

ПІЛОТНИЙ ПРОЄКТ ІНТЕРНАЛІЗАЦІЇ СТРУКТУРНОГО БЛОКУ ЦИФРОВОГО ПІДПИСУ (ESIG BB)

Настанова щодо Угоди про взаємне визнання
електронних довірчих послуг

Статус документа

Статус
Кінцева редакція

Внесені зміни

Редакція	Дата	Створено	Короткий опис змін
1.0	10.07.2020	eSignature Механізму "З'єднання Європи"	Створення
1.1	18.01.2021	eSignature Механізму "З'єднання Європи"	Незначне оновлення

Підготовка українського примірника

Переклад	Рецензія	Дизайн та верстка
Галина Сташків	Андрій Дресвянніков Андрій Мелашенко	Олександр Іванов



У Ц
Є П
УКРАЇНСЬКИЙ ЦЕНТР
ЄВРОПЕЙСЬКОЇ
ПОЛІТИКИ



Government Offices of Sweden
Ministry for Foreign Affairs

Документ підготовлено Українським центром європейської політики за підтримки уряду Швеції, Міністерства закордонних справ та Шведського Центру розвитку міжнародного співробітництва. Інформація та точки зору, висловлені в роботі, належать лише авторам та не обов'язково відповідають точці зору уряду Швеції, Міністерства закордонних справ та Шведського Центру розвитку міжнародного співробітництва. Помилки в роботі є відповідальністю лише автора. Усі частини роботи захищені авторським правом.

Цей документ є тотожним перекладом [MRA Cook-book](#).

© Європейський Союз, 2020 р.

Передрук цього документа дозволено за умови зазначення першоджерела. Політика щодо передруку матеріалів регламентується Рішенням Комісії 2011/833/ЄС від 12 грудня 2011 року про повторне використання документів Комісії.

© Український центр європейської політики, 2021 р.

ЗМІСТ

4	ПОСИЛАННЯ
7	АБРЕВІАТУРИ
10	1. ВСТУП
11	1.1. Загальні дані щодо Регламенту (ЄС) № 910/2014
13	1.2. Послідовність процесів і методика реалізації УВВ/MRA
16	1.3. Сфера застосування і мета цього документа і додатків до нього
17	1.4. Структура документа
18	2. МІНІМАЛЬНІ ВИМОГИ ДО СТРУКТУРИ НДП/ДП ТРЕТІХ КРАЇН + ЧЕКЛИСТ ДЛЯ САМОСТІЙНОГО ОЦІНЮВАННЯ
20	2.1. Законодавчі вимоги
22	2.2. Вимоги щодо нагляду й оцінювання відповідності
25	2.3. Технічні умови та найкращі практики
28	2.4. Модель формування Довіри
30	3. ОСНОВНІ ТЕХНІЧНІ РЕКОМЕНДАЦІЇ ДЛЯ 3-х КРАЇН
32	3.1. Рекомендації щодо формату і змісту конкретних результатів НДП/ДП
36	3.2. Рекомендації щодо реалізації довірчих списків третіх країн
44	4. ПРОГРАМНІ ВКАЗІВНИКИ УВВ У КДС ЄК І ДОВІРЧИХ СПИСКАХ ТРЕТІХ КРАЇН
47	4.1. Передумови
48	4.2. Впровадження УВВ/MRA в КДС ЄС
49	4.3. Впровадження УВВ/MRA у довірчий список третьої країни
49	5. ВЗАЄМНА ВАЛІДАЦІЯ “КВАЛІФІКОВАНИХ” ЕЛЕКТРОННИХ ПІДПИСІВ/ ПЕЧАТОК ЄС/ ТРЕТЬОЇ КРАЇНИ

ПОСИЛАННЯ

Статус документа

Посилання	Назва
[Специфікація УВВ/MRA]	Пілотний проєкт інтерналізації структурного блоку цифрового підпису (eSig BB) – специфікація елемента MRainfo
Пілотний проєкт інтерналізації структурного блоку цифрового підпису (eSig BB) – специфікація елемента MRainfo	Пілотний проєкт інтерналізації структурного блоку цифрового підпису (eSig BB) – чеклист оцінювання за ст. 14 eIDAS
[Чеклист УВВ]	Пілотний проєкт інтерналізації структурного блоку цифрового підпису (eSig BB) – використання елемента MRainfo

Стандарти

Посилання	Назва
[TR 103 684]	ETSI TR 103 684: "Електронні підписи та інфраструктури (ESI); Глобальне прийняття довірчих послуг ЄС". https://www.etsi.org/deliver/etsi_tr/103600_103699/103684/01.01.01_60/tr_103684v010101p.pdf
[TS 119 101]	ETSI TS 119 101: "Електронні підписи та інфраструктури (ESI); Вимоги та політики безпеки для додатків формування та перевірки підписів".
[TS 119 102-1]	ETSI TS 119 102-1 v1.2.1: "Електронні підписи та інфраструктури (ESI); Процедури створення та валідації цифрових підписів AdES; Частина 1: Створення та валідація".
[TS 119 102-2]	ETSI TS 119 102-2: "Електронні підписи та інфраструктури (ESI); Процедури створення та валідації цифрових підписів AdES; Частина 2: Звіт про валідацію підпису".
[EN 319 122]	Серія ETSI EN 319 122: Електронні підписи та інфраструктури (ESI); Цифрові підписи CAdES; Частина 1: "Структурні блоки та базові підписи CAdES". Частина 2: "Розширені підписи CAdES".
[EN 319 132]	Серія ETSI EN 319 132: Електронні підписи та інфраструктури (ESI); Цифрові підписи XAdES; Частина 1: "Структурні блоки та базові підписи XAdES". Частина 2: "Розширені підписи XAdES".
[EN 319 142]	Серія ETSI EN 319 142: Електронні підписи та інфраструктури (ESI); Цифрові підписи PAdES; Частина 1: "Структурні блоки та базові підписи PAdES". Частина 2: "Додаткові профілі підписів PAdES".

[EN 319 162]	Серія ETSI EN 319162: Електронні підписи та інфраструктури (ESI); Контейнери, пов'язані з підписом (ASiC); Частина 1: "Структурні блоки та базові контейнери ASiC". Частина 2: "Додаткові контейнери ASiC".
[TS 119 172]	Серія ETSI TS 119 172: Електронні підписи та інфраструктури (ESI); Політики підпису; Частина 1: "Складники та зміст документів щодо політик підпису, призначені для читання людиною"; Частина 2: "Формат XML для політик підпису"; Частина 3: "Формат ASN.1 для політик підпису"; Частина 4: "Політика валідації підпису для європейських кваліфікованих електронних підписів/печаток із використанням довірчих списків".
[EN 319 401]	ETSI EN 319 401: "Електронні підписи та інфраструктури (ESI); Загальні вимоги політики для надавачів довірчих послуг".
[EN 319 403]	ETSI EN 319 403: "Електронні підписи й інфраструктури (ESI). Оцінювання відповідності надавачів довірчих послуг. Вимоги до органів з оцінювання відповідності, які оцінюють надавачів довірчих послуг". На даний час готується нова редакція відповідно до EN 319403-1
[EN 319 411-1]	ETSI EN 319 411-1: "Електронні підписи та інфраструктури (ESI); Вимоги щодо політики та безпеки для надавачів довірчих послуг, що видають сертифікати; Частина 1: Загальні вимоги".
[EN 319 411-2]	ETSI EN 319 411-2: "Електронні підписи та інфраструктури (ESI); Вимоги щодо політики та безпеки для надавачів довірчих послуг, що видають сертифікати; Частина 2: Вимоги до надавачів довірчих послуг, що видають кваліфіковані сертифікати ЄС".
[TR 119 411-4]	ETSI TR 119 411-4: "Електронні підписи та інфраструктури (ESI); Вимоги щодо політики та безпеки для надавачів довірчих послуг, що видають сертифікати; Частина 4: Чеклист для аудиту НДП на відповідність EN 319 411-1 або EN 319 411-2".
[EN 319 412-2]	ETSI EN 319 412-2: "Електронні підписи та інфраструктури (ESI); Профілі сертифікатів; Частина 2: Профілі сертифікатів. Частина 2. Профіль сертифікатів, що видаються фізичним особам".
[EN 319 412-3]	ETSI EN 319 412-3: "Електронні підписи та інфраструктури (ESI); Профілі сертифікатів; Частина 3: Профілі сертифікатів, що видаються юридичним особам".
[EN 319 412-4]	ETSI EN 319 412-4: "Електронні підписи та інфраструктури (ESI); Профілі сертифікатів; Частина 4: Профілі сертифікатів для сертифікатів вебсайтів".
[EN 319 412-5]	ETSI EN 319 412-5: "Електронні підписи та інфраструктури (ESI); Профілі сертифікатів; Частина 5: Системи контролю якості (QCStatements)".
[EN 319 421]	ETSI EN 319 421: "Електронні підписи та інфраструктури (ESI); Вимоги щодо політики та безпеки для надавачів довірчих послуг, що видають мітки/позначки часу".
[EN 319 422]	ETSI EN 319 422: "Електронні підписи та інфраструктури (ESI); Протокол мітки/позначки часу та профілі токенів позначки часу".
[TS 119 441]	ETSI TS 119 441: "Електронні підписи та інфраструктури (ESI); Вимоги щодо політики для НДП, що надають послуги з валідації/перевірки цифрових підписів".
[TS 119 442]	ETSI TS 119 442: "Електронні підписи та інфраструктури (ESI); Профілі протоколу щодо надавачів довірчих послуг, які надають послуги з валідації/перевірки цифрових підписів AdES".
[TS 119 511]	ETSI TS 119 511: "Електронні підписи та інфраструктури (ESI); Вимоги щодо політики та безпеки для надавачів довірчих послуг, що забезпечують тривале зберігання цифрових підписів чи загальних даних з використанням методів цифрового підпису".

[TS 119 512]	ETSI TS 119 512: "Електронні підписи та інфраструктури (ESI); Протоколи для надавачів довірчих послуг, що забезпечують тривале зберігання даних".
[EN 319 521]	ETSI EN 319 521: "Електронні підписи та інфраструктури (ESI); Вимоги щодо політики та безпеки для надавачів послуг реєстрованої електронної доставки".
[EN 319 522]	Серія ETSI EN 319 522: Електронні підписи та інфраструктури (ESI); Послуги реєстрованої електронної доставки; Частина 1: "Модель та архітектура"; Частина 2: "Семантичний вміст"; Частина 3: "Формати"; Частина 4: "Прив'язки": Підрозділ 1: "Прив'язки доставки повідомлень"; Підрозділ 2: "Прив'язки підтвердження та ідентифікації"; Підрозділ 3: Прив'язки можливостей / вимог".
[TS 119 524]	ETSI TS 119 524 (усі частини): "Електронні підписи та інфраструктури (ESI); Тестування відповідності та інтероперабельності послуг реєстрованої електронної доставки".
[EN 319 531]	ETSI EN 319 531: "Електронні підписи та інфраструктури (ESI); Вимоги щодо політики та безпеки для постачальників послуг реєстрованої електронної пошти".
[EN 319 532]	Серія ETSI EN 319 532: Електронні підписи та Інфраструктури (ESI); Послуги реєстрованої електронної пошти (REM); Частина 1: "Модель та архітектура"; Частина 2: "Семантичний вміст"; Частина 3: "Формати"; Частина 4: "Профілі інтероперабельності".
[TS 119 534]	ETSI TS 119 534 (усі частини): "Електронні підписи та інфраструктури (ESI); Тестування відповідності та інтероперабельності послуг реєстрованої електронної пошти".
[TS 119 612]	ETSI TS 119 612 v2.1.1 (2015-07): "Електронні підписи та інфраструктури (ESI); Довірчі списки".
[TS 119 615]	ETSI TS 119 615: "Електронні підписи та інфраструктури (ESI); Довірчі списки; Процедури використання і тлумачення національних довірчих списків держав-членів Європейського Союзу".

Усі стандарти ETSI доступні на вебсторінці <https://www.etsi.org/standards/get-standards>

АБРЕВІАТУРИ

Щоб уникнути неоднозначностей, в документі використовуються такі скорочення:

Скорочення	Пояснення
ІПК (англійською CID)	Імплементативне Рішення Комісії
ЄК (англійською EC)	Європейська Комісія
ЄС (англійською EU)	Європейський Союз
3rdC	третья країна
ДС (англійською TL)	Довірчий список
КДС (англійською LOTL)	Кореневий довірчий список ЄС
ДЧ (англійською MS)	держава-член ЄС (англійською Member State)
ВВ (англійською MR)	Взаємне визнання
УВВ (англійською MRA)	Угода про взаємне визнання
НО (англійською SB)	Наглядовий орган
ЗОВ (англійською CAR)	Звіт з оцінки відповідності
ООВ (англійською CAB)	Орган з оцінки відповідності
НОА (англійською NAB)	Національний орган з акредитації
НДП (англійською TSP)	Надавач довірчих послуг
НДП/ДП (англійською TSP/TS)	Надавач довірчих послуг і довірча послуга, яку він надає
КДП (англійською QTS) - кваліфікована довірча послуга	Кваліфікований надавач довірчих послуг
КНДП (англійською QTSP)	Кваліфікований надавач довірчих послуг
КНДП/КДП (англійською QTSP/QTS)	Кваліфікований надавач довірчих послуг і кваліфікована довірча послуга, яку він надає
КЕПечатка (англійською QESeal)	Кваліфікована електронна печатка
КЕП (англійською QESig)	Кваліфікований електронний підпис
КЕП-ЄС (англійською EU-QESig)	Кваліфікований електронний підпис, як визначено в Регламенті eIDAS.
КЕП третьої країни (англійською 3rdC-QESig)	Кваліфікований електронний підпис третьої країни, як визначено в законодавстві третьої країни, але, що не суперечить ¹ Регламенту eIDAS, який базується на AdES третьої країни, на основі кваліфікованого сертифікату (QC-eSig) третьої країни, і створеному за допомогою КЗСП третьої країни.
AdES ЄС	Удосконалений / розширений електронний підпис, як визначено в Регламенті eIDAS (примітка редактора: AdES українською – це підпис удосконалений, але він базується на розширеному сертифікаті, тому інколи виникає термінологічна плутанина і AdES називають розширений електронний підпис, особливо у контексті різних технічних реалізацій таких як CAdES, XAdES, PAdES).

1. Оскільки можуть існувати вимоги, за яких валідація QESig третьої країни відрізняється від валідації QESig-ЄС, як визначено у статті 32 eIDAS

AdES Удосконалений електронний підпис третьої країни (англійською 3rdC-AdES) (примітка редактора AdES – українською це підпис удосконалений, але він базується на розширеному сертифікаті, тому інколи виникає термінологічна плутанина і AdES називають розширений електронний підпис, особливо що до різних технічних реалізацій таких як CAdES XAdES PAdES)	Удосконалений / розширений електронний підпис третьої країни, як визначено законодавством третьої країни.
КНДП ЄС (англійською EU-QTSP)	Кваліфікований надавач довірчих послуг, як визначено в Регламенті eIDAS.
КДП ЄС (англійською EU-QTS)	Кваліфікована довірча послуга, як визначено в Регламенті eIDAS.
QC-eSig ЄС (англійською EU-QC-eSig)	Кваліфікований сертифікат електронних підписів, як визначено в Регламенті eIDAS.
КЗСП ЄС (англійською EU-QSCD)	Кваліфікований засіб створення підпису (або печатки), як визначено в Регламенті eIDAS.
КНДП третьої країни (англійською 3rdC-QTSP)	Кваліфікований надавач довірчих послуг третьої країни, заснований у третій країні.
КДП третьої країни (англійською 3rdC-QTS)	Кваліфікована довірча послуга третьої країни від КНДП третьої країни, створеного в третій країні.

Оскільки можуть існувати вимоги, за яких валідація QESig третьої країни відрізняється від валідації QESig-ЄС, як визначено у статті 32 eIDAS.

QC-КЕП третьої країни (англійською 3rdC-QC-eSig)	Сертифікат кваліфікованих електронних підписів третьої країни, як визначено у законодавстві третьої країни.
КЗСП третьої країни (англійською 3rdC-QSCD)	Засіб створення підписів, сертифікований як такий, що відповідає вимогам, встановленим законодавством третьої країни, як необхідний елемент для створення QESig третьої країни.
КЗСП третьої країни-ЄС (англійською 3rdC-EU-QSCD)	КЗСП третьої країни, який сертифікований як КЗСП ЄС. Хронологія цих двох сертифікацій не має значення для пілотного проєкту. Основне – те, що засіб сертифіковано як КЗСП за обома законодавствами.
КДС ЄК (англійською EC-LOTL)	Кореневий / об'єднаний Довірчий Список країн ЄС (у формі ЄК) відповідно до eIDAS (див. КДС ЄС).
КДС ЄС (англійською EU-LOTL)	Кореневий довірчий список, складений державами-членами ЄС, як визначено в eIDAS.
ДС ЄС (англійською EC-TL)	Національний довірчий список держави-члена ЄС, як визначено в Регламенті eIDAS.
КДС третьої країни (англійською 3rdC-LOTL)	Кореневий довірчий список, складений групою третіх країн. Див. також "ДС третьої країни".
ДС третьої країни (англійською 3rdC-TL)	Довірчий список третьої країни. Задля простоти в цьому документі на позначення КДС третьої країни або ДС третьої країни використовуватиметься термін "ДС третьої країни".
КДС-ВССДП ЄС до третьої країни (англійською EC-LOTL-PTOTSL 3rdC)	У КДС ЄС "програмний вказівник на інший Список статусів довірчих послуг", що вказує на ДС третьої країни.

