатор послуги», «Sdi») (ключ та назва CA вважаються вхідними даними точки довіри), є кваліфікованим сертифікатом (QC) за умови, що він містить щонайменше один з таких ідентифікаторів:

— id-etsi-qcs-QcCompliance: визначена ETSI заява (id-etsi-qcs 1),

— 0.4.0.1456.1.1: визначений ETSI OID (об'єктний ідентифікатор) політики сертифікації (QCP+),

— 0.4.0.1456.1.2: визначений ETSI OID (об'єктний ідентифікатор) політики сертифікації (QCP), —

і за умови, що це забезпечено наглядовим органом держави-члена на підставі поточного статусу послуги (тобто «під наглядом», «припинення нагляду», «акредитований», або «наданий») для такого запису.

— **і якщо** присутня інформація щодо «Sie» «Qualifications Extension» («Розширення кваліфікацій»), то, крім зазначеного вище стандартного правила, сертифікати, ідентифіковані шляхом використання інформація щодо «Sie» «Qualifications Extension», структурованої у послідовності застосування фільтрів, які у подальшому ідентифікують набір сертифікатів, повинні розглядатися відповідно до пов'язаних з ними класифікаторів, які надають додаткову інформацію щодо їхнього кваліфікованого статусу, «SSCD support» («Підтримки SSCD ») та/або «Legal person as subject» («Юридичної особи як суб'єкта») (наприклад, сертифікати, що містять конкретний OID у розширенні «Політика сертифікації», та/або мають конкретну модель «Призначення ключів», та/або відфільтровані шляхом використання конкретного значення, яке з'являється в одному конкретному полі або розширенні сертифіката та ін.). Ці кваліфікатори є частиною зазначеного нижче набору «Кваліфікатори», що використовується для компенсації браку інформації у відповідному змісті сертифіката, та застосовуються відповідно, щоб:

— позначити вид кваліфікованого сертифіката:

— «QCStatement», що означає, що ідентифікований сертифікат або ідентифіковані сертифікати кваліфіковано відповідно до Директиви 1999/93/ЄС;

— «QCForESig», що означає, що ідентифікований сертифікат або ідентифіковані сертифікати, заявлені або зазначені як кваліфіковані, є кваліфікованим сертифікатом або кваліфікованими сертифікатами для електронного підпису відповідно до Регламенту (ЄС) № 910/2014;

— «QCForESeal», що означає, що ідентифікований сертифікат або ідентифіковані сертифікати, заявлені або зазначені як кваліфіковані, є кваліфікованим сертифікатом або кваліфікованими сертифікатами для електронної печатки відповідно до Регламенту (ЄС) № 910/2014;

— «QCForWSA», що означає, що ідентифікований сертифікат або ідентифіковані сертифікати, заявлені або зазначені як кваліфіковані, є кваліфікованим сертифікатом або кваліфікованими сертифікатами для автентифікації веб-сайту відповідно до Регламенту (ЄС) № 910/2014;

— вказати, що сертифікат не вважається кваліфікованим:

— «NotQualified» («Некваліфікований»), що означає, що ідентифікований сертифікат або ідентифіковані сертифікати не вважаються кваліфікованими; та/або

— позначити вид підтримки SSCD:

— «QCWithSSCD», що означає, що ідентифікований сертифікат або ідентифіковані сертифікати, заявлені або зазначені як кваліфіковані, мають власні особисті ключі, що містяться

в SSCD, або

— «QCNoSSCD», що означає, що ідентифікований сертифікат або ідентифіковані сертифікати, заявлені або зазначені як кваліфіковані, не мають власних особистих ключів, що містяться в SSCD, або

— «QCSSCDStatusAsInCert», що означає, що ідентифікований сертифікат або ідентифіковані сертифікати, заявлені або зазначені як кваліфіковані, містять відповідну придатну для машинної обробки інформацію щодо того, чи їхні особисті ключі містяться в SSCD;

— позначити вид підтримки QSCD:

— «QCWithQSCD», що означає, що ідентифікований сертифікат або ідентифіковані сертифікати, заявлені або зазначені як кваліфіковані, мають власні особисті ключі, що містяться в QSCD, або

— «QCNoQSCD», що означає, що ідентифікований сертифікат або ідентифіковані сертифікати, заявлені або зазначені як кваліфіковані, не мають власних особистих ключів, що містяться в QSCD, або