ДС-3-ї країни-ВССДП-ЄС	У ДС третьої країни "програмний вказівник на список статусів довірчих послуг", що вказує на КДС ЄС.
XML	Розширювана мова розмітки.
Sti	Ідентифікатор типу послуги.
Sdi	Цифровий ідентифікатор послуги.
Sie	Розширення інформації про послугу.
Sie:aSI	Розширення додаткової інформації про послугу (additional Service Information).
Sie:Q	Кваліфікаційне розширення.
DN	Унікальне ім'я.

1. ВСТУП

- 1.1. Загальні дані щодо Регламенту (ЄС) № 910/2014
- 1.2. Послідовність процесів і методика реалізації УВВ/MRA
- 1.3. Сфера застосування і мета цього документа і додатків до нього
- 1.4. Структура документа



1. ВСТУП

1.1. ЗАГАЛЬНІ ДАНІ ЩОДО РЕГЛАМЕНТУ (ЄС) № 910/2014

1.1.1. Кваліфіковані надавачі довірчих послуг і кваліфіковані довірчі послуги

Регламент (ЄС) № 910/2014² (надалі – Регламент eIDAS) про електронну ідентифікацію та довірчі послуги для електронних транзакцій на внутрішньому ринку забезпечує регуляторне середовище для електронної ідентифікації фізичних і юридичних осіб та для довірчих послуг.

Щоб підвищити, зокрема, довіру між підприємствами та споживачами на внутрішньому ринку і сприяти використанню довірчих послуг, Регламент eIDAS запроваджує поняття кваліфікованих довірчих послуг (КДП) і кваліфікованого надавача довірчих послуг (КНДП) з метою засвідчити, що ці КДП і КНДП відповідають вимогам та виконують обов'язки щодо високого рівня безпеки.

У Регламенті eIDAS встановлено 9 видів кваліфікованих довірчих послуг:

- ◆ і. надання кваліфікованих сертифікатів для електронних підписів,
- ◆ ii. надання кваліфікованих сертифікатів для електронних печаток,
- ◆ iii. надання кваліфікованих сертифікатів для автентифікації вебсайтів,
- ◆ iv. кваліфікована послуга валідації кваліфікованих електронних підписів,
- ◆ v. кваліфікована послуга валідації кваліфікованих електронних печаток,
- ◆ vi. кваліфікована послуга зберігання кваліфікованих електронних підписів,
- ◆ vii. кваліфікована послуга зберігання кваліфікованих електронних печаток,
- ◆ viii. надання кваліфікованих позначок часу, та
- ◆ ix. кваліфіковані послуги електронної доставки.

Нарешті, у eIDAS викладено визначення фізичної або юридичної особи, що надає одну або кілька таких КДП і якій наглядовим органом надано кваліфікованого статусу КНДП.

1.1.2. Довірчі рамки, Довірчий список і Кореневий довірчий список

Щоб забезпечити високий рівень захисту кваліфікованих довірчих послуг, Регламент eIDAS передбачає схему активного переддозвільного нагляду за КНДП і КДП, які вони надають, (надалі – КНДП/КДП) компетентним національним наглядовим органом, який *ex ante* та *ex post* здійснює нагляд за виконанням обов'язків і вимог, пов'язаних із КНДП/КДП. КНДП/КДП повинні відповідати усім цим вимогам, що має бути показано у звіті про оцінювання відповідності та підтверджено Наглядовим Органом (НО) ще до початку надання кваліфікованих довірчих послуг, наприклад, перед тим, як видати першу кваліфіковану позначку часу, якщо КНДП спеціалізується на послугах із надання кваліфікованих позначок часу. КНДП можуть починати надавати КДП лише після надання їм компетентним наглядовим органом кваліфікованого статусу і внесення до Національного Довірчого Списку.

Довірчі списки держав-членів ЄС є юридичними установчими інструментами, що дають змогу перевірити актуальність кваліфікованого статусу КНДП/КДП. Через них контрольно-наглядова система показує увесь життєвий цикл кожної КДП і кожного КНДП від започаткування до припинення. Це відображається у довірчих списках, в яких назавжди зберігається повна історія змін кваліфікованого статусу кожної КДП, яку надає кожен КНДП, створений в ЄС.

Регламент eIDAS зобов'язує держави-члени ЄС створити свої національні довірчі списки, у форматі придатному для автоматизованої обробки (формат XML), відповідно до специфікацій,

2. 20J L 257, 28.8.2014, с. 73-114. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

встановлених ІРК (ЄС) 2015/1505³, в якому викладено технічні специфікації та формати довірчих списків відповідно до статті 22 (5) Регламенту eIDAS. Ці специфікації та формати спираються на редакцію 2.1.1 стандарту [ETSI TS 119 612]⁴.

В ІРК (ЄС) 2015/1505 також визначено правила використання та тлумачення національних довірчих списків ЄС. [ETSI TS 119 615]⁵ визначає процедури, що дозволяють застосовувати ці правила під час валідації результатів КДП ЄС відповідно до таких довірчих списків ЄС (напр., валідації кваліфікованих сертифікатів, кваліфікованих позначок часу ЄС, підтверджень, створених кваліфікованими сервісами реєстрованої електронної доставки, електронних підписів або печаток ЄС на кваліфікованих звітах ЄС про валідацію/перевірку кваліфікованих електронних підписів або печаток ЄС).

Для забезпечення легкого доступу до довірчих списків усіх держав-членів Європейська Комісія (ЄК) публікує центральний (XML) список, який називається кореневим довірчим списком (КДС = LOTL), з посиланнями на опубліковані довірчі списки держав-членів. Для підписання довірчого списку ЄС використовують електронний підпис та печатку, що базуються на сертифікатах відкритого ключа з відповідними приватними ключами, таким чином сторони-користувачі можуть проводити валідацію підписів/печаток цих довірчих списків держав-членів ЄС за умови нотифікування ЄК та оприлюднення інформації про них у КДС (LOTL).

1.1.3. Стаття 14 про міжнародні аспекти

Регламент eIDAS передбачає можливість визнання довірчих послуг, що надаються НДП з третіх країн, юридично еквівалентними КНДП країн ЄС. Таке взаємне визнання передбачено у статті 14 eIDAS і може відбуватися лише на основі угоди між ЄС і зацікавленими третіми країнами відповідно до статті 218 ДФЄС (TFEU).

Стаття 14 обмежує погодження і взаємне визнання довірчих послуг з третіми країнами до дев'яти типів КДП, що їх на даний час визначено Регламентом eIDAS та надають КНДП.

Очікується, що основною метою Угоди про взаємне визнання (УВВ/MRA) буде взаємне визнання третьою країною та ЄС кваліфікованих електронних підписів (QESigs) і кваліфікованих електронних печаток (QESeals). Відповідно до eIDAS, QESigs та QESeals третьою країною підлягають дії трьох умов:

- ◆ а. відповідність вимогам ст. 26 eIDAS щодо розширених електронних підписів (AdESigs) або ст. 36 eIDAS щодо розширених електронних печаток (AdESeals) відповідно;
- ◆ б. розміщення відповідного особистого ключа в QSigCD ЄС або QSealCD ЄС відповідно; та

- ◆ с. їх підтримка сертифікатом підпису/печатки, який визнано рівнозначним кваліфікованому сертифікату (КС = QC) для електронних підписів або електронних печаток відповідно.

Умови (а) та (б) виходять за рамки предмета МРА, встановленого відповідно до ст. 14, і можуть виконуватися незалежно. Отже, йдеться про поєднання безпосередньої відповідності вимогам eIDAS (для виконання умов (а) і (б)) та визнання сертифікатів через УВВ за ст. 14 (для виконання умови (с)).

1.1.4. Технічна складова статті 14

Попередньою умовою УВВ/MRA за ст. 14 eIDAS до третьої країни-кандидата є створити, опублікувати та вести довірчий список третьої країни з інформацією принаймні щодо тих НДП/ДП, які визнані юридично рівнозначними КНДП/КДП ЄС.

Очікується, що укладення УВВ/MRA за ст. 14 вводиться в дію шляхом внесення до КДС ЄС (LOTL):

- ◆ Програмного вказівника на відповідний довірчий список третьої країни за стандартом ([ETSI TS 119 612], п. 5.3.13 "Програмні вказівники на інші Списки статусів довірчих послуг");
- ◆ і у такому вказівнику – елементи MRInfo, спрямовані на зіставлення еквівалентності між ключовими URI або стейтментами, що використовуються в довірчих списках держав-членів ЄС, та тими, що використані в довірчому списку третьої країни відповідно.

Мета – уможливити використання цього елемента з MRInfo для правильної ініціалізації стандартизованого процесу для валідації рівнозначності вихідних даних КДП третьої країни та КДП ЄС за стандартом [ETSI TS119 615].

Відповідно, очікується, що довірчий список третьої країни міститиме еквівалентний вказівник-конектор на КДС ЄК (ЄС LOTL) з відповідним елементом MRInfo для введення в дію УВВ/MRA щодо особливостей роботи НДП/ДП 3-ї країни.

Перед внесенням до КДС ЄК (ЄС LOTL) програмного вказівника на довірчий список третьої країни, процес укладення УВВ/MRA за ст. 14 передбачатиме низку кроків, зокрема пілотні інтеграцію, апробацію та узгодження. Потрібно також брати до уваги технічне обслуговування та потенційне припинення УВВ/MRA за ст. 14 eIDAS.

На рисунку нижче зображено схему типової послідовності процесів підготовки, укладення й управління життєвим циклом УВВ/MRA за ст. 14 Регламенту eIDAS між ЄС і третьою країною.

Типова послідовність процесів життєвого циклу УВВ/MRA за ст. 14

3. OJ L 235, 9.9.2015, p. 26–36. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015D1505>

4. https://www.etsi.org/deliver/etsi_ts/119600_119699/119612/02_01_01_60/ts_119612v020101p.pdf

5. https://portal.etsi.org/webapp/workProgram/Report_WorkItem.asp?wiki_id=54329

1.2. ПОСЛІДОВНІСТЬ ПРОЦЕСІВ І МЕТОДИКА РЕАЛІЗАЦІЇ УВВ/MRA

1.2.1. Підготовчий етап

З позиції ЄС, зображений вище перший крок виконує третя країна – вона має встановити предмет і цілі УВВ з ЄС щодо НДП, заснованих на території цієї країни, та ДП, які вони надають. Ці підготовчі етапи повинні зосереджуватися на проведенні техніко-економічного обґрунтування і самооцінювання вірогідності та/або проблемних моментів щодо укладення такої УВВ з ЄС. Один з можливих кроків – це проведення пілотної технічної апробації з ЄК для перевірки технічних аспектів і послідовності дій, передбачуваних або вжитих третьою країною. У разі позитивних результатів досліджень щодо доцільності, апробації та самооцінювання третя країна може прийняти рішення щодо початку офіційних переговорів про взаємне визнання.

Оцінювання, що проводитимуться до укладення УВВ за ст. 14 eIDAS (починаючи з самооцінювання), не повинні обмежуватися законодавчими аспектами, натомість вони мають фокусуватися на таких чотирьох базових елементах, вказаних у стандарті [ETSI TR 103 684]:

- ◆ а. Законодавча нормативна база, тобто законодавчий контекст, первинне і вторинне законодавство та/або правила, нормативи та стандарти, за якими працюють (К)НДП/(К)ДП.
- ◆ б. Системи нагляду й аудиту, зокрема здійснення наглядової діяльності суб'єкта(ів) (К)НДП/(К)ДП, відповідність правил аудиту, що застосовуються до (К)НДП/(К)ДП, й органи оцінки відповідності та контролю.
- ◆ с. Технічні аспекти та ті, що пов'язані з найкращими практиками, до яких входять і вимоги щодо політик безпеки, технічні критерії, протокол і формати, що їх використовують КНДП/(К)ДП для підтвердження, що вони відповідають необхідним законодавчим вимогам, очікуваному рівню безпеки та належному рівню підтримки інтероперабельності.
- ◆ д. Модель формування довіри, що стосується способу подання і поширення затвердження і рівня надійності (К)НДП, які підтримують певну (К)ДП. Така довіра може бути реалізована різними способами, такими як довірчі списки, репозиторії довірчих послуг, кореневе підписання або кроссертифікація довірчих сервісів або через поєднання механізмів. Однак у контексті УВВ за ст. 14 третя країна повинна створити та вести національний довірчий список принаймні для тих НДП/ДП, які будуть визнані юридично рівнозначними КНДП/КДП ЄС.

1.2.2. Початок процесу ВВ і попередня оцінка

В контексті ЄС етап оцінювання повинен складатися з двох фаз, а саме:

- ◆ е. Спочатку проводиться попереднє зіставлення глобальної сумісності системи чотирьох засадничих складників 3-ї країни з системою ЄС на основі наданої документації. Якщо порівнювані структури занадто різні (напр., відсутні рівнозначні КДП, не передбачено заходів щодо порушень безпеки, використовуються суттєво інші стандарти, відсутній захист даних), результат оцінювання буде негативним.
- ◆ ф. Якщо ж попереднє оцінювання виявиться позитивним, далі проводитиметься детальне оцінювання, що дасть змогу ухвалити рішення щодо можливості підготовки УВВ/MRA.

Відтак разом з офіційним запитом третя країна подає до ЄК детальну документацію для оцінювання, зокрема:

- ◆ і. Загальний опис структури (К)ДП третьої країни із зазначенням усіх чотирьох аспектів – законодавчого, контрольно-наглядового, технічного й аспекту моделі формування довіри.
- ◆ ii. Законодавчі документи, що регулюють структуру (К)ДП, в тому числі первинне та відповідне вторинне законодавство.
- ◆ iii. Інші відповідні законодавчі акти, наприклад, про захист даних, права споживачів, конфіденційність, свободу слова тощо.
- ◆ iv. Посилання на відповідні нормативні чи інформаційні ресурси, що стосуються структури (К)ДП 3-ї країни, такі як чинний(і) або який(і) розробляється(ються) довірчий(і) список(ски) 3-ї країни, список(ски) затверджених засобів інформаційної безпеки (напр., національний еквівалент надійних засобів створення підпису (НЗСП=SSCD) та/або кваліфікованих засобів створення підпису (КЗСП=QSCD), список затверджених органів з оцінки відповідності 3-ї країни та опис засадничих правил тощо.
- ◆ v. Самооцінка за ст. 14 eIDAS.
- ◆ vi. Перелік стандартів, на які посилаються / які використовуються в структурі (К)ДП третьої країни, й опис того, як ці стандарти використовуються / як їх дотримуються.

ЄК проводить попередню оцінку структури (К) ДП третьої країни на предмет її сумісності зі структурою за eIDAS. Він подає попередній звіт про оцінку державам-членам ЄС і, у разі позитивного висновку щодо сумісності структури третьої країни зі структурою за eIDAS, консультує їх щодо подальшої взаємодії з третьою країною з метою проведення детального (взаємного) оцінювання як наступного кроку.

На цьому етапі також може бути проведено добровільну технічну апробацію, особливо якщо вона не проводилася на попередньому етапі.

1.2.3. Детальне взаємооцінювання

ЄК проводить детальне оцінювання, що дасть змогу ухвалити рішення щодо доцільності підготовки УВВ/MRA та визначити основні принципи плану виконання, плану моніторингу і плану припинення дії УВВ/MRA. На цьому етапі може проводитися добровільна технічна та/або законодавча апробація, зокрема через пілотні проекти.

Ця фаза також передбачає укладення плану виконання УВВ/MRA, в тому числі має бути запропоновано програмний вказівник для КДС ЄК (EC LOTL) як конкретний результат виконання, що відповідає умовам УВВ, а також опис його використання та тлумачення.

Так само у рамках процесу складання тексту УВВ/MRA або паралельно з його складанням слід розробити й обговорити з третьою країною/організацією-кандидатом план моніторингу УВВ/MRA і план припинення дії УВВ/MRA.

У планах моніторингу слід враховувати обмін щорічними звітами між підписантами УВВ/MRA, в тому числі до прикладу, звітами про виявлення змін у відповідних рамкових угодах, наглядовій діяльності, урахування нової судової практики, повідомлень про порушення безпеки та/або захисту особистих даних тощо. Також слід передбачити необхідність щорічного аналізу наглядової діяльності (на основі отриманих звітів і потенційних скарг) та проведення офіційного поглибленого аналізу імплементації УВВ/MRA (кожні 3 роки).

1.2.4. Підготовка УВВ/MRA

У разі позитивних результатів оцінювання обома сторонами можна переходити до етапів складання тексту угоди та переговорів щодо ухвалення рішення про укладання УВВ/MRA.

З боку ЄС це передбачає, що ЄК повинен ініціювати процедуру за ст. 218 та скласти текст УВВ/MRA на основі типового закону Комісії ООН з прав міжнародної торгівлі (UNCITRAL). Перед підписанням УВВ повинен схвалити Європейський Парламент і затвердити Рада ЄС.

В рамках складання проекту УВВ/MRA або паралельно з цим складанням слід затвердити й остаточно погодити проекти виконання, моніторингу та припинення дії УВВ/MRA.

Остаточне погодження УВВ/MRA і пов'язаних з нею планів може передбачати один або кілька раундів переговорів між сторонами.

1.2.5. Підписання, виконання та моніторинг і припинення дії УВВ/MRA

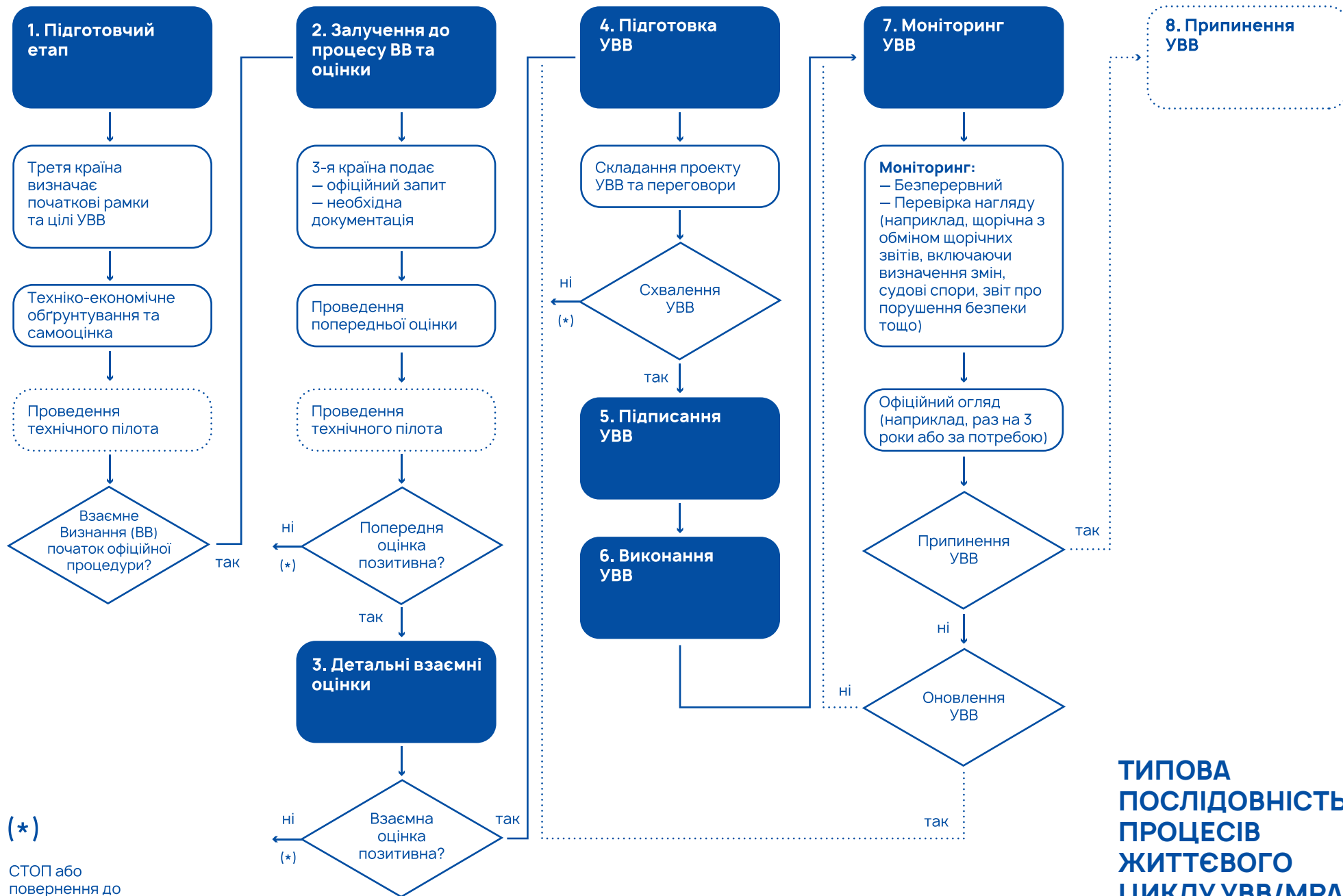
Після підписання УВВ та початку виконання УВВ/MRA відповідно до плану проводиться моніторинг виконання УВВ. Протягом усього циклу виконання УВВ необхідно проводити моніторинг на предмет правильності її виконання обома сторонами. Сюди входить моніторинг впровадження структури КНДП/КПД третьої країни, згідно з її оцінкою. Моніторинг також повинен передбачати обмін щорічними звітами (у тому числі щодо виявлення змін, новітніх судових практик, порушення безпеки тощо).

Проведення контрольних-наглядових заходів і повної оцінки УВВ/MRA визначено в плані моніторингу УВВ/MRA. Можлива також позапланова оцінка УВВ, наприклад, у зв'язку зі змінами у структурі чи фреймворках, інцидентами чи з будь-якими іншими значними чинниками.

Результатом моніторингу УВВ/MRA може стати необхідність оновлення або припинення дії УВВ/MRA.

1.2.6. Припинення дії УВВ/MRA

Наслідки припинення дії УВВ/MRA слід передбачити до підписання УВВ/MRA та викласти у плані припинення дії. У разі необхідності припинення дії УВВ сторони повинні затвердити оновлену редакцію плану припинення дії УВВ та виконати його відповідним чином.



(*)
СТОП або повернення до попереднього кроку

ТИПОВА ПОСЛІДОВНІСТЬ ПРОЦЕСІВ ЖИТТЄВОГО ЦИКЛУ УВВ/MRA ЗА СТ. 14

1.3. СФЕРА ЗАСТОСУВАННЯ І МЕТА ЦЬОГО ДОКУМЕНТА І ДОДАТКІВ ДО НЬОГО

Зважаючи на те, що дедалі більше країн виявляють зацікавленість у приведенні довірчих послуг у відповідність із eIDAS та зацікавлені у взаємному визнанні довірчих послуг, аналіз показує, що третім країнам стали б у пригоді конкретні настанови.

Мета цього документа і додатків до нього – запропонувати такі настанови, зосередившись на наданні допомоги третім країнам-кандидатам на підготовчому етапі:

- ◆ у проведенні самооцінювання сумісності структури НДП/ДП 3-ї країни зі структурою КНДП/КДП за eIDAS;
- ◆ у визначенні вимог, рекомендацій та елементів технічних змін, необхідних для імплементації УВВ, задля забезпечення належного перебігу цієї імплементації;
- ◆ та у підготовці технічної апробації (за потреби).

Цей документ і додатки до нього укладено у відповідності зі структурними блоками (Сервісами для Цифрових Підписів (DSS), TL-Manager і Trusted List Browser засобів eSignature Механізму "З'єднання Європи" (CEF), які було або буде адаптовано для аналогів КДП з-поза ЄС або щодо яких надано версію для суб'єктів, що не входять до ЄС (TL-Manager).

1.4. СТРУКТУРА ДОКУМЕНТА

У розділі 2 цього документа розглянуто мінімальні вимоги до структури НДП/ДП, про які повинна знати третя країна, коли розглядає можливість взаємного визнання КНДП/КДП з ЄС.

Настанови щодо цих вимог супроводжує контрольний лист для самооцінювання щодо УВВ (документ Excel), структурований відповідно до чотирьох засадничих складників (законодавчий контекст, нагляд і аудит, найкращі практики та модель формування довіри, як описано в [ETSI TR 103 684]), що дозволяє третій країні підготувати самостійну оцінку поточної структури НДП/ДП, яка існує або розробляється, з урахуванням типів довірчих послуг, які запропоновані до включення до переговорів щодо взаємного визнання (УВВ) та відповідності вимогам до КНДП ЄС згідно з Регламентом eIDAS. Розділ 2 і контрольний лист спрямовані на те, щоб допомогти третім країнам у поінформований спосіб досягти таких цілей:

- ◆ самооцінювання сумісності відповідних структур НДП/ДП з eIDAS на предмет рівнозначності законодавства щодо тих національних довірчих сервісів, які претендують бути визнаними юридично рівнозначними КДП ЄС;
- ◆ визначення основних технічних припущень, що взаємопов'язують, з одного боку, законодавчі вимоги eIDAS, яким мають відповідати національні довірчі сервіси, що можуть бути визнаними юридично рівнозначними КДП ЄС, а з іншого боку, подання щодо виконання УВВ на основі довірчого списку.
- ◆ самооцінювання сумісності процедур надання дозволу, нагляду й аудиту тих національних довірчих сервісів, які претендують на взаємне визнання;
- ◆ визначення фактичних еталонних стандартів для впровадження КНДП/КДП ЄС, спрощення порівняння з технічною структурою та фреймворками найкращих практик для національних НДП/ДП;
- ◆ створення національного довірчого списку третьої країни як моделі довірчого подання для підтвердження статусу національних довірчих послуг, що претендують на визнання юридично рівнозначними КДП ЄС, і розширення довірчого списку для встановлення та оновлення інформації щодо виконання УВВ/MRA і транскордонного визнання юридично рівнозначних (кваліфікованих) довірчих послуг.

У розділі 3 йдеться про технічні імплікації або припущення щодо технічних специфікацій, зазначених у Розділі 2, що становлять основу такого взаємного визнання і повинні бути врегульовані до впровадження в дію УВВ через КДС ЄК і довірчий список третьої країни, щоб забезпечити безперебійність цього впровадження. За потреби буде розглянуто взаємозв'язок технічних рекомендацій та/або вимог із методом встановлення та виконання моделі формування довіри на основі довірчих списків країн-членів ЄС і зокрема КДС ЄК. До переліку рекомендацій/вимог входять рекомендації, що застосовуються до вмісту довірчого списку третьої країни (це, зокрема, може вимагати коригування наявних довірчих списків третьої країни).

У розділі 4 зазначено необхідні корективи до КДС ЄК (і до довірчого списку третьої країни) для реалізації виконання УВВ за ст. 14 eIDAS, тобто для викладу в технічних термінах суті УВВ та уможливлення взаємної перевірки юридичної рівнозначності між відповідними довірчими послугами третьої країни та КДП ЄС. Обов'язковою передумовою є публікація третьою країною довірчого списку відповідно до [ETSI TS 119 612] та викладеними вище рекомендаціям/вимогам так, щоб КДС ЄК міг вказувати на / інтегруватись з довірчим списком третьої країни, та щоб технічно уможливити взаємне визнання через встановлення взаємозв'язку КДС ЄК з довірчим списком третьої країни. КДС ЄК повинен містити програмний вказівник на довірчий список третьої країни, і навпаки – довірчий список третьої країни повинен містити програмний вказівник на КДС ЄК. Обидві вказівки міститимуть елементи зіставлення взаємного визнання між КДП КЧ ЄС та ДП третьої країни, що відображають суть УВВ між третьою країною та ЄС, укладеної відповідно до ст. 14 Регламенту eIDAS.

У розділ 5 йдеться про необхідну адаптацію стандартів (головно [ETSI TS 119 615]) для валідації електронних підписів/печаток третьої країни на основі вмісту КДС ЄК, що вказує на довірчий список третьої країни. ЄК відповідно адаптував або адаптуватиме структурні блоки eSignature Механізму "З'єднання Європи", зокрема, DSS eSignature для валідації вихідних даних НДП/ДП третьої країни, визнаних рівнозначними за вмістом КДС ЄК, non-EUTL-Manager, щоб дати змогу країнам, що не входять до ЄС, адмініструвати довірчий список і Trusted List Browser для відображення вмісту довірчих списків ЄС та інших країн, на які у КДС ЄК містяться програмні вказівники.

2. МІНІМАЛЬНІ ВИМОГИ ДО СТРУКТУРИ НДП/ДП ТРЕТІХ КРАЇН ЧЕКЛИСТ ДЛЯ САМОСТІЙНОГО ОЦІНЮВАННЯ

2.1. Законодавчі вимоги

2.2. Вимоги щодо нагляду й оцінювання відповідності

2.3. Технічні умови та найкращі практики

2.4. Модель формування Довіри



2. МІНІМАЛЬНІ ВИМОГИ ДО СТРУКТУРИ НДП/ДП ТРЕТІХ КРАЇН

ЧЕКЛИСТ ДЛЯ САМООЦІНЮВАННЯ

Супровідний документ у додатку [чеклист УВВ/МРА] дає можливість третім країнам самостійно провести оцінювання відповідності їх національної структури (кваліфікованих) надавачів довірчих послуг і (кваліфікованих) довірчих послуг, які вони надають, (надалі (К)НДП/(К)ДП) вимогам ЄС до КНДП/КДП згідно з Регламентом eIDAS.

Цей інструмент у формі документу Excel пропонує різноманітні блоки, що охоплюють чотири засадничі складники, описані у стандарті [ETSI TR 103 684], уможливаючи порівняння різних довірчих моделей або структур (К)НДП/(К)ДП.

У подальших розділах описано вміст вимог [чеклиста УВВ] у такому порядку:

- ◆ У розділі 2.1 "Законодавчі вимоги" описано перші два блоки, які стосуються вимог щодо "законодавчого контексту", це дозволяє порівняти нормативну базу \ фреймворки третьої країни з законодавчими вимогами Регламенту eIDAS щодо КНДП/КДП ("P1. Законодавча відповідність eIDAS") і з модельними положеннями договорів міжнародної торгівлі (UNCITRAL, Комісії ООН) та іншими законодавчими нормами ЄС, пов'язаними з eIDAS, зокрема щодо захисту персональних даних і конфіденційності, щодо захисту прав споживачів, свободи слова ("P1. Законодавство – нормативно-правовий базис ООН-ЄС").
- ◆ У розділі 2.2 "Вимоги щодо нагляду та оцінки відповідності" описано в "P2. Нагляд та аудит", що дозволяє порівняння відповідність фреймворків третьої країни на основі наданої детальної інформації про режим нагляду та аудиту структури (К)ДП.
- ◆ У розділі 2.3 "Технічні аспекти та найкращі практики" описано блок "P3. Технічні аспекти та найкращі практики", що дозволяє провести порівняння структури третьої країни на основі надання детальної інформації про встановлені та застосовані технічні специфікації та стандарти для впровадження (К)НДП/(К)ДП.
- ◆ У розділі 2.4 "Модель формування довіри" описано блок "P4. Модель формування довіри", що дозволяє провести порівняння структури третьої країни на основі надання детальної інформації про використовувану модель формування довіри зокрема щодо довірчих списків третьої країни.

За потреби, вищезазначені розділи містять відповідні технічні специфікації, припущення та/або переліки технічних змін, необхідні для імплементації УВВ/МРА, та відсилання на відповідні частини розділу 3 для отримання додаткової інформації.

2.1. ЗАКОНОДАВЧІ ВИМОГИ

Основні законодавчі вимоги для визнання довірчих послуг, що надаються НДП, заснованими в третій країні, юридично рівнозначними КДП ЄС, що надаються КНДП, заснованими в ЄС, такі:

Додатково для визнання потрібно виконати ще дві умови:

- ◆ (а) Юридична рівнозначність цих НДП/ДП третьої країни повинна бути визнана угодою, укладеною між ЄС і відповідною третьою країною або міжнародною організацією відповідно до статті 218 ДФЄС (TFEU); та

- ◆ (б) Угода повинна бути взаємною, тобто КДП, що надаються КНДП, створеним в ЄС, повинні бути визнані юридично рівнозначними довірчим послугам, що надаються надавачами довірчих послуг у третій країні, з якою укладено угоду.

Вимога щодо відповідності НДП/ДП третьої країни вимогам Регламенту eIDAS, які застосовуються до КНДП/КДП ЄС, детальніше описана у наступній таблиці для кожного з дев'яти видів КДП ЄС, положення щодо яких викладено в Регламенті eIDAS:

Таблиця 1: Вимоги eIDAS, що застосовуються до КНДП/КДП

Загальні вимоги eIDAS, що застосовуються до всіх типів КДП	Конкретні вимоги eIDAS, що застосовуються до певного типу КДП
<ul style="list-style-type: none"> • Стаття 5 – Обробка та захист даних • Стаття 13 – Відповідальність та обов'язок доведення • Стаття 15 – Доступність для людей з інвалідністю • Стаття 19.1 – Оцінка ризиків, пов'язаних з безпекою та комплексна фінансово-юридична експертиза • Стаття 19.2 – Повідомлення про порушення безпеки та захисту персональних даних • Стаття 20 – Нагляд за КНДП <ul style="list-style-type: none"> • Аудит щонайменше кожні 24 місяці органом оцінки відповідності, акредитованим згідно з eIDAS, для підтвердження відповідності eIDAS • НДП дозволяє Наглядовому органу (НО) та ООВ перевіряти його відповідність eIDAS • Усунення будь-яких невідповідностей вимогам eIDAS відповідно до вказівок НО • Повідомлення про намір надавати КДП та первинний звіт про оцінку відповідності • КНДП може розпочати надавати КДП після реєстрації його кваліфікованого статусу в довірчому списку • Стаття 23 – Використання Знака Довіри ЄС • Стаття 24.2 – Вимоги до КНДП <ul style="list-style-type: none"> • Інформувати НО про будь-які зміни у забезпеченні КДП та про намір припинити їх надання; • Вимоги до персоналу; • Фінансові ресурси та/або страхування відповідальності; • Інформація для споживачів; • Використання надійних систем і продуктів; • Використання надійних систем для зберігання даних (в тому числі персональних даних); • Належні заходи проти фальсифікації та викрадення даних; • Записування і доступність даних, пов'язаних із діяльністю; • Актуальний план припинення дії; • Обробка персональних даних відповідно до законодавства. 	<p>Надання кваліфікованих сертифікатів для електронних підписів:</p> <ul style="list-style-type: none"> • Ст. 24.1 (a–d) • ст. 24.2 (k) • ст. 24.3 • Ст. 24.4 • Ст. 28.1 та Додаток I, ст. 28 (2), ст. 28 (3), ст. 28 (4), ст. 28 (5)
	<p>Надання кваліфікованих сертифікатів для електронних печаток:</p> <ul style="list-style-type: none"> • Ст. 24.1 (a–d) • ст. 24.2 (k) ст. 24.3 • Ст. 24.4 • Ст. 38.1 та Додаток III, ст. 38. (2), ст. 38. (3), ст. 38. (4), ст. 38. (5)
	<p>Надання кваліфікованих сертифікатів для автентифікації вебсайтів:</p> <ul style="list-style-type: none"> • Ст. 24.1 (a–d) • ст. 24.2 (k) • ст. 24.3 • Ст. 24.4 • Ст. 45.1 та Додаток IV
	<p>Кваліфікований сервіс валідації кваліфікованих електронних підписів:</p> <ul style="list-style-type: none"> • Ст. 33.1
	<p>Кваліфікований сервіс валідації кваліфікованих електронних печаток:</p> <ul style="list-style-type: none"> • Ст. 40
	<p>Кваліфікований сервіс архівування кваліфікованих електронних підписів:</p> <ul style="list-style-type: none"> • Ст. 34.1
	<p>Кваліфікований сервіс архівування кваліфікованих електронних печаток:</p> <ul style="list-style-type: none"> • Ст. 40
	<p>Надання кваліфікованих позначок часу:</p> <ul style="list-style-type: none"> • Ст. 42.1
	<p>Кваліфіковані сервіси електронної доставки:</p> <ul style="list-style-type: none"> • Ст. 44.1

"P1. Законодавство – зіставний аналіз з eIDAS" та "P1. Модельне Законодавство для зіставлення з нормативно-правовою базою ООН-ЄС" що дає змогу 3-м країнам-кандидатам здійснити самооцінювання з використанням [чеклист УВВ]:

- ◆ Рівнозначність законодавчої бази третьої країни щодо НДП/ДП Регламентів eIDAS щодо КНДП/КДП;
- ◆ Відповідність законодавчої бази третьої країни (щодо НДП/ДП) типовому закону Комісії ООН з прав міжнародної торгівлі (UNCITRAL) та іншими законами ЄС, пов'язаними з eIDAS, зокрема щодо захисту персональних даних і конфіденційності, щодо захисту споживачів і прав споживачів, свободи слова.