— «QCSSCDStatusAsInCert», що означає, що ідентифікований сертифікат або ідентифіковані сертифікати, заявлені або зазначені як кваліфіковані, містять відповідну придатну для машинної обробки інформацію щодо того, чи їхні особисті ключі містяться в QSCD;

— «QCQSCDManagedOnBehalf», що означає, що усі сертифікати, ідентифіковані за застосовним списком критеріїв, якщо такі заявлені або зазначені як кваліфіковані, мають власні особисті ключі, які містяться в QSCD та генерацію яких і управління якими здійснюють у межах кваліфікованого TSP від імені суб'єкта, особу якого засвідчено у сертифікаті; та/або

— позначити видачу сертифіката юридичній особі:

— «QCForLegalPerson», що означає, що ідентифікований сертифікат або ідентифіковані сертифікати, заявлені або зазначені як кваліфіковані, видано юридичній особі відповідно до Директиви 1999/93/ЄС.

Примітка: Інформацію, зазначену у довірчому списку, необхідно вважати точною, відповідно:

— якщо жодну інформацію щодо заяви id-etsi-qcs 1, OID QCP або OID QCP + не внесено до сертифіката кінцевого користувача, та

— якщо відсутня інформація щодо «Sie» «Qualifications Extension» у відповідному записі про послугу, що відповідає CA/QC точки довіри, для кваліфікації сертифіката як «QCStatement», або

— якщо присутня інформація щодо «Sie» «Qualifications Extension» у відповідному записі про послугу, що відповідає CA/QC точки довіри, для кваліфікації сертифіката як «NotQualified»,

то сертифікат не повинен вважатися кваліфікованим.

«Цифрові ідентифікатори послуги» повинні використовуватись як точки довіри у контексті підтвердження електронних підписів або печаток, для яких необхідно здійснити підтвердження сертифіката підписувача або розробника печатки на підставі інформації довірчого списку, оскільки тільки відкритий ключ та відповідна назва суб'єкту необхідні як інформація про точку довіри. Якщо більше ніж один сертифікат представляє відкритий ключ, що ідентифікує послугу, їх вважають сертифікатами точки довіри, що містять інформацію, ідентичну тій, яку строго вимагають як інформацію про точку довіри.

Загальне правило інтерпретації запису про будь-який інший вид «Sti» полягає у тому, що, для такого ідентифікованого «Sti» виду послуги, внесена до списку послуга, названа відповідно до значення поля «Service name» («Назва послуги») та однозначно ідентифікована за допомогою значення поля «Service digital identity» («Цифрова ідентичність послуги»), має поточний статус

«Кваліфікований» або «Затверджений» відповідно до значення поля «Service current status» («Поточний статус послуги»), актуального з дня, зазначеного в «Current status starting date and time» («Дата і час встановлення поточного статусу»).

Конкретні правила інтерпретації будь-якої додаткової інформації щодо зазначених у списку послуг (наприклад, поле «Service information extensions» («Розширення інформації про послуги»)) можна знайти, у відповідних випадках, у конкретному URI держави-члена як частини поля «Scheme type/community/rules» («Вид/спільнота/правила схеми»).

Дивіться застосовуване вторинне законодавство відповідно до Регламенту (ЄС) № 910/2014 для отримання додаткової інформації про поля, опис та значення довірчих списків держав-членів».

(2) Конкретний для довірчого списку кожної держави-члена URI, що вказує на описовий текст, який необхідно застосовувати до довірчого списку цієї держави-члена:

http://uri.etsi.org/TrstSvc/TrustedList/schemerules/CC, де CC = ISO 3166-1 ([5]) alpha-2 код країни, що використовують у полі «Територія схеми» (положення 5.3.10)

— де користувачі можуть отримати конкретні політики/правила згаданих держав-членів, за якими оцінюють довірчі послуги, внесені до списку, відповідно до режиму нагляду держави-члена і, у відповідних випадках, схеми затвердження.

— де користувачі можуть отримати конкретний опис згаданих держав-членів щодо використання та інтерпретації змісту довірчого списку стосовно зазначених у списку некваліфікованих довірчих послуг та/або національно визначених довірчих послуг. Це може бути використано для ілюстрації можливого рівня деталізації в національній системі затвердження, пов'язаної з CSP, що не видають кваліфікованих сертифікатів, та способів використання полів «Scheme service definition URI» («URI для визначення схеми обслуговування» (положення 5.5.6)) та «Service information extension» («Розширення інформації про послугу» (положення 5.5.9)) для цієї цілі.