Основне технічне припущення:

Щодо КДП ЄС, які полягають у видачі кваліфікованих сертифікатів для електронних підписів, кваліфікованих сертифікатів для електронних печаток і кваліфікованих сертифікатів для автентифікації вебсайтів, існують основні технічні припущення, які слід враховувати, коли йдеться про вимоги встановлені:

- ◆ у пункті (a) eIDAS, додатки I, III, IV;
- ◆ у пункті (b) eIDAS, додатки I, III, IV; та
- ◆ у пункті (j) eIDAS, додатки I, III.

Ці технічні припущення детально описано в розділі 3.1.1.

2.2. ВИМОГИ ЩОДО НАГЛЯДУ ТА ОЦІНЮВАННЯ ВІДПОВІДНОСТІ

Передумовою надання КДП претендентом на статус КНДП/КДП є проходження перевірки органом з оцінювання відповідності (ООВ=СAB), акредитованим згідно з eIDAS, що підтверджується звітом про оцінку відповідності (аудит) (аЗОВ=аСAR), висновком якого є те, що КНДП і КДП, які він надає, відповідають вимогам Регламенту eIDAS. Коли потенційний КНДП повідомляє компетентний національний наглядовий орган (НО) про свій намір надавати КДП, разом із таким повідомленням він повинен подати ЗОВ / СAR. На основі поданого ЗОВ/СAR НО перевірить відповідність претендента на статус КНДП/КДП вимогам Регламенту eIDAS і вдовольнить або відхилить заявку на кваліфікований статус.

Отримавши кваліфікований статус для надання ДП, КНДП повинен проходити перевірку ООВ/СAB, акредитованим згідно з eIDAS, не рідше, ніж раз на 24 місяці, та подавати ЗОВ/СAR в строк до трьох робочих днів з дати його отримання. Мета перевірки – підтвердити відповідність КНДП/КДП вимогам, викладеним у Регламенті eIDAS.

Окрім первинного аудиту та перевірки що два роки, компетентний НО може в будь-який час провести перевірку КНДП/КДП або таку перевірку може бути проведено на вимогу НО ООВ, акредитованим згідно з eIDAS, щоб підтвердити відповідність Регламенту eIDAS.

Утім у Регламенті eIDAS не вказано конкретної схеми оцінювання відповідності (або сертифікації), згідно з якою повинен бути акредитований ООВ. Натомість Регламент eIDAS вимагає акредитації ООВ у рамках Регламенту (ЄС) № 765/2008⁶, який є загальним європейським нормативно-правовим актом щодо акредитації. До того ж встановлено вимогу, щоб схема оцінювання відповідності (СОВ), що використовується ООВ, була орієнтована на eIDAS.

Європейська кооперація з акредитації⁷ (ЕА) є органом, за яким Регламентом (ЄС) № 765/2008 закріплено право управляти системою взаємного оцінювання серед національних органів з акредитації (НОА) держав-членів ЄС та інших європейських країн. ЕА використовує схему акредитації⁸ eIDAS, засновану на [ISO/IEC 17065], з доповненнями з [EN 319 403] як один із можливих способів для ООВ оцінити відповідність вимогам Регламенту eIDAS.

Як показано на рисунку 2, схема акредитації eIDAS, рекомендована ЕА, вимагає:

- ◆ Щоб національні органи з акредитації здійснювали акредитацію ООВ відповідно до [ISO/IEC17011]
- ◆ Щоб акредитація ООВ ґрунтувалася на фреймворку сертифікації [ISO / IEC 17065]
- ◆ Щоб фреймворк акредитації [ISO/IEC17065] ООВ було доповнено [EN 319 403], де визначено додаткові спеціальні вимоги до ООВ, що здійснюють сертифікацію НДП/ДП згідно зі встановленими критеріями (ці критерії визначаються як "Нормативний документ")
- ◆ Акредитації ООВ / СAB для підтвердження компетенції ООВ проводити оцінку відповідності НДП/ДП вимогам Регламенту eIDAS. Власне, у цій схемі Регламент eIDAS визначено як Нормативний документ, що встановлює критерії/вимоги, за якими повинна оцінюватися відповідність НДП/ДП.

Рисунок 2: Рекомендована ЕА схема акредитації ООВ за eIDAS

EA-MLA (EA 1/06) – IAF PR4

Level 1 – ISO/IEC 17011

Level 2 – Certification

Level 3 – ISO/IEC 17065

Level 4 – EN 319 403

Level 5 – REG (EU) 910/2014

6. OJ L 218, 13.8.2008, p. 30–47. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32008R0765&locale=en>

7. <http://www.european-accreditation.org/>

8. EA Resolution 2014 (34) 22 and EA document EAGA(14)31: <https://european-accreditation.org/wpcontent/uploads/2018/10/34th-ea-ga-approved-resolutions-.pdf>

Особливістю схеми акредитації за eIDAS, рекомендованої ЕА, є те, що вимоги, за якими КНДП/КДП повинні проходити сертифікацію, є не технічними вимогами, а технологічно нейтральними законодавчими вимогами, представленими через функціональні цілі, які багато в чому є продовженням загальної політики Регламенту eIDAS щодо технологічної нейтральності.

Отже, Нормативний документ є не технічним стандартом, а вимогами застосовними до КНДП/КДП з Регламенту eIDAS. Ні Регламент eIDAS, ні ЕА не вказують чинних технічних критеріїв або схем технічної сертифікації, що впливають із положень Регламенту eIDAS.

До того ж відповідно до Регламенту eIDAS, жоден стандарт не є і не може бути обов'язковим для отримання КНДП або КДП кваліфікованого статусу. КНДП мають право застосовувати будь-який стандарт або взагалі не застосовувати жодного стандарту, за умови, що зможуть продемонструвати, що вони та КДП, які вони надають, відповідають вимогам Регламенту eIDAS.

До того ж на сьогодні не прийнято жодного вторинного законодавства щодо eIDAS, яке посилалося б на будь-який стандарт, що створювало би правову презумпцію відповідності будь-яким вимогам Регламенту eIDAS для КНДП, які вирішили дотримуватися цього стандарту, або для КДП, які вони надають. Якби таке вторинне законодавство було прийнято, відповідність таким стандартам залишатиметься для КНДП добровільною: їх використання залишиться необов'язковим.

На основі механізму взаємного оцінювання, запровадженого на рівні НОА Регламентом (ЄС) 765/2008, та того факту, що більшість НОА ЄС є підписантами Багатосторонньої угоди про визнання (MLA) Міжнародного форуму з акредитації (IAF)⁹ щодо ISO/IEC 17065, КНДП можуть скористатися послугами ООВ з будь-якої країни ЄС, акредитованого НОА з країни, що не є країною, де створено КНДП.

РЕКОМЕНДАЦІЇ ДЛЯ ТРЕТІХ КРАЇН

Саме схему акредитації Багатосторонньої угоди про визнання (MLA) Міжнародного форуму з акредитації (IAF), засновану на [ISO/IEC 17065] (в поєднанні з [EN 319 403]), кандидати від третіх країн можуть вважати базою формування своєї національної схеми сертифікації КНДП/КДП. Схема, ґрунтована на ISO/IEC 17065 та доповнена [EN 319 403], застосовується до будь-якого типу КНДП/КДП для оцінювання відповідно до будь-якого стандарту, технічних специфікацій або регламентів. Вище запропонована схема цілковито незалежна від Регламенту eIDAS. Рекомендована

ЕА схема за eIDAS додає до загальної схеми Регламенту eIDAS як нормативний документ, відповідно до якого слід оцінювати відповідність КНДП/КДП. Третя країна, що не входить до ЄС, може діяти подібним чином, додаючи власні законодавчі чи технічні специфікації як нормативні критерії, згідно з якими повинна оцінюватися відповідність національних НДП/ДП.

Однак для укладення УВВ за ст. 14 eIDAS важливо, щоб нормативні критерії, за якими будуть оцінюватися НДП/ДП третьої країни, відповідали вимогам eIDAS, що застосовуються до КНДП/КДП ЄС, або навіть перевищували їх.

Таким чином, треті країни можуть розширити та доопрацювати схему, ґрунтовану на [EN 319 403], шляхом створення національної, гармонізованої, спеціальної та повної схеми сертифікації.

Ця національна схема повинна достатньо детально обумовлювати технічні аспекти, точний набір засобів контролю та цілей контролю, які ООВ повинен буде використовувати для оцінювання відповідності КНДП/КДП на основі загальніших нормативних положень. Якщо така національна схема не є обов'язковою, у разі використання для сертифікації КНДП/КДП вона може бути пов'язана з презумпцією відповідності цільовим критеріям і законодавчим вимогам.

Рекомендація:

Оцінку відповідності КНДП/КДП третьої країни, що мають на меті домогтися рівнозначності КНДП/КДП ЄС, доцільно розробляти на основі стандартів IAF MLA ISO/IEC 17065, доповнених ETSI EN 319 403-1 для оцінювання відповідності критеріям, які відповідають вимогам Регламенту eIDAS або перевищують їх.

Альтернативний варіант передбачає проведення оцінювання національної системи оцінки відповідності для НДП/ДП, продемонструвавши її рівнозначність.

Цьому може сприяти посилання в національному законодавстві на стандарти як обов'язкові нормативні документи (всупереч Регламенту eIDAS) або як специфікації, що передбачають презумпцію відповідності належним вимогам, коли їх виконують (подібно до Регламенту eIDAS).

Однією з переваг використання схеми, яку обстоює ЕА, згідно з фреймворками, ґрунтованими на IAF MLA за ISO/IEC 17065, є легкий доступ до 30 наявних ООВ, акредитованих за eIDAS.

9. <https://www.iaf.eu>

Їх використання національним НДП третьої країни для оцінювання його відповідності національним вимогам та демонстрації відповідності ДП, які він надає, вимогам eIDAS, було б значно простішим, якби різниця між національною схемою та схемою, що підтримує ЕА, була мінімальною.

Блок "Р2. Нагляд та аудит" супровідного документа [чеклист УВВ/МРА] дає змогу третій країні порівняти режим нагляду й аудиту щодо їхніх (К)НДП/(К)ДП з режимами нагляду й оцінювання відповідності за eIDAS.

Однією з переваг використання схеми, яку обстоює ЕА, згідно з фреймворками, ґрунтованими на IAF MLA за ISO/IEC 17065, є легкий доступ до 30 наявних ООВ, акредитованих за eIDAS. Їх використання національним НДП третьої країни для оцінювання його відповідності національним вимогам та демонстрації відповідності ДП, які він надає, вимогам eIDAS, було б значно простішим, якби різниця між національною схемою та схемою, що підтримує ЕА, була мінімальною.

Блок "Р2. Нагляд та аудит" супровідного документа [чеклист УВВ/МРА] дає змогу третій країні порівняти режим нагляду й аудиту щодо їхніх (К)НДП/(К)ДП з режимами нагляду й оцінювання відповідності за eIDAS.

2.3. ТЕХНІЧНІ УМОВИ ТА НАЙКРАЩІ ПРАКТИКИ

Як зазначалося вище, на сьогодні не прийнято жодного вторинного законодавства щодо eIDAS із посиланням на будь-який стандарт, який створював би правову презумпцію відповідності будь-яким вимогам Регламенту eIDAS для КНДП, які вирішили дотримуватися цього стандарту, або для КДП, які вони надають. КНДП ЄС можуть застосовувати будь-який стандарт або взагалі не застосовувати жодного стандарту, за умови, що зможуть продемонструвати, що вони та КДП, які вони надають, відповідають вимогам Регламенту eIDAS. Те саме стосується НДП/ДП третьої країни, що ставлять собі за мету домогтися юридичної рівнозначності КНДП/КДП ЄС.

Утім було розроблено ряд стандартів, що їх застосовують КНДП/КДП ЄС, та які використовуються як орієнтири акредитованими ООВ для оцінювання відповідності вимогам Регламенту eIDAS.

Блок "Р3. Технічні аспекти та найкращі практики" супровідного документа [контрольний чеклист УВВ] дає змогу третім країнам порівняти фреймворки технічних аспектів і найкращих практик, пов'язані з їхніми КНДП/КДП, з нижченаведеними технічними специфікаціями та найкращими практиками за eIDAS.

2.3.1. НДП/ДП третьої країни, що мають на меті домогтися юридичної рівнозначності з КНДП/КДП ЄС

НДП третьої країни, що мають на меті домогтися юридичної рівнозначності КНДП/КДП ЄС, а також ООВ, що оцінюють відповідність НДП/ДП третьої країни належним вимогам eIDAS, рекомендовано брати за основу такі стандарти:

Таблиця 2: Рекомендовані стандарти для впровадження КНДП/КДП

Види КДП за eIDAS	Стандарти
Надання кваліфікованих сертифікатів для електронних підписів	ETSI EN 319 411-2 (вимагає відповідності ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 412-2, ETSI EN 319 412-5) ETSI TR 119 411-4
Надання кваліфікованих сертифікатів для електронних печаток	ETSI EN 319 411-2 (вимагає відповідності ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 412-3, ETSI EN 319 412-5) ETSI TR 119 411-4
Надання кваліфікованих сертифікатів для автентифікації вебсайтів	ETSI EN 319 411-2 (вимагає відповідності ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 412-4, ETSI EN 319 412-5) ETSI TR 119 411-4
Кваліфікований сервіс валідації кваліфікованих електронних підписів	ETSI TS 119 441 (вимагає відповідності ETSI EN 319 401), ETSI TS 119 442, ETSI EN 319 102-1, ETSI TS 119 102-2 ETSI TS 119 172-4, ETSI TS 119 615
Кваліфікований сервіс валідації кваліфікованих електронних печаток	ETSI TS 119 441 (вимагає відповідності ETSI EN 319 401), ETSI TS 119 442, ETSI EN 319 102-1, ETSI TS 119 102-2 ETSI TS 119 172-4, ETSI TS 119 615
Кваліфікований сервіс зберігання/ архівування (кваліфікованих електронних підписів)	ETSI EN 319 401, ETSI TS 119 511, ETSI TS 119 512
Кваліфікований сервіс зберігання кваліфікованих електронних печаток	ETSI EN 319 401, ETSI TS 119 511, ETSI TS 119 512
Надання кваліфікованих позначок часу	ETSI EN 319 421 (вимагає відповідності ETSI EN 319 401), ETSI EN 319 422
Кваліфіковані послуги реєстрованої електронної доставки	ETSI EN 319 401 ETSI EN 319 521, ETSI EN 319 522, ETSI TS 119 524 ETSI EN 319 531, ETSI EN 319 532, ETSI TS 119 534

Слід зазначити, що якість цих стандартів, їх придатність для використання КНДП для задоволення вимог Регламенту eIDAS, а отже й належність посилання на них у контексті виконання вимог ще не було офіційно оцінено.

2.3.2. Формати електронного підпису/печатки

Для УВВ/MRA за ст. 14 визнання в ЄС розширених електронних підписів (AdESigs) або розширених електронних печаток (AdESeals) не є обов'язковим, якщо створення цифрового підпису або, відповідно, печатки відбувається у країні, що не входить до ЄС.

За умови що електронні підписи з-поза ЄС відповідають вимогам ст. 26 (AdESigs), а електронні печатки з-поза ЄС відповідають вимогам ст. 26 (AdESeals), їх юридична сила і прийнятність у статусі доказів на судових процесах не заперечуватиметься лише на тих підставах, що вони мають електронну форму або що вони не відповідають вимогам щодо кваліфікованих електронних підписів/печаток (ст. 25.1 / ст. 35.1). Також, коли ці AdESigs/AdESeals з-поза ЄС створено у форматах, встановлених у IPK (ЄС) 2015/1506¹⁰, їх повинні визнати чинними у всіх державах-членах ЄС для онлайн-послуг, що пропонуються державними органами або від їх імені, коли для використання таких послуг потрібні AdESigs/AdESeals¹¹.

Щодо форматів цифрових підписів та електронних печаток ЄС слід орієнтуватися на список стандартних форматів, на які посилається IPK (ЄС) 2015/1506, а також подальші стандарти ETSI EN 319 122-1, ETSI EN 319 132-1, ETSI EN 319 142-1 та ETSI EN 319 162-1. На ці стандарти, ймовірно, будуть додаткові посилання в нових редакціях або поправках до IPK (ЄС) 2015/1506 з поступовим замощенням попередніх посилань.

Рекомендація:

Технічні формати для створення AdESigs/AdESeals повинні відповідати стандартним форматам, зазначеним в IPK (ЄС) 2015/1506, або радше подальшим редакціями стандартів ETSI EN 319 122-1, ETSI EN 319 132-1, ETSI EN 319 142-1 та ETSI EN 319 162-1.

Слід зазначити, що зобов'язання за ст. 27 та ст. 37 Регламенту eIDAS стосуються не сторони яка створює підпис/печатку, а "сторони, яка приймає", тобто онлайн-послуг, що пропонуються

державним органом або від його імені, коли для використання таких послуг потрібні AdESigs/AdESeals. Слід також зазначити, що створення AdESigs / AdESeals у форматі, вказаному в IPK (ЄС) 2015/1506, не передбачає презумпції відповідності вимогам ст. 26 / ст. 36.

2.3.3. Засіб створення кваліфікованого електронного підпису / печатки (QSigCD/QSealCD)

Регламент eIDAS не встановлює жодних конкретних (ст. 14) вимог щодо взаємного визнання посиленних електронних підписів або посиленних електронних печаток. Навіть без будь-якої угоди третьої країни з ЄС за ст. 14 будь-який електронний підпис / печатка з-поза ЄС, що відповідає вимогам ст. 26 / ст. 36 Регламенту відповідно, може бути визнаний посиленим електронним підписом або посиленою електронною печаткою. Стандартні формати, перелічені в попередньому розділі, допоможуть максимізувати сумісність.

Для того, щоб електронні підписи / печатки з-поза ЄС, які відповідають вимогам ст. 26 / ст. 36 Регламенту eIDAS відповідно, можна було розглядати як QESigs/QESeals ЄС, вони не тільки повинні підтримуватися сертифікатами, визнаними рівнозначними або такими, що відповідають вимогам до QESigs/QESeals ЄС, а й бути створеними кваліфікованими засобами створення електронного підпису/печатки (QSigCD / QSealCD).

Оскільки QSigCD/QSealCD або їх надання не є КДП, в Регламенті eIDAS, зокрема у його статті 14, немає положень про визнання засобів створення підпису/печатки з-поза ЄС кваліфікованими засобами створення електронного підпису/печатки (QSigCD/QSealCD). На цей час для підпису / печатки з-поза ЄС єдиний спосіб бути визнаними кваліфікованими засобами створення підпису / печатки – це відповідати вимогам Регламенту, а саме:

- ◆ а) (Ст. 29) Відповідати вимогам, викладеним у Додатку II;
- ◆ б) (Ст. 30) Для відповідності вимогам, викладеним у Додатку II:
 - ◆ і. бути сертифікованими,
 - ◆ ii. відповідними державними або приватними органами, уповноваженими державою-членом ЄС.
- ◆ с) Сертифікація відповідності Додаткові II повинна базуватися на:

10. OJ L 235, 9.9.2015, p. 37–41. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AJOL_2015_235_R_0006

11. Слід зазначити, що зобов'язання за ст. 27 та ст. 37 Регламенту eIDAS стосуються не сторони яка створює підпис/печатку, а "сторони, яка приймає", тобто онлайн-послуг, що пропонуються державним органом або від його імені, коли для використання таких послуг потрібні AdESigs/AdESeals. Слід також зазначити, що створення AdESigs / AdESeals у форматі, вказаному в IPK (ЄС) 2015/1506, не передбачає презумпції відповідності вимогам ст. 26 / ст. 36.

- ◆ i. Або переліку стандартів для оцінювання безпеки продуктів інформаційних технологій, встановленого ІРК (ЄС) 2016/650 (ст. 30 (3).а);
- ◆ ii. Або, коли можливо, альтернативному процесові, який спирається на аналогічні рівні безпеки та про який було повідомлено ЄК (ст. 30 (3).b).

Це не означає, що жоден засіб створення підписів/печаток з-поза ЄС не може бути сертифікованим та визнаним QSigCD/QSealCD. Багато засобів з-поза ЄС уже сертифіковано органами з сертифікації ЄС як QSigCD/QSealCD і фігурують у статті 31.2 у списку сертифікованих QSigCD/QSealCD, що його публікує ЄК на основі повідомлень держав-членів ЄС¹².

Це також не означає, що жоден орган із сертифікації з-поза ЄС не може сертифікувати засоби відповідно до статті 30 (3) Регламенту. Їм "просто" потрібно бути уповноваженими державою-членом ЄС відповідно до статті 30.1. Слід зазначити, що ЄК досі не прийняла жодних делегованих актів відповідно до статті 30(4) щодо встановлення конкретних критеріїв, яким повинні відповідати такі уповноважені органи, незалежно від того, є вони європейськими чи ні. Якщо такий делегований акт буде прийнято, він може передбачати конкретні критерії для органів, не уповноважених ЄС.

Вимога:

Щоб засіб було визнано QSigCD або QSealCD відповідно (незалежно від того, звідки він походить), такий засіб повинен відповідати вимогам Додатку II eIDAS, а його відповідність Додатку II повинна бути сертифікована відповідно до ст. 30 та ІРК (ЄС) 2016/650 органом з сертифікації, уповноваженим державою-членом ЄС.

Це стосується всіх типів засобів, у тому числі:

- ◆ коли дані створення електронного підпису або дані створення електронної печатки зберігаються у повністю (але не обов'язково винятково) керованому користувачем середовищі (наприклад, на смарткартах, криптографічних токенах USB або інших портативних криптографічних засобах), або
- ◆ коли даними створення електронного підпису або даними створення електронної печатки керує кваліфікований надавач довірчих послуг (КНДП) від імені власника підпису або власника печатки (наприклад, засоби віддаленого накладання підпису = RSS).

12. <https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds>

2.4 МОДЕЛЬ ФОРМУВАННЯ ДОВІРИ

З огляду на те, що довірчі списки держав-членів ЄС є юридичними установчими інструментами, які дозволяють перевірити чи надано КНДП/КДП кваліфікований статус, чи цей статус скасовано, а також беручи до уваги те, що УВВ за ст. 14 повинна вводитися в дію шляхом внесення до КДС ЄК програмного вказівника на відповідний довірчий список третьої країни, передумовою для укладення такої УВВ є створення та ведення третьою країною довірчого списку відповідно до [ETSI TS 119 612] та вимог і рекомендацій, наведених у цьому документі.

Вимога:

Третя країна повинна створити та вести довірчий список відповідно до [ETSI TS 119 612] та вимог і рекомендацій, наведених у цьому документі, вносячи до цього списку як мінімум НДП/ДП, визнані юридично рівнозначними КНДП/КДП ЄС.

Специфікації щодо створення, ведення, накладання підпису/печатку та публікації довірчих списків держав-членів ЄС, в тому числі інформації, що стосується КНДП/КДП, за яку відповідає кожна держава-член, викладено в ІРК (ЄС) 2015/1505 на основі [TS 119 612].

Ці специфікації з ІРК (ЄС) 2015/1505 містять правила щодо інтерпретації довірчих списків, які також доступні через поле Тип схеми/співтовариство/правила (зазначені в пункті 5.3.9) довірчого списку кожної держави-члена ЄС (<http://uri.etsi.org/TrstSvc/TrustedList/schemerules/EUcommon>).

Таким чином, "кваліфікований" статус довірчої послуги позначається поєднанням:

- ◆ а. значення "Ідентифікатор типу послуги" ("Sti") (яке може бути додатково уточнено в записі про послугу;
- ◆ б. статусу відповідно до значення поля "Поточний статус послуги", починаючи з дати, зазначеної в "Дата і час актуалізації поточного статусу".

Історична інформація про такий кваліфікований статус за потреби подається аналогічним чином.

Щодо КДП, які полягають у наданні кваліфікованих сертифікатів певного типу (тобто для eSigs, eSeals, авторизації вебсайтів), без додаткового повідомлення у відповідному довірчому списку, стейтменти у форматі, придатному

для автоматизованої обробки, які вважаються конститутивними для сертифікатів кінцевих об'єктів, виданих цими кваліфікованими довірчими сервісами, відповідно такі:

- ◆ id-etsi-qcs-QcCompliance (id-etsi-qcs 1) вираз/стейтмент, додатково уточнюється через "id-etsi-qcs-QcType (id-etsi-qcs 6)", що дозволяє підтвердити, що сертифікат видано як кваліфікований сертифікат, із зазначенням його виду, як визначено у стандарті ETSI EN 319 412-5 і
- ◆ id-etsi-qcs-QcSSCD (id-etsi-qcs 4) вираз/стейтмент для підтвердження того, що відповідний особистий ключ міститься в КЗСП ЄС.

Однак довірчий список може відхилити цю інформацію, включену до сертифіката, виданого зареєстрованим довірчим сервісом, використовуючи Кваліфікаційне розширення "Розширення інформації про послугу" ("Sie: Q") та конкретні "кваліфікатори", які застосовуються до одного або кількох наборів сертифікатів, ідентифікованих розширенням (напр., за допомогою певних об'єктних ідентифікаторів (OID) сертифікаційної політики, ключових патернів використання тощо).

"Цифрові ідентифікатори послуги" повинні використовуватися як точки формування довіри в контексті валідації електронних підписів або печаток, щодо яких потрібна валідація сертифікату відповідно до інформації з довірчого списку, для цього потрібен лише відкритий ключ та відповідна назва суб'єкта, яка є інформацією точки формування довіри (трастовим якорем). Коли відкритий ключ, що ідентифікує послугу, представлений кількома сертифікатами, їх слід розглядати як сертифікати точки формування довіри (трастового якоря), що передають інформацію ідентичну інформації, що вимагається як інформація точки формування довіри (трастового якоря).

Загальним правилом для інтерпретації будь-якого іншого запису типу "Sti" є те, що для цього типу послуги, ідентифікованого "Sti", послуга в списку, названа відповідно до значення поля "Назва послуги" з унікальною ідентифікацією через значення поля "Цифровий ідентифікатор послуги" має поточний статус кваліфікованої або статус затвердження відповідно до значення поля "Поточний статус послуги", починаючи з дати, зазначеної в полі "Дата і час актуалізації поточного статусу".

Інтерпретацію довірчих списків ЄС і користування ними додатково стандартизовано в ETSI TS 119 615.

“Р4. Модель формування довіри” супровідного документа [контрольний чеклист УВВ] дає змогу третій країні порівняти використання моделі(ей) формування довіри, пов'язаних із їхніми (К)НДП/ (К)ДП, із моделлю формування довіри на основі довірчих списків за Регламентом eIDAS.

Основне технічне припущення:

Самооцінювання придатності довірчого списку третьої країни як інструменту для імплементації та введення в дію УВВ за ст. 14 eIDAS слід проводити з урахуванням ключових технічних припущень і рекомендацій, викладених у розділі 3.2.

3. ОСНОВНІ ТЕХНІЧНІ РЕКОМЕНДАЦІЇ ДЛЯ 3-Х КРАЇН

3.1. Рекомендації щодо формату і змісту конкретних результатів НДП/ДП

3.2. Рекомендації щодо реалізації довірчих списків третіх країн



3. ОСНОВНІ ТЕХНІЧНІ РЕКОМЕНДАЦІЇ ДЛЯ 3-Х КРАЇН

У цьому розділі розглянуто основні технічні рекомендації та засадничі припущення, зазначені в розділі 2, що слугують основою для імплементації УВВ за eIDAS і повинні бути врегульовані до впровадження в дію угоди УВВ через КДС ЄК і довірчого списку третьої країни.

Існує дві основні категорії рекомендацій для третіх країн, що впливають на їхні НДП/ДП та на забезпечення можливості довірчого взаємного визнання їх рівнозначності з КНДП/КДП ЄС:

- ◆ а) Рекомендації щодо формату та вмісту конкретних послуг НДП/ДП третьої країни; та
- ◆ б) Рекомендації щодо впровадження довірчих списків третьої країни на основі не пов'язаних з ЄС специфікацій [ETSI TS 119612].

3.1. РЕКОМЕНДАЦІЇ ЩОДО ФОРМАТУ ТА ВМІСТУ КОНКРЕТНИХ РЕЗУЛЬТАТІВ НДП/ДП

Припускається, що впровадження НДП/ДП третьої країни, особливостей надання цих послуг, управління їх життєвим циклом, використання електронних підписів, електронних печаток, електронних сертифікатів, їх валідація та зберігання технологічно базуються на криптографії з відкритими ключами та на основі інфраструктури відкритих ключів (PKI).

3.1.1. (Кваліфіковані) сертифікати

Більшість, якщо не всі, різновидів технічних реалізацій кваліфікованих сертифікатів ЄС для електронних підписів, електронних печаток або автентифікації вебсайтів базуються на ITU-TX.509 I ISO / IEC9594-8, RFC 5280 та RFC3739.

Основні технічні обмеження, що впливають із вимог Регламенту eIDAS щодо кваліфікованих сертифікатів електронних підписів, електронних печаток або автентифікації вебсайтів, пов'язані з тим, що ці сертифікати мають містити:

- ◆ а. "Зазначення, щонайменше в формі, придатній для автоматизованої обробки, того, що сертифікат видано як кваліфікований сертифікат електронного підпису / електронної печатки / автентифікації вебсайту" (пор. пункт (а) Додатків I, III, IV);
- ◆ б. "набір даних, що однозначно представляють кваліфікованого надавача довірчих послуг, який видає кваліфіковані сертифікати, і містять щонайменше назву держави-члена, у якій засновано такого надавача, та:
 - ◆ для юридичної особи: найменування та, за доцільності, реєстраційний номер, як зазначено в офіційних записах,
 - ◆ для фізичної особи: прізвище та ім'я особи;" (пор. пункт (б) Додатків I, III, IV);
- ◆ с. "якщо дані для створення електронного підпису/печатки, пов'язані з даними для валідації електронного підпису/печатки, знаходяться в засобах для створення кваліфікованого електронного підпису/печатки, належне зазначення цього щонайменше в формі, придатній для автоматизованої обробки." (пор. пункт (j) Додатків I, III).

3.1.1.1. Декларація про видачу сертифіката про кваліфікований статус

КНДП ЄС, що видають кваліфіковані сертифікати як КДП, можуть демонструвати відповідність пункту (а) Додатків I, III, IV будь-якими технічними засобами. Однак у специфікаціях довірчих списків держав-членів ЄС, визначених в IPK (ЄС) 2015/1505, використовується конкретний еталонний стейтмент/вираз придатної для автоматизованої обробки індикації, про яку йдеться в пункті а) вище. Воно базується на стандартизованій еталонній індикації, що довірчий список держави-члена ЄС міститиме підтвердження кваліфікованого статусу цифрового сертифіката або зазначатиме, що на цей цифровий сертифікат не поширюється дія кваліфікованого статусу, наданого КНДП/КДП ЄС, який видав цей сертифікат.

Цей еталонний стейтмент ЄС визначається в ETSI як вираз "id-etsi-qcs-QcCompliance (id-etsi-qcs1)", який, як зазначено в ETSI EN 319 412-5, має бути належним чином поєднано з виразом "id-etsi-qcs-QcType(id-etsi-qcs 6)" та виразом "id-etsi-qcs-QcCClegislation (id-etsi-qcs 7)".

Останній вираз/стейтмент було нещодавно додано до специфікацій ETSI EN 319 412-5, щоб дозволити країнам, які не входять до ЄС, використовувати вираз/стейтмент "QcCompliance" (див. пункт 4.2.1 ETSI EN 319 412-5 v2.3.1).

КНДП третьої країни наполегливо рекомендовано використовувати вираз/стейтмент з ETSI QcCompliance (id-etsi-qcs 1), який стверджує, що такий сертифікат є кваліфікованим сертифікатом у рамках законодавства третьої країни та має на меті відповідати пункту (а) Додатків I, III або IV Регламенту eIDAS відповідно.

Використання того ж виразу ETSI QcCompliance наполегливо рекомендують для довірчих списків третьої країни як еталонне, що виражає підтвердження (або спростування) факту "надання третьою країною кваліфікованого статусу" в рамках законодавства третьої країни.

Якщо у законодавчій базі третьої країни та специфікаціях довірчих списків не використано стейтмент ETSI QcCompliance, в них мало би бути використано відповідне альтернативний стейтмент, такий як:

- ◆ визначений третьою країною "кваліфікований стейтмент" RFC 3739,
- ◆ або визначена на національному рівні політика щодо сертифікатів об'єктних ідентифікаторів (OID).

Відсутність у третьої країни (національного) еталонного виразу / стейтменту для реалізації національного аналога вимог пункту (а) Додатків I, III та IV eIDAS, практично унеможливує сумісність інтерпретації довірчого списку третьої країни зі специфікаціями довірчих списків країн-членів ЄС і [TS 119612]. Такий еталонний вираз має ключове значення для надання кваліфікованого статусу (або аналога в третій країні) у записі в довірчому списку, що відповідає наданню кваліфікованого статусу (ЄС / третя країна) та для інтерпретації (опціонального) "Розширення інформації про послугу" ("Sie") "Розширення типу кваліфікації" ("Sie: Q") та значення відповідних кваліфікаторів. Про вплив вибору ідентифікаторів (URI) для "ідентифікаторів типу послуги" ("Sti"), кваліфікаторів Sie:Q, використання подібного розширення "Sie:Q", визначеного третьою країною, йдеться в наступному розділі 4.2 цього документа.

Наполеглива рекомендація:

Законодавча база третьої країни повинна містити вимогу (бажано), або принаймні рішуче заохочувати включення в сертифікат відповідної комбінації визначених ETSI EN 319 412-5 стейтментів "id-etsi-qcs-QcCompliance (id-etsi-qcs 1)", "id-etsi-qcs-QcType (id-etsi-qcs 6)" та "id-etsi-qcs-QcCClegislation (id-etsi-qcs 7)" для декларування, що сертифікат видано як "кваліфікований на національному рівні" сертифікат третьої країни для електронних підписів, електронних печаток або автентифікації вебсайту відповідно.