Держави-члени МОЖУТЬ визначати та використовувати додаткові URI, що розширюють зазначені вище конкретні URI держави-члена (тобто URI, визначені на підставі цього ієрархічного конкретного URI).

Політика застосування списків статусу довірчої послуги/правове повідомлення (положення 5.3.11)

Це поле повинно бути присутнім та повинно відповідати специфікаціям положення 5.3.11 TS 119 612, де політика/правове повідомлення стосовно правового статусу схеми або правових вимог, яким відповідає схема згідно з юрисдикцією, в якій її створено, та/або будь-яких обмежень та умов, згідно з якими ведеться та публікується довірчий список,

повинні становити послідовність багатомовних рядків символів (див. положення 5.1.4), у яких міститься, англійською мовою у британському варіанті як обов'язковою мовою та, за бажанням, однією або більше національними мовами, актуальний текст будь-якої такої політики або будь-якого такого повідомлення, структурований таким чином:

(1) Перша обов'язкова частина, однакова для довірчих списків усіх держав-членів, у якій зазначено застосовувану нормативно-правову базу, у такій англійській версії:

The applicable legal framework for the present trusted list is Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

Текст національною мовою або національними мовами держави-члена:

Нормативно-правовою базою, застосовуваною до довірчого списку, є Регламент Європейського Парламенту і Ради (ЄС) № 910/2014 від 23 липня 2014 року про електронну ідентифікацію та довірчі послуги для електронних транзакцій на внутрішньому ринку та про скасування Директиви 1999/93/ЄС.

(2) Друга, необов'язкова, частина, яка є індивідуальною для кожного довірчого списку та

охоплює покликання на конкретну застосовну національну нормативно-правову базу

Поточний статус послуги (положення 5.5.5)

Це поле повинно бути присутнім та повинно відповідати специфікаціям положенням 5.5.4 TS 119 612.

Міграція значення «Поточний статус послуги» послуг, внесених до довірчого списку Військового штабу Європейського Союзу (EUMS) у день, що передує дню застосування Регламенту (ЄС) № 910/2014 (тобто 30 червня 2016 року), здійснюється у день застосування цього Регламенту (тобто 1 липня 2016 року), як зазначено у додатку J до ETSI TS 119 612.

ГЛАВА III

БЕЗПЕРЕРВНА ДІЯ ДОВІРЧИХ СПИСКІВ

Сертифікати, які підлягають нотифікації Комісії відповідно до статті 4(2) цього Рішення, повинні відповідати вимогам положення 5.7.1 ETSI TS 119 612 та бути виданими таким чином, щоб:

— різниця між кінцевими термінами дії таких («не після») становила щонайменше три місяці,

— їх було створено на основі нової пари ключів. Пари ключів, які використовувались раніше, не підлягають повторній сертифікації.

У разі закінчення терміну дії одного з сертифікатів відкритих ключів, який міг бути використаний для підтвердження підпису або печатки довірчого списку, який було нотифіковано Комісії та який було опубліковано в основному списку покажчиків Комісії, держави-члени повинні:

— якщо чинний опублікований довірчий список було скріплено підписом або печаткою за допомогою особистого ключа, у сертифіката відкритого ключа якого закінчився термін дії, повторно видати без затримки новий довірчий список, скріплений підписом або печаткою за допомогою особистого ключа, термін дії нотифікованого сертифіката відкритого ключа якого не закінчився;

— за необхідності згенерувати нові пари ключів, які можуть бути використані для скріплення підписом або печаткою довірчого списку, і взяти на себе генерацію їхніх відповідних сертифікатів відкритих ключів;

— негайно нотифікувати Комісії новий список сертифікатів відкритих ключів, що відповідають особистим ключам, які могли би бути використані для скріплення підписом або печаткою довірчого списку.