Законодавча база третьої країни повинна забороняти (бажано) або, принаймні, категорично не рекомендувати включення до сертифіката стейтменту "QcCompliance" без використання стейтменту "QcCClegislation", оскільки це свідчитиме про те, що сертифікат видається відповідно до Регламенту eIDAS, що неможливо, коли емітент не походить з ЄС.

Вимога:

В довірчому списку третьої країни повинні використовуватися відповідні актуальні комбінації цих стейтментів "QcCompliance", "QcType" та "QcCClegislation" для інтерпретації обсягу надання кваліфікованого (або аналогічного для третьої країни) статусу в записі про послугу в довірчому списку та, у відповідних випадках, інтерпретація (опціонального) "Розширення інформації про послугу" ("Sie") "Розширення кваліфікації" ("Sie:Q") та значення відповідних кваліфікаторів.

Слід наголосити, що для досягнення відповідності вимогам Регламенту eIDAS один кваліфікований сертифікат може видаватися винятково для однієї мети – або для електронного підпису, або для електронної печатки, або для автентифікації вебсайту.

3.1.1.2. КНДП/Назва емітента

Щоб спростити перевірку відповідності значень між, з одного боку, зазначенням імені емітента в кваліфікованому сертифікаті, де вказано КНДП-емітента, якому надано / скасовано кваліфікований статус, і, з іншого боку, ідентифікацією імені цього КНДП у відповідному довірчому списку держави-члена ЄС¹³, переданому через поле "TSP name", або, як виняток, через одне зі значень поля "TSP trade name", елементи вмісту еталонного сертифіката, зазначені в IPK (ЄС) 2015/1505 – це атрибути "organizationName" та "countryName" значення унікального найменування поля емітента сертифіката в сертифікаті кінцевого об'єкта та ті самі атрибути значення унікального найменування поля Subject у сертифікаті "Цифрова ідентичність послуги" ("Sdi") НДП.

- ◆ Пункт 5.5.3 стандарту [TS 119 612]:

"Що стосується сертифікатів X.509, які претендують на те, щоб представляти відкритий ключ, що ідентифікує зазначену в списку послуг, Оператор схеми довірчих списків (ОСДС) не братиме до уваги сертифікати, для яких атрибут "O =" [унікального найменування суб'єкта] не відповідає строго значенню "TSP name" (п. 5.4.1), крім випадків, коли не вдається знайти жодного поданого до розгляду сертифіката, який відповідав би таким вимогам. Якщо НДП не може замінити подані до розгляду сертифікати, для яких атрибут "O=" не містить значення "TSP name" (пункт 5.4.1), ОСДС може включити їх до ДС.

13. Відповідна держава-член ЄС – це держава / територія, на якій засновано зазначеного в списку КНДП-емітента.

Таким чином ОСДС надасть для таких сертифікатів зі списку офіційний стейтмент в "URI визначення послуги схеми" (пункт 5.5.6) із зазначенням того, що вони видані та належать НДП, ідентифікованому значенням "TSP name", навіть якщо значення "TSP name" у ДС та значення "O=" у сертифікаті відрізняються. Значення "O=", що відрізняються від значення "TSP name", буде внесено в список як значення "TSP trade name" (пункт 5.4.2).

Наполеглива рекомендація:

Наполегливо рекомендується виявляти більшу вимогливість, ніж це передбачено у вищезазначеному пункті [TS 119 612], та жорстко вимагати, щоб атрибут "O=" [унікальне найменування суб'єкта сертифіката 'Sdi'] чітко відповідав значенню "TSP name" (п. 5.4.1) відповідного запису у довірчому списку, тобто точно збігався з назвою (К)НДП, зафіксованою в офіційних документах.

Законодавча база третьої країни повинна містити вимогу, щоб точна назва (К)НДП, зафіксована в офіційних документах, для юридичних осіб:

- ◆ вносилися як значення атрибута "O=" унікального імені емітента будь-якого
- ◆ кваліфікованого сертифіката;
- ◆ використовувалась як значення атрибута "O=" унікального імені Суб'єкта сертифіката "Sdi", що використовується як точка формування довіри \ трастовий якір для валідації ланцюжка сертифікатів з будь-якого кваліфікованого сертифіката;
- ◆ використовувалась як значення "TSP name" (п. 5.4.1 ETSI TS 119 612) відповідного запису у довірчому списку третьої країни

Ці три види використання одного і того ж значення повинні чітко збігатися.

Важливо дотримуватися вимоги пункту (b) Додатків I, II та IV eIDAS та проводити його верифікацію при валідації кваліфікованого статусу сертифіката кінцевого об'єкта у довірчому списку для уникнення помилкової транзитивності / атрибуції статусу некваліфікованої довірчої послуги, наприклад через перехресну або кореневу сертифікацію CA-CA.

Рекомендація:

Третім країнам рекомендується забезпечити, дати відповідне посилання в законодавстві (для відповідності вимогам законодавства) або принаймні рекомендувати дотримання відповідності стандартам серії ETSI EN 319 412 або їх аналогам.

3.1.1.3. Декларація про те, що особистий ключ, пов'язаний із сертифікованим відкритим ключем, перебуває під контролем КЗСП

Технічні характеристики довірчих списків країни-члена ЄС за ІРК (ЄС) 2015/1505 використовують визначений еталонний стейтмент, придатний для автоматизованої обробки, про яку йдеться в пункті j) Додатків I і III eIDAS. Він базується на стандартах, що визначають спосіб заповнення довірчих списків держав-членів ЄС так, щоб визначити чи особистий ключ, який відповідає відкритому ключу, сертифікованому за правилами кваліфікованих сертифікатів ЄС, міститься в ЗСКП ЄС (EU-QSCD), чи ні.

Це еталонний вираз / стейтмент – визначений в ETSI як "id-etsi-qcs-QcSSCD(id-etsi-qcs 4)", що вказано у пункті 4.2.2 ETSI EN 319 412-5. Цей вираз / стейтмент "декларує, що особистий ключ, пов'язаний із сертифікованим відкритим ключем, міститься у Засобі створення кваліфікованого підпису/печатки (ЗСКП/QSCD) відповідно до Регламенту (ЄС) № 910/2014 або [з історичних причин] в захищеному засобі створення підпису, як визначено в Директиві 1999/93/ЄС". Той самий вираз / стейтмент ETSI "QcSSCD" стосується як QSigCD, так і QSealCD.

Наполеглива рекомендація:

КНДП наполегливо рекомендовано використовувати визначений в ETSI "QcSSCD" вираз / стейтмент (id-etsi-qcs 4) з метою дотримання пункту (j) Додатку I або III eIDAS відповідно, але винятково якщо засіб, якому він відповідає, було сертифіковано як ЗСКП ЄС (EU-QSCD) відповідно до статті 30 Регламенту.

Наполегливо рекомендовано використовувати вираз / стейтмент "QcSSCD" у довірчих списках третьої країни як основу для підтвердження (або спростування) в рамках законодавства третьої країни того, що особистий ключ кваліфікованих сертифікатів для eSig / eSeal міститься в ЗСКП ЄС.

Вимога:

Визначений в ETSI вираз / стейтмент "QcSSCD" (id-etsi-qcs 4) не підлягає використанню КНДП, створеними у третій країні, для декларування того, що особистий ключ, пов'язаний із сертифікованим відкритим ключем, міститься в засобі, який не є ЗСКП ЄС (EU-QSCD).

Якщо законодавча база третьої країни та специфікації довірчого списку не використовують виразу / стейтменту ETSI "QcSSCD" в описаний вище спосіб, очікується, що вони використовуватимуть альтернативний стейтмент. Як альтернатива може використовуватися визначений третьою країною "кваліфікований стейтмент" RFC 3739 або конкретний національно визначений об'єктний ідентифікатор політики щодо сертифікатів. Це також важливо для можливості розрізнати за допомогою чітких ідентифікаторів у сертифікаті, що вважається ЗСКП згідно із законодавством третьої країни (ЗСКП 3-ї країни), а що – засобом третьої країни, який сертифіковано як ЗСКП ЄС у відповідності з Регламентом eIDAS (ЗСКП 3-ї країни-ЄС), та для підтвердження / спростування у довірчому списку третьої країни.

У разі відсутності національного еталонного виразу / стейтменту третьої країни для реалізації її юридичного еквівалента вимоги, викладеної в пункті (j) Додатків I і II, сумісність тлумачення довірчого списку третьої країни зі специфікаціями довірчих списків держав-членів ЄС та [TS 119 612] є малоімовірною. Власне, такий еталонний стейтмент є вкрай важливим для належної валідації електронних підписів / печаток третьої країни як рівнозначних QESig/QESeal ЄС, адже дає змогу належно інтерпретувати обсяг надання кваліфікованого (або аналогічного для третьої країни) статусу в записі довірчого списку про послугу, що відповідає видачі кваліфікованого статусу (ЄС / 3-тя країна) та інтерпретації (опціональних) "Розширення інформації про послугу" ("Sie") "Розширення кваліфікації" ("Sie:Q") та відповідних кваліфікаторів.

3.2. РЕКОМЕНДАЦІЇ ЩОДО ВПРОВАДЖЕННЯ ДОВІРЧИХ СПИСКІВ ТРЕТЬОЇ КРАЇНИ

3.2.1. Рекомендації, спрямовані на сприяння імплементації УВВ/MRA за ст. 14 eIDAS

Треті країни, що прагнуть укласти з ЄС УВВ/MRA за ст. 14, повинні створити та вести довірчий список відповідно до [ETSI TS 119 612], вносячи до цього списку як мінімум НДП/ДП, визнані юридично рівнозначними КНДП/КДП ЄС

Додатково або в рамках профілювання специфікацій, встановлених у [ETSI TS 119 612] для довірчих списків з-поза ЄС, створюючи довірчий

список, придатний для виконання УВВ за ст. 14, треті країни повинні взяти до уваги викладені у Таблиці 3 вимоги / рекомендації щодо конкретних полів або елементів довірчих списків.

Отримане в результаті зіставлення відповідних полів довірчих списків держав-членів ЄС з відповідними довірчими списками третьої країни буде використано як основу для розробки програмного вказівника специфікацій УВВ в КДС ЄК для довірчого списку третьої країни (та аналогічного вказівника УВВ у довірчому списку третьої країни до КДС ЄК).

Таблиця 3

	Довірчий список ЄС (ДС)	Довірчий список третьої країни (ДС)
Тип Списку статусів довірчих послуг	http://uri.etsi.org/TrstSvc/TrustedList/TSLType/EUgeneric	Рекомендоване значення http://uri.etsi.org/TrstSvc/TrustedList/TSLType/CClist де "CC" = Scheme territory Альтернативне значення: спеціально визначений URI
Назва схеми	"en": CC:EN_name_value "xx": CC:name_value	Потрібне значення "en": CC:EN_name_value "xx": CC:name_value Де "CC", "EN_name_value", "name_value" and "xx" відповідають зазначеному в пункті 5.3.6 ETSI TS 119 612
Підхід до визначення статусу	http://uri.etsi.org/TrstSvc/TrustedList/StatusDetn/EUappropriate	Рекомендоване значення http://uri.etsi.org/TrstSvc/TrustedList/StatusDetn/CCdetermination , де "CC" = Scheme territory Альтернативне значення: спеціально визначений URI
Тип схеми /спільнота /правила	http://uri.etsi.org/TrstSvc/TrustedList/schemerules/EUcommon http://uri.etsi.org/TrstSvc/TrustedList/schemerules/CC , де "CC" = Scheme territory	Рекомендоване значення http://uri.etsi.org/TrstSvc/TrustedList/schemerules/CC де "CC" = Scheme territory Альтернативне значення: спеціально визначений URI
Ідентифікатори типу послуги Sie:aSI - Sti supplements	КНДП, що видає кваліфікований сертифікат (КС) для електронних підписів Sti: http://uri.etsi.org/TrstSvc/Svctype/CA/QC Sie:aSI: http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures	КНДП, що видає кваліфікований сертифікат (КС) для електронних підписів Потрібне значення спеціально визначені URI (лише 'Sti' або комбінація 'Sti'/Sie:aSI) У разі використання поля "Sti" лише для передавання типу КПП з видачі кваліфікованого електронного сертифіката для електронних підписів рекомендованим значенням є: http://.../TrstSvc/Svctype/ForeSignatures/CA/QC де замість "..." слід вказати вузол відповідної організації (напр., Оператора схеми) або корінь URI. У разі використання комбінації полів 'Sti'/Sie:aSI для передачі типу КДП з видачі кваліфікованого електронного сертифіката для електронних підписів, рекомендованими значеннями є: Sti: http://.../TrstSvc/Svctype/CA/QC де замість "..." слід вказати вузол відповідної організації (напр., Оператора схеми) або корінь URI, та Sie:aSI: http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

(*)

	<p>КНДП, що видає кваліфікований сертифікат (КС) для електронних печаток</p> <p>Sti: http://uri.etsi.org/TrstSvc/Svctype/CA/QC</p> <p>Sie:aSI: http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals</p>	<p>КНДП, що видає кваліфікований сертифікат (КС) для електронних печаток</p> <p>Потрібне значення спеціально визначені URI (лише 'Sti' або комбінація 'Sti'/'Sie:aSI')</p> <p>У разі використання поля "Sti" лише для передавання типу КПП з видачі кваліфікованого електронного сертифіката для електронних печаток рекомендованим значенням є http://.../TrstSvc/Svctype/ForeSeals/CA/QC де замість "... " слід вказати вузол відповідної організації (напр., Оператора схеми) або корінь URI.</p> <p>У разі використання комбінації полів 'Sti'/'Sie:aSI' для передачі типу КДП з видачі кваліфікованого електронного сертифіката для електронних печаток рекомендованими значеннями є: Sti: http://.../TrstSvc/Svctype/CA/QC де замість "... " слід вказати вузол відповідної організації (напр., Оператора схеми) або корінь URI та Sie:aSI: http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals</p> <p>(*)</p>
	<p>КНДП, що видає кваліфікований сертифікат (КС) автентифікації вебсайту</p> <p>Sti: http://uri.etsi.org/TrstSvc/Svctype/CA/QC</p> <p>Sie:aSI: http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication</p>	<p>КНДП, що видає кваліфікований сертифікат (КС) для автентифікації вебсайту</p> <p>Потрібне значення спеціально визначені URI (лише 'Sti' або комбінація 'Sti'/'Sie:aSI')</p> <p>У разі використання поля "Sti" лише для передавання типу КПП з видачі кваліфікованого електронного сертифіката для автентифікації вебсайту рекомендованим значенням є: http://.../TrstSvc/Svctype/ForWebSiteAuthentication/CA/QC де замість "... " слід вказати вузол відповідної організації (напр., Оператора схеми) або корінь URI.</p> <p>За використання комбінації полів 'Sti'/'Sie:aSI' для передачі типу КДП з видачі кваліфікованого електронного сертифіката для автентифікації вебсайту рекомендованими значеннями є: Sti: http://.../TrstSvc/Svctype/CA/QC де замість "... " слід вказати вузол відповідної організації (напр., Оператора схеми) або корінь URI та Sie:aSI: http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForWebSiteAuthentication</p> <p>(*)</p>

	<p>КНДП, що надає кваліфіковані послуги валідації для QESig</p> <p>Sti: http://uri.etsi.org/TrstSvc/Svctype/QESValidation/Q</p> <p>Sie:aSI:</p> <p>http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</p>	<p>КНДП, що надає кваліфіковані послуги валідації для QESig</p> <p>Потрібне значення</p> <p>спеціально визначені URI (лише 'Sti' або комбінація 'Sti'/'Sie:aSI')</p> <p>У разі використання поля "Sti" лише для передавання типу КПП з кваліфікованою валідацією кваліфікованих електронних підписів рекомендованим значенням є:</p> <p>http://.../TrstSvc/Svctype/ForeSignatures/QESValidation/Q</p> <p>де замість "..." слід вказати вузол відповідної організації (напр., Оператора схеми) або корінь URI.</p> <p>У разі використання комбінації полів 'Sti'/'Sie:aSI' для передавання типу КДП рекомендованими значеннями є:</p> <p>Sti: http://.../TrstSvc/Svctype/QESValidation/Q</p> <p>де замість "..." слід вказати вузол відповідної організації (напр., Оператора схеми) або корінь URI та Sie:aSI:</p> <p>http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</p> <p>(*)</p>
	<p>КНДП, що надає кваліфіковані послуги валідації для QESeal</p> <p>Sti: http://uri.etsi.org/TrstSvc/Svctype/QESValidation/Q</p> <p>Sie:aSI:</p> <p>http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals</p>	<p>КНДП, що надає кваліфіковані послуги валідації для QESeal</p> <p>Потрібне значення</p> <p>спеціально визначені URI (лише 'Sti' або комбінація 'Sti'/'Sie:aSI')</p> <p>У разі використання поля "Sti" лише для передавання типу КПП з кваліфікованою валідацією кваліфікованих електронних печаток рекомендованим значенням є:</p> <p>http://.../TrstSvc/Svctype/ForeSeals/QESValidation/Q</p> <p>де замість "..." слід вказати вузол відповідної організації (напр., Оператора схеми) або корінь URI.</p> <p>У разі використання комбінації полів 'Sti'/'Sie:aSI' для передавання типу КДП рекомендованими значеннями є:</p> <p>Sti: http://.../TrstSvc/Svctype/QESValidation/Q</p> <p>де замість "..." слід вказати вузол відповідної організації (напр., Оператора схеми) або корінь URI, та Sie:aSI:</p> <p>http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals</p> <p>(*)</p>
	<p>КНДП, що надає кваліфіковані послуги зберігання для QESig</p> <p>Sti: http://uri.etsi.org/TrstSvc/Svctype/PSES/Q</p> <p>Sie:aSI:</p> <p>http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</p>	<p>КНДП, що надає кваліфіковані послуги зберігання для QESig</p> <p>Потрібне значення</p> <p>спеціально визначені URI (лише 'Sti' або комбінація 'Sti'/'Sie:aSI')</p> <p>У разі використання поля "Sti" лише для передавання типу КДП з кваліфікованого зберігання кваліфікованих електронних підписів рекомендованим значенням є:</p> <p>http://.../TrstSvc/Svctype/ForeSignatures/PSES/Q</p> <p>де замість "..." слід вказати вузол відповідної організації (напр., Оператора схеми) або корінь URI.</p> <p>У разі використання комбінації полів 'Sti'/'Sie:aSI' для передавання типу КДП рекомендованими значеннями є:</p> <p>Sti: http://.../TrstSvc/Svctype/PSES/Q</p> <p>де замість "..." слід вказати вузол відповідної організації (напр., Оператора схеми) або корінь URI та Sie:aSI:</p> <p>http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</p> <p>(*)</p>