У разі компрометації або втрати чинності одного з особистих ключів, що відповідає одному з сертифікатів відкритих ключів, який міг би бути використаний для підтвердження підпису або печатки довірчого списку, який було нотифіковано Комісії та який було опубліковано в основному списку покажчиків Комісії, держави-члени повинні:

— повторно видати без затримки новий довірчий список, скріплений підписом або печаткою за допомогою нескомпрометованого особистого ключа, якщо опублікований довірчий список було скріплено підписом або печаткою за допомогою особистого ключа, який було скомпрометовано або втратив чинність;

— за необхідності згенерувати нові пари ключів, які можуть бути використані для скріплення підписом або печаткою довірчого списку, і взяти на себе генерацію їхніх відповідних сертифікатів відкритих ключів;

— негайно нотифікувати Комісії новий список сертифікатів відкритих ключів, що відповідають особистим ключам, які могли би бути використані для скріплення підписом або печаткою довірчого списку.

У разі компрометації або втрати чинності усіх особистих ключів, які відповідають сертифікатам відкритих ключів, які могли би бути використані для підтвердження підпису або печатки довірчого списку, які було нотифіковано Комісії та які було опубліковано в основному списку покажчиків Комісії, держави-члени повинні:

— згенерувати нові пари ключів, які можуть бути використані для скріплення підписом або печаткою довірчого списку, і взяти на себе генерацію їхніх відповідних сертифікатів відкритих ключів;

— повторно видати без затримки новий довірчий список, який скріплено підписом або печаткою за допомогою одного з таких нових особистих ключів та відповідний сертифікат відкритого ключа якого необхідно нотифікувати;

— негайно нотифікувати Комісії новий список сертифікатів відкритих ключів, що відповідають особистим ключам, які могли би бути використані для скріплення підписом або печаткою довірчого списку.

ГЛАВА IV

СПЕЦИФІКАЦІЇ ЩОДО ПРИДАТНОЇ ДЛЯ СПРИЙНЯТТЯ ЛЮДИНОЮ ФОРМИ ДОВІРЧОГО СПИСКУ

Коли придатну для сприйняття людиною форму довірчого списку встановлено та опубліковано, її необхідно надати у форматі Portable Document Format (PDF) відповідно до ISO 32000 ([6]), а саме у форматі PDF/A (ISO 19005 ([7])).

Зміст придатної для сприйняття людиною форми довірчого списку у форматі PDF/A повинен відповідати таким вимогам:

— Структура придатної для сприйняття людиною форми повинна відображати логічну модель, описану в TS 119 612;

— Кожне присутнє поле повинно відображатися та охоплювати:

— Назву поля (наприклад, *«Service type identifier» («Ідентифікатор типу послуги»));*

— Значення поля (наприклад, «http://uri.etsi.org/TrstSvc/Svctype/CA/QC}»);

— Зміст (опис) значення поля у відповідних випадках (наприклад, «*Послуга генерування сертифіката для створення та підписання кваліфікованих сертифікатів на основі тотожності особи та інших атрибутів, перевірених відповідними реєстраційними службами*»);

— Версії кількома природними мовами, як передбачено у довірчому списку, у відповідних випадках.

— Зазначені нижче поля та відповідні значення цифрових сертифікатів ([8]), якщо такі присутні в полі «Service digital identity» («Цифрова ідентичність послуги»), повинні щонайменше відображатися у придатній для сприйняття людиною формі:

— Номер версії сертифіката

— Унікальний реєстраційний номер сертифіката

— Найменування криптоалгоритму, що використовується центром

— Найменування центру — усі відповідні поля унікального найменування

— Строк чинності сертифіката

— Власник сертифіката — усі відповідні поля унікального найменування

— Відкритий ключ

— Ідентифікатор відкритого ключа центру

— Ідентифікатор відкритого ключа підписувача

— Призначення відкритого ключа, що міститься в сертифікаті

— Уточнене призначення відкритого ключа, що міститься в сертифікаті

— Політика сертифікації — усі ідентифікатори та кваліфікатори політики

— Політика відповідності

— Додаткові дані підписувача

— Персональні дані підписувача

— Основні обмеження

— Обмеження, передбачені політикою

— Точки доступу до списків відкликаних сертифікатів (CRL) ([9])

— Доступ до інформації про центр

— Доступ до інформації про підписувача

— Повідомлення про кваліфіковані сертифікати

— Алгоритм гешування

— Геш-значення сертифіката

— Придатна для сприйняття людиною форма повинна підлягати безперешкодному друку

— Придатна для сприйняття людиною форма скріплюється підписом та печаткою оператора схеми відповідно до вимог стандарту PDF advanced signature («Удосконалений підпис PDF»), зазначеного у статтях 1 та 3 Імплементаційного рішення Комісії (ЄС) 2015/1505.