	<p>КНДП, що надає кваліфіковані послуги зберігання для QESeal</p> <p>Sti: http://uri.etsi.org/TrstSvc/Svctype/PSES/Q</p> <p>Sie:aSi:</p> <p>http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals</p>	<p>КНДП, що надає кваліфіковані послуги зберігання для QESeal</p> <p>Потрібне значення</p> <p>спеціально визначені URI (лише 'Sti' або комбінація 'Sti'/'Sie:aSi')</p> <p>У разі використання поля "Sti" лише для передавання типу КПП з кваліфікованого зберігання кваліфікованих електронних печаток рекомендованим значенням є:</p> <p>http://.../TrstSvc/Svctype/ForeSeals/PSES/Q</p> <p>де замість "... " слід вказати вузол відповідної організації (напр., Оператора схеми) або корінь URI.</p> <p>У разі використання комбінації полів 'Sti'/'Sie:aSi' для передачі типу КДП рекомендованими значеннями є:</p> <p>Sti: http://.../TrstSvc/Svctype/PSES/Q</p> <p>де замість "... " слід вказати вузол відповідної організації (напр., Оператора схеми) або корінь URI та Sie:aSi:</p> <p>http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSeals</p> <p>(*)</p>
	<p>КНДП, що видають кваліфіковані позначки часу</p> <p>Sti: http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST</p>	<p>КНДП, що видають кваліфіковані позначки часу</p> <p>Потрібне значення</p> <p>Sti: спеціально визначений URI</p> <p>(e.g. http://.../TrstSvc/Svctype/TSA/QTST</p> <p>де замість "... " слід вказати вузол відповідної організації (напр., Оператора схеми) або корінь URI)</p> <p>(*)</p>
	<p>КНДП, що надають кваліфіковані послуги реєстрованої електронної доставки</p> <p>Sti: http://uri.etsi.org/TrstSvc/Svctype/EDS/Qor</p> <p>Sti: http://uri.etsi.org/TrstSvc/Svctype/EDS/REM/Q</p>	<p>КНДП, що надають кваліфіковані послуги реєстрованої електронної доставки</p> <p>Потрібне значення</p> <p>Sti: спеціально визначений URI</p> <p>(напр., http://.../TrstSvc/Svctype/EDS/Q або http://.../TrstSvc/Svctype/EDS/REM/Q</p> <p>де замість "... " слід вказати вузол відповідної організації (напр., Оператора схеми) або корінь URI)</p> <p>(*)</p>
Поточний статус послуги	http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted або http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/withdrawn	Потрібне значення: спеціально визначені URI
Sie:Q Кваліфікатори	QCWithQSCD (http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithQSCD)	Не застосовується або спеціально визначений URI як потрібне значення (**)
	QCNoQSCD (http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCNoQSCD)	Не застосовується або спеціально визначений URI як потрібне значення (**)
	QCQSCDManagedOnBehalf (http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCQSCDManagedOnBehalf)	Не застосовується або спеціально визначений URI як потрібне значення (**)
	QCForESig (http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForESig)	Не застосовується або спеціально визначений URI як потрібне значення (**)
	QCForESeal (http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForESeal)	Не застосовується або спеціально визначений URI як потрібне значення (**)

	QCForWSA (http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForWSA)	Не застосовується або спеціально визначений URI як потрібне значення (**)
	NotQualified (http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/NotQualified)	Не застосовується або спеціально визначений URI як потрібне значення (**)
	QCStatement (http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCStatement)	Не застосовується або спеціально визначений URI як потрібне значення (**)

(*) "Sti", визначені у пункті 5.5.1.1 стандарту [TS 119 612], відповідають типу зареєстрованих у списку довірчих послуг для кваліфікованих довірчих послуг, зазначених у Регламенті eIDAS, що їх надають відповідно до положень Регламенту eIDAS. Теоретично ці "Sti" не мали би використовуватися як такі, щоб представляють довірчу послугу з-поза ЄС, навіть якщо мають по суті ті самі специфікації, що й послуги, встановлені в eIDAS. Слід зазначити, що визначення "Sti", подане у пункті 5.5.1.1 [TS 119 612], може містити посилання на чинне національне законодавство на території, визначеній як територія застосування схеми певного довірчого списку (пор. п. 5.3.10 TS 119 612). Однак ці згадки про національне законодавство було включено як наслідок транспонування в національне законодавство держав-членів ЄС попередньої законодавчої бази Директиви про електронний підпис 1999/93/ЄС, яку було замінено Регламентом eIDAS. Це було зроблено для забезпечення безперервності посилання, оскільки такі довірчі послуги могли бути внесені в довірчий список держав-членів ЄС в рамках Директиви (як визначено в ETSI TS 119 612 v1.1.1, на який посилається IPK 2013/662/ЄС про внесення змін до Рішення 2009/767/ЄС щодо створення, ведення та публікації довірчих списків надавачів послуг сертифікації, що контролюються/акредитовані державами-членами. Ці національні законодавчі територіальні посилання у чинних специфікаціях не слід тлумачити поза сферою дії законодавства ЄС, тобто вони не підлягають використанню країнами, що не входять до ЄС. Однак деякі країни, що не входять до ЄС, могли вже створити національний довірчий список відповідно до ETSI TS 119 612 (v1.1.1 або v2.1.1) і можуть уже використовувати ці "Sti". У такому разі їм слід рекомендувати адаптувати специфікації їхнього національного довірчого списку або створити та вести відповідний спеціальний (ad hoc) довірчий список. Власне, специфікації "Sti" <http://uri.etsi.org/TrstSvc/Svctype/CA/QC> не містять жодних посилань на жодне національне "територіальне" законодавство як частину сфери їх застосування, яка суворо обмежена або Директивою ЄС 1999/93/ЄС, або Регламентом eIDAS.

Згідно із загальним принципом, від третіх країн вимагається використовувати спеціально визначені URI або лише за допомогою "Sti", або за допомогою комбінації 'Sti'/'Sie:aSI', як зазначено в таблиці 3.

Для URI 'Sti' третьої країни, повинен відповідати 'Sti' <http://uri.etsi.org/TrstSvc/Svctype/CA/QC> ЄС, рекомендовано, щоб цей URI закінчувався на '/CA/QC', щоб уможливити використання розширення 'Sie:Q', як зазначено у пункті 5.5.9.2 стандарту [TS 119 612]. Проте, якщо точне тлумачення пункту 5.5.9.2 обмежує його для використання для 'Sti' <http://uri.etsi.org/TrstSvc/Svctype/CA/QC> ЄС, і якщо третя країна бажає використовувати розширення з подібною метою та сферою застосування, для цього може знадобитися визначення нового розширення 'Sie'.

(**) Аналогічно до зазначеного у (*) пункт 5.5.9.2.3 ETSI TS 119 612 обмежує використання заздалегідь визначених "кваліфікаторів" розширення 'Sie:Q' або Директивою ЄС 1999/93/ЄС або Регламентом eIDAS, вони не підлягають використанню для довірчих списків третіх країн.

З цієї причини або зі специфічних для третьої країни причин спеціально визначені URI можуть використовуватися третьою країною для "кваліфікаторів" з пункту 5.5.9.2.3 в контексті розширення 'Sie:Q' або аналогічного національно визначеного розширення 'Sie: Q'.

3.2.2. Додаткові рекомендації щодо впровадження довірчого списку третьої країни

Цей розділ надає додаткові поради для третіх країн щодо створення та ведення національного довірчого списку, зокрема, якщо третя країна має на меті укласти з ЄС УВВ/MRA за ст. 14 eIDAS.

Створюючи довірчий список, головне – пам'ятати, для чого його створено. Призначення довірчого списку – надавати інформацію про статус та історію статусу довірчих послуг від НДП щодо їх відповідності актуальним положенням чинного законодавства.

Включення такого статусу та історії статусу – це видимий результат засадничої схеми затвердження, тобто організованого процесу і пов'язаних із ним практик авторизації, нагляду, оцінки / аудиту, моніторингу і затвердження, призначених для застосування нагляду з метою забезпечити дотримання конкретних критеріїв, щоб підтримувати довіру до послуг в межах сфери дії схеми.

Довірчі списки, зазначені у стандарті [TS 119 612], містять кілька полів, що передбачають необхідність для 3-ї країни, зокрема для організації, відповідальної за створення, публікацію, підписання та ведення довірчого списку (тобто "Оператора схеми" довірчого списку або ОСДС, як визначено в пункті 5.3.4 [TS119 612]), надавати сторонам-користувачам достатню та належну інформацію щодо схеми затвердження, на якій ґрунтується довірчий список. Ці поля містять:

- ◆ "URI інформації про схему" (Siu) – пункт 5.3.7 [TS 119612];
- ◆ "Підхід до визначення статусу" (Siu) – пункт 5.3.8 [TS 119612];
- ◆ "Тип схеми / спільнота / правила" (Stcr) – пункт 5.3.9 [TS 119612];
- ◆ "Політика ССДП / юридично значущі повідомлення" (Siu) – пункт 5.3.11 [TS 119 612]; і, меншою мірою
- ◆ "Назва схеми" (Sn) – пункт 5.3.6 [TS 119612].

Відповідно до загальної вимоги стандарту [TS 119 612] (напр., пункт 5.1.4), інформація, що надається у вищезазначених полях списку, повинна надаватися британським варіантом англійської мови. Слід не лише забезпечувати багатомовні вказівники з мовним кодом "en", коли це вимагається, але й інформація, що надається за допомогою відповідного URI (напр., вебсторінка, документи), має бути доступна англійською мовою. Також передбачено багатомовну підтримку, яка за потреби дозволяє надавати точно таку ж інформацію іншими національними або міжнародними мовами.

Загалом формат вищевказаних полів визначено як URI, щодо якого третім країнам доступні три варіанти:

- ◆ а) Використання наперед визначеного URI на основі [http://uri.etsi.org/...](http://uri.etsi.org/),
- ◆ б) Використання URI для реєстрації третьою країною в домені організації ідентифікованої ETSI, як описано в пункті D.3 стандарту [TS 119 612], або
- ◆ с) Використання URI, спеціально визначеного третьою країною.

З цих трьох варіантів останній забезпечує третій країні більшу гнучкість і контроль за адмініструванням, оскільки інші варіанти вимагають взаємодії з секретаріатом ETSI для реєстрації URI, коли це потрібно, і у всіх випадках потрібно подавати текст або вміст вебсторінки, щоб вони були доступні при розіменуванні URI на основі ETSI.

Ще одне загальне міркування полягає в тому, що, на перший погляд, може бути не дуже легко визначити, яка інформація повинна бути доступною з URI із полів, про які йдеться в пунктах 5.3.6–5.3.9 та 5.3.11. Основна рекомендація – забезпечити послідовне, актуальне й організоване управління інформацією, що надається через ці поля. Подальші настанови викладено в наступних підрозділах.

3.2.2.1. URI "Інформація про схему"

Це найважливіше поле та канал для надання сторонам-користувачам якомога вичерпнішої та максимально чіткої інформації щодо схеми затвердження, на якій ґрунтується внесення НДП/ДП до довірчого списку, його статусу і зміни статусу (напр., щодо основи надання або скасування "кваліфікованого" статусу).

URI, який повинен бути наданий (принаймні за допомогою мовного вказівника "en"), повинен містити "шлях" (бажано якомога пряміший) до інформації, що описує відповідну інформацію про схему, в тому числі:

- ◆ а) Сферу застосування і контекст довірчого списку: сюди входить й опис типів і класів НДП/ДП, які можуть бути внесені до довірчого списку. Термін "типи" тут стосується сутності й обсягу довірчих послуг, що надаються НДП, а термін "класи" тут стосується рівня надійності НДП/ДП. Для ілюстрації в національні довірчі списки ЄС держави-члени ЄС повинні вносити принаймні НДП/ДП, за які вони відповідають, і можуть на добровільній основі вносити некваліфіковані НДП/ДП або довірчі послуги, визначені на національному рівні, та НДП, які їх надають.
- ◆ б) Загальний опис і детальна інформація про схему дії (затвердження), що передбачає:
 - ◆ а. інформацію про процес і процедури, яких дотримуються:
 - ◆ і. для затвердження і зміни статусу НДП/ДП відповідальним компетентним органом (який може бути або не бути тим самим органом, що відповідає за створення та публікацію довірчого списку); та
 - ◆ ii. НДП для затвердження;

Примітка: Ці процеси та процедури можуть базуватися на злитті та поєднанні моделі попередньої авторизації та моделі постверифікації з моделлю ліцензування тощо.

- ◆ б. інформацію про критерії, за якими затверджується НДП;

Примітка: Критерії можуть бути функціональними, як це визначено в юридичних документах, законах та / або постановах. Вони можуть бути детальними технічними специфікаціями, що спираються на, або самі є національними, регіональними або міжнародними стандартами. Вони можуть поєднувати як правові, так і технічні положення. Ці критерії можуть бути або обов'язковими або рекомендованими.

- ◆ с. інформацію про критерії та правила, які використовуються для вибору експертів з оцінювання/аудиторів, та визначення того, як вони оцінюють НДП/ДП.

- ◆ d. якщо окремі аспекти нагляду, акредитації аудиторів, сертифікації НДП/ДП та функціонування схеми забезпечують різні органи, інформацію про ідентифікацію цих органів та окремих обов'язків і будь-яких зобов'язань кожного органа.

Надана інформація повинна містити щонайменше дані про національну систему затвердження і нагляду третьої країни, що застосовується до тих НДП/ДП, які прагнуть бути визнаними юридично рівнозначними КНДП/КДП ЄС на виконання УВВ/МРА за ст. 14 eIDAS.

- ◆ с) Іншу контактну і загальну інформацію, яка може стосуватися роботи схеми.

Слід уникати простого переліку юридичних посилань без загального опису схеми. Якість і кількість наданої інформації має бути однаковою незалежно від мови її викладення.

3.2.2.2. Підхід до визначення статусу

У пункті 5.3.8 стандарту [TS 119 612] немає вказівок щодо того, який тип інформації повинен надаватися через URI, що ідентифікує підхід до визначення статусу. Причина полягає в тому, що згідно з [TS119612] цей URI має бути простим ідентифікатором, який не передає додаткової інформації.

Деякі настанови щодо тексту, який повинен бути пов'язаний з URI, а отже, міститись на вебсторінці, на яку потрапляють при розіменуванні URI, можна довідатися з тексту, пов'язаного з відповідним довірчим списком держави-члена ЄС, як визначено у пункті D. 5.2 [TS 119 612]:

D.5.2 Спосіб визначення статусу <https://uri.etsi.org/TrstSvc/TrustedList/StatusDetn/EUassign>

Статус внесених до списку сервісів визначається Оператором схеми або за дорученням Оператора схеми у рамках відповідної системи, як це визначено механізмом реалізації відповідного європейського законодавства держави-члена ЄС, і далі описано в інформації, на яку вказує URI "Інформація про схему".

Текст, що відповідає обраному URI, може, наприклад, зазначити, що довірчі послуги (третьої країни), внесені до списку (третьої країни), мають статус, який визначається Оператором схеми або за дорученням Оператора схеми у рамках відповідної системи, як це визначено механізмом реалізації (третьою країною) відповідного законодавства (третьої країни) і далі описано в інформації, на яку вказує URI "Інформація про схему" довірчого списку (третьої країни).

У тексті можна уточнити:

- ◆ який саме орган третьої країни фактично визначає статус довірчої послуги, внесеної до довірчого списку третьої країни, та який її зв'язок із органом, визначеним як "Оператор схеми" у довірчому списку, якщо це різні суб'єкти;
- ◆ визначення відповідного законодавства третьої країни;
- ◆ подальший опис "відповідної системи" для визначення (затвердження і надання) статусу довірчої послуги та внесення її до довірчого списку третьої країни.

Утім що детальнішою є інформація, то частіше вона може потребувати оновлення.

3.2.2.3. Тип схеми/спільнота/правила

Текст / дані, що надаються при розіменюванні URI, повинні містити таку основну інформацію (зокрема щодо НДП/ДП третьої країни, які претендують на визнання юридично рівнозначними КНДП/КДП ЄС):

- ◆ Про політику/правила оцінювання внесених до списку сервісів, в тому числі інформації про режим попередньої авторизації НДП/ДП третьої країни, режим нагляду, режим аудиту, систему затвердження для отримання кваліфікованого статусу тощо.

Примітка: Щоб уникнути дублювання інформації, можна скористатися посиланням на подану інформацію через "URI Інформація про схему".

- ◆ Про те, як інтерпретувати довірчий список третьої країни для перевірки, чи вихідні дані довірчої послуги було видано НДП/ДП з "кваліфікованим" (або аналогічним) статусом.

Щодо останнього пункту, прикладом такого тексту є текст, доступний у ІПК (ЄС) 2015/105 або на <https://uri.etsi.org/TrstSvc/TrustedList/schemerules/EUcommon>. Для третьої країни, яка впроваджує [TS 119 612], надзвичайно важливо створити власний довірчий список, щоби встановити чіткі правила та визначення щодо використання та інтерпретації таких елементів та їх значень (а також для кваліфікованих сертифікатів відповідних еталонних стейтментів у формі, що придатна для автоматизованої обробки), які використовуються як посилання для інтерпретації довірчого списку:

- ◆ Ідентифікатори типу послуги (пункт 5.5.1 [TS 119 612]) і, у відповідних випадках, доповнення Sie:aSI до цих ідентифікаторів типу (пункт 5.5.9.4 [TS 119 612]);

- ◆ Поточний статус послуги (пункт 5.5.4 [TS 119 612]); і (у відповідних випадках)
- ◆ Розширення інформації про послугу / кваліфікації (Sie:Q) (пункт 5.5.9.2 [TS 119 612]) або аналогічне розширення та відповідні кваліфікатори (пункт 5.5.9.2.3 [TS 119 612]).

Що стосується розширення Sie:Q – третім країнам рекомендовано розробити систему затвердження у такий спосіб, щоб таке розширення не потрібно було використовувати. У стандарті [TS 119612] Sie:Q призначене для застосування у виняткових випадках, коли неможливо вчинити інакше. В ідеалі у третьої країни не мало б виникати потреби використовувати розширення Sie:Q. Треті країни можуть визначити чіткі правила, забезпечивши, щоб у разі, якщо виданий сертифікат не відповідає правилам включення певних додатних для автоматизованої обробки стейтментів (напр., був виданий як кваліфікований сертифікат певного типу), цей сертифікат скасували та/або не вважали кваліфікованим (або аналогічним) сертифікатом без необхідності використання Sie:Q у довірчому списку третьої країни.

3.2.2.4. Політика ССДП/ юридично значуще повідомлення

Основна інформація, що повинна бути в тексті / даних, що надаються при розіменюванні відповідного URI, стосується ідентифікації відповідного законодавства / схеми / фреймворка.

3.2.2.5. Назва схеми

Специфікації пункту 5.3.6 є однозначно зрозумілими.

3.2.2.6. Строк зберігання попередньої інформації

Значення '65535', передбачене пунктом 5.3.12 стандарту [TS 119 612], вимагає від Оператора схеми забезпечити, щоб попередня інформація, що її надано у довірчому списку, НІКОЛИ не вилучалася.

Відповідно, якщо чинне національне законодавство третьої країни вимагатиме, щоб за певних обставин раніше внесених до списку НДП та/або ДП було "вилучено" з довірчого списку третьої країни, повинно бути зрозуміло, що це слід тлумачити не буквально, а в переносному сенсі, та реалізовувати шляхом визнання недейсним рішення про затвердження (напр., кваліфікованого або аналогічного) статусу відповідного НДП/ДП у довірчому списку третьої країни.

4. ПРОГРАМНІ ВКАЗІВНИКИ УВВ У КДС ЄК І ДОВІРЧИХ СПИСКАХ ТРЕТІХ КРАЇН

4.1. Передумови

4.2. Впровадження УВВ/MRA в КДС ЄС

4.3. Впровадження УВВ/MRA у довірчий список третьої країни



4. ПРОГРАМНІ ВКАЗІВНИКИ УВВ/MRA У КДС ЄК І ДОВІРЧОМУ СПИСКУ 3-Ї КРАЇНИ

Як зазначено у Розділі 1.1.2 Регламенту eIDAS, формування довірчого визнання електронних кваліфікованих довірчих послуг базується на сукупності довірчих списків держав-членів ЄС, що надають структуровану інформацію про кваліфікований статус надавачів кваліфікованих довірчих послуг і кваліфікованих довірчих послуг, які вони надають.

Технічні специфікації та формати довірчих списків держав-членів ЄС визначено в IPK (ЄС) 2015/1505, що базується на стандарті [TS 19 612]. Держави-члени ЄС зобов'язані підписати XML-версію свого національного довірчого списку електронним підписом або печаткою, що відповідають вимогам IPK (ЄС) 2015/1505, виходячи з положення 5.7.1 [TS119612]. Для верифікації такого цифрового підпису сторони-користувачі повинні мати доступ до відповідного відкритого ключа.

Для забезпечення доступу до довірчих списків усіх держав-членів Європейська Комісія (ЄК) публікує спільний довірчий список, який називається кореневим довірчим списком (КДС (LOTL)), з посиланнями на опубліковані довірчі списки держав-членів ЄС. Сертифікат (и) відкритого ключа, що відповідають особистому ключу (ключам), за допомогою яких можна підписувати довірчі списки держав-членів ЄС, а, отже, останні можуть використовуватися сторонами-користувачами для валідації підписів цих довірчих списків, що опубліковані в КДС державами-членами ЄС. КДС доступний у форматі, придатному для автоматизованої обробки (XML). Технічні специфікації КДС ЄК не публікувалися, але спираються на [TS 119612].

У разі укладення угоди згідно зі ст. 14 eIDAS між ЄС та третьою країною, очікується, що технічна реалізація взаємного визнання КНДП/КДП ЄС та відповідних НДП/ДП третьої країни відбудеться шляхом:

- ◆ (а) Внесення до КДС додаткового запису "Програмний вказівник до інших ССДП",

що міститиме:

- ◆ I. ідентифікацію третьої країни, з якою було укладено УВВ/MRA,

- ◆ II. місцеперебування довірчого списку третьої країни,
 - ◆ III. список сертифікату(ів) відкритого ключа, що відповідає(ють) особистому(им) ключу(ам), які можуть використовуватись для підписання довірчого списку третьої країни, та
 - ◆ IV елемент MutualRecognitionAgreementInformation, що дозволяє зазначати ті типи КНДП/КДП, на які поширюється УВВ/MRA, та зіставляти засоби, за допомогою яких відображають факт надання/відкликання статусу НДП/ДП третьої країни, із засобами, за допомогою яких відображають факт надання/відкликання кваліфікованого статусу КНДП/КДП.
- ◆ (b) Шляхом внесення до довірчого списку третьої країни аналога вищевказаної інформації, тобто:
 - ◆ I. ідентифікації ЄС як територіальної сфери дії або "регіонального об'єкта", з яким укладено УВВ,
 - ◆ II. місцеперебування КДС ЄК,
 - ◆ III. списку сертифікату(ів) відкритого ключа, що відповідає(ють) особистому(им) ключу(ам), які можуть використовуватись для підписання КДС ЄК (так звані сертифікати ОС КДС), та
 - ◆ IV елементу MutualRecognitionAgreementInformation, що дозволяє зазначати ті типи КНДП/КДП, на які поширюється УВВ, та зіставляти засоби, за допомогою яких відображають факт надання/відкликання статусу НДП/ДП третьої країни, із засобами, за допомогою яких відображають факт надання/відкликання кваліфікованого статусу КНДП/КДП.

Щодо ведення та оновлення локації КДС ЄК і сертифікатів ОС КДС КДС ЄК пропонує можливість автоматизованого оновлення за допомогою концепції "опорних КДС", як вказано в Офіційному віснику ЄС¹⁴ та зокрема на <https://ec.europa.eu/tools/lotl/pivot-lotl-explanation.html>.

Щоб спростити ведення й оновлення локації та сертифікатів ОСДС третьої країни в КДС ЄК, третій країні рекомендовано впровадити подібний механізм "опорного ДС".

Рекомендація:

Третім країнам створити та вказати механізм "опорного ДС" в рамках специфікацій ДС третьої країни подібно до того, як це робиться для "опорних КДС".

14. Інформація, пов'язана з даними про довірчі списки держав-членів, згідно з повідомленням відповідно до ІПК (ЄС) 2015/1505, ОВ 276, від 16.8.2019, с. 1-7 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2019.276.01.0001.01.ENG

4.1. ПЕРЕДУМОВИ

Висуваються такі передумови:

1. Передбачається, що КНДП 3-ї країни та надавані ними КДП 3-ї країни, що полягають у видачі QC-eSig 3-ї країни, визнаються на виконання ст. 14 Регламенту eIDAS рівнозначними та такими, що відповідають вимогам до КНДП ЄС і КДП ЄС, які вони надають (напр., видача QC-eSig ЄС).
2. Передбачається, що QESig 3-ї країни, подібно до QESig, визначатимуться як AdES 3-ї країни, підтримувані QC-eSig 3-ї країни та створені за допомогою ЗСКП 3-ї країни, щодо яких:
 - ◆ а) Передбачається, що визначення та положення для AdES 3-ї країни у законодавстві третьої країни функціонально рівнозначні та відповідають вимогам до AdES ЄС у eIDAS;
 - ◆ б) Передбачається, що визначення та положення щодо QC-eSig 3-ї країни у законодавстві 3-ї країни функціонально рівнозначні та відповідають вимогам до QC-eSig ЄС у eIDAS;
 - ◆ с) Передбачається, що визначення та положення щодо ЗСКП 3-ї країни у законодавстві 3-ї країни функціонально рівнозначні та відповідають вимогам до ЗСКП ЄС у eIDAS;
3. Передбачається, що придатний для автоматизованої обробки референційний стейтмент як для декларування у сертифікаті, так і для підтвердження / спростування у довірчому списку 3-ї країни, що особистий ключ, пов'язаний із сертифікованим відкритим ключем, міститься в ЗСКП ЄС або ЗСКП 3-ї країни-ЄС:
 - ◆ а. це або стейтмент id-etsi-qcs-QcSSCD, або
 - ◆ б. аналогічний національний стейтмент третьої країни, або
 - ◆ с. унікальний, спеціальний, відповідний цільовому призначенню об'єктний ідентифікатор політики сертифіката (CPOID).
4. Передбачається, що придатний для автоматизованої обробки референційний стейтмент як для декларування у сертифікаті, так і для підтвердження / спростування у довірчому списку 3-ї країни, що даний сертифікат є кваліфікованим сертифікатом для певних видів, це:
 - ◆ а) або стейтмент id-etsi-qcs-QcCompliance (додатково уточнений в підстейтментах id-etsi-qcs-QcType та id-etsi-qcs-QcCClegislation), або
 - ◆ б) аналогічний¹⁵ національний стейтмент третьої країни, або
 - ◆ с) унікальний, спеціальний, відповідний цільовому призначенню об'єктний ідентифікатор політики сертифіката (CPOID).
5. Передбачається, що придатний для автоматизованої обробки референційний стейтмент як для ідентифікації у сертифікаті, так і для підтвердження / спростування у довірчому списку 3-ї країни назви та (у відповідних випадках) реєстраційного номера, згідно з офіційними записами КНДП, є відповідно атрибутами organizationName і organizationIdentifier унікального імені (DN) емітента сертифіката та унікального імені (DN) Суб'єкта "Sdi".
6. У контексті пілотного проєкту зазначено, що AdES ЄС та AdES 3-ї країни створюються відповідно до одного зі стандартизованих форматів, вказаних в ІРК (ЄС) 2015/1506 або в подальших базових редакціях EN 319 1x2-1 цих довідкових стандартів.

15. По суті

4.2. ВПРОВАДЖЕННЯ УВВ/MRA В КДС ЄС

З боку ЄС укладення УВВ/MRA між ЄС та третьою країною технічно тягнутиме за собою внесення до в КДС ЄС "програмного вказівника" до ДС 3-ї країни, а саме КДС-ВССДП ЄС-3-ї країни (EU-LOTL-PTOTSL-3rdC).

Поточний КДС ЄС уже містить перелік "Програмний вказівників на інші ССДП", що вказують на всі ДС ЄС. Ці вказівники в основному містять:

- ◆ Локацію вказуваного довірчого списку держави-члена ЄС (aURL).
- ◆ Список сертифікатів підписів, призначений для валідації підписів / печаток у вказуваному довірчому списку, що дозволяє сторонам-користувачам провести автентифікацію його вмісту.
- ◆ Тип довірчого списку (тобто "<http://uri.etsi.org/TrstSvc/TrustedList/TSLType/EUGeneric>", стандартизований за [TS 119 612] для довірчих списків держав-членів ЄС).
- ◆ Ім'я "Оператора схеми" довірчого списку із зазначенням назви органу, відповідального за створення, публікацію, підписання та ведення довірчого списку.
- ◆ URL типу схеми / спільноти / правил, за яким користувачі (сторони-користувачі) можуть отримати інформацію про тип схеми/спільноту / правила, на основі яких внесені до списку послуги проходять затвердження та оцінювання, і за якими може бути визначено тип схеми або спільноти.

Подібним чином програмний вказівник у КДС ЄС на довірчий список третьої країни (тобто КДС-ВССДП ЄС-3-ї країни (EU-LOTL-PTOTSL-3rdC)) повинен містити:

- ◆ Локацію ДС 3-ї країни.
- ◆ Список сертифікатів підпису, які будуть використовуватися для автентифікації ДС 3-ї країни.
- ◆ Тип ДС 3-ї країни, як зазначено в ДС 3-ї країни (наприклад, URI, визначений у [TS 119 612] <http://uri.etsi.org/TrstSvc/TrustedList/TSLType/CCList>, де "CC" – це код ISO 3166-1 AlphaGo 2 для третьої країни або відповідного, спеціально визначеного URI третьої країни).

- ◆ Назва оператора схеми ДС 3-ї країни, як зазначено в ДС 3-ї країни.
- ◆ URL типу схеми/ спільноти / правил, що вказує на вміст, що чітко описує для всіх зацікавлених сторін:
- ◆ Як інтерпретувати вміст ДС 3-ї країни. Це може бути реалізовано через аналоги IPK (ЄС) 2015/1505 у законодавстві третьої країни та/або через регулювання, що обумовлюють випуск і валідацію підпису QESig 3-ї країни відповідно до законодавства 3-ї країни¹⁶.
- ◆ У контексті УВВ/MRA за ст. 14 зіставлення між типами довірчих послуг ('Sti' та 'Sie: aSI') в обох законодавствах, статусами довірчих послуг ('Scs'¹⁷ та 'Sps'¹⁸) та референційними кваліфікованими стейтментами (KC певного типу, ЗСКП ЄС), укладені як зі стейтментів, що містяться в сертифікатах і видаються у рамках схеми, так і з відповідної компенсаційної інформації в записі про НДП у довірчому списку. Цей опис повинен пояснювати, як інтерпретувати елемент MutualRecognitionAgreementInformation.
- ◆ Елемент **MutualRecognitionAgreementInformation**, що надає придатну для автоматизованої обробки інформацію про УВВ/MRA за ст.14, виражену як зіставлення КНДП ЄС/КДП ЄС з визнаним аналогом КНДП 3-ї країни/КДП 3-ї країни.

Оскільки в реалізації УВВ за ст. 14 можуть відбуватися збої (напр., тимчасове призупинення або припинення дії угоди), інформаційні елементи УВВ повинні бути структуровані подібно до записів про довірчі послуги та записів із попередньою інформацією про довірчі послуги. Це потрібно для урахування можливості змін у репрезентації довірчого списку третьої країни через зміну законодавчого режиму (напр., перехід від режиму Директиви про електронні підписи до режиму eIDAS в ЄС передбачав суттєві зміни деяких значень та URI в довірчих списках держав-членів ЄС), підходу до стандартизації тощо.

Специфікації інформаційного елемента УВВ містяться у супровідному документі [специфікації УВВ].

16. Може містити національні особливості, як-от наявність позначки часу, кваліфікованої Швейцарською Конфедерацією (CH) CH-QESig у законодавстві Швейцарії.

17. Поле "Поточний статус послуги", як визначено у пункті 5.5.4 ETSI TS 119 612 v2.1.1.

18. Поле "Попередній статус послуги", як визначено у пункті 5.6.4 ETSI TS 119 612 v2.1.1

4.3. ВПРОВАДЖЕННЯ УВВ/МРА В ДОВІРЧИХ СПИСКАХ ТРЕТІХ КРАЇН

Очікується, що в ДП 3-ї країни буде створено ВССДС ЄС-3-ї країни з програмним вказівником на КДС ЄС, як викладено в розділі вище з урахуванням відповідних змін.

5. ВЗАЄМНА ВАЛІДАЦІЯ “КВАЛІФІКОВАНИХ” ЕЛЕКТРОННИХ ПІДПИСІВ / ПЕЧАТОК ЄС-3-Ї КРАЇНИ



5. ВЗАЄМНА ВАЛІДАЦІЯ “КВАЛІФІКОВАНИХ” ЕЛЕКТРОННИХ ПІДПИСІВ / ПЕЧАТОК ЄС-3-Ї КРАЇНИ

Валідація кваліфікованих електронних підписів третьої країни (або печаток, або інших еквівалентних вихідних даних КДП, визнаних за УВВ/MRA) повинна базуватися на стандарті ETSI TS 119 615 з необхідними корективами для врахування пов'язаних із УВВ програмних вказівників у КДС ЄК і в довірчому списку третьої країни відповідно.

Пропозиції щодо адаптації TS 119 615 наведено у супровідному документі [Використання УВВ/MRA].

Український центр європейської політики (УЦЄП) – це незалежний аналітичний центр аналізу та вироблення політики, який був заснований у 2015 році.

Наша місія – сприяти проведенню реформ в Україні задля сталого економічного зростання та побудови відкритого суспільства в партнерстві з інституціями на всіх рівнях.

Пріоритетні напрями діяльності:

- підготовка та розповсюдження експертно-аналітичних матеріалів для сприяння євроінтеграційним реформам в Україні;
- популяризація європейських цінностей в українському суспільстві;
- інформування суспільства про можливості і переваги тісної співпраці з ЄС;
- сприяння посиленій економічній, політичній та торговельній співпраці України з Європейським Союзом;
- інформування міжнародної спільноти про виклики і досягнення в здійсненні Україною реформ, передбачених Угодою про асоціацію між Україною та ЄС.



УКРАЇНСЬКИЙ ЦЕНТР
ЄВРОПЕЙСЬКОЇ
ПОЛІТИКИ