

## ПОРІВНЯЛЬНА ТАБЛИЦЯ

до проекту наказу Міністерства цифрової трансформації України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України “Про внесення змін до наказу Міністерства цифрової трансформації України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 30 вересня 2020 року № 140/614”

Зміст положення акта законодавства	Зміст відповідного положення проекту акта
<p>3. Суб'єкти відносин у сфері електронних довірчих послуг, що використовують у своїй діяльності кваліфіковані сертифікати відкритих ключів, застосовують кваліфікований електронний підпис:</p> <p>1) в межах країни з метою забезпечення електронного документообігу та електронної автентифікації осіб відповідно до:</p> <p>ДСТУ 4145-2002 “Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння” з функцією гешування за ГОСТ 34.311-95 “Информационная технология. Криптографическая защита информации. Функция хэширования”. Ці національні стандарти застосовуються для створення кваліфікованого електронного підпису до 01 січня 2022 року та для створення кваліфікованого електронного підпису з метою надання інформації щодо статусу</p>	<p>3. Суб'єкти відносин у сфері електронних довірчих послуг, що використовують у своїй діяльності кваліфіковані сертифікати відкритих ключів, застосовують кваліфікований електронний підпис:</p> <p>1) в межах країни з метою забезпечення електронного документообігу та електронної автентифікації осіб відповідно до:</p> <p>ДСТУ 4145-2002 “Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння” з функцією гешування за ГОСТ 34.311-95 “Информационная технология. Криптографическая защита информации. Функция хэширования”. Ці національні стандарти застосовуються для створення кваліфікованого електронного підпису до 01 січня 2022 року та для створення кваліфікованого електронного підпису з метою надання інформації щодо статусу</p>

<p>сертифікатів відкритих ключів до завершення терміну їх дії та для перевірки кваліфікованого електронного підпису;</p> <p>ДСТУ 4145-2002 “Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння” з функцією гешування за ДСТУ 7564-2014 “Інформаційні технології. Криптографічний захист інформації. Функція гешування”. Ці національні стандарти застосовуються для створення кваліфікованого електронного підпису з 01 січня 2021 року та для перевірки кваліфікованого електронного підпису;</p> <p>ДСТУ ISO/IEC 14888-3:2019 “Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 3. Механізми на основі дискретного логарифмування” із застосуванням алгоритму ECDSA зі ступенем розширення основного поля еліптичної кривої не менше ніж 256 з функціями гешування sha256 або sha512 відповідно до національного стандарту, визначеного пунктом 55 Переліку;</p> <p>2) для транскордонного співробітництва з будь-якою метою відповідно до вимог:</p> <p>встановлених національним стандартом, визначеним в пункті 55 Переліку;</p> <p>зазначених у підпункті 1 цього пункту.</p>	<p>сертифікатів відкритих ключів до завершення терміну їх дії та для перевірки кваліфікованого електронного підпису;</p> <p>ДСТУ 4145-2002 “Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння” з функцією гешування за ДСТУ 7564-2014 “Інформаційні технології. Криптографічний захист інформації. Функція гешування”. Ці національні стандарти застосовуються для створення кваліфікованого електронного підпису з 01 січня 2021 року та для перевірки кваліфікованого електронного підпису;</p> <p>ДСТУ ISO/IEC 14888-3:2019 “Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 3. Механізми на основі дискретного логарифмування” із застосуванням алгоритму ECDSA зі ступенем розширення основного поля еліптичної кривої не менше ніж 256 з функціями гешування sha256 або sha512 відповідно до національного стандарту, визначеного пунктом 55 Переліку;</p> <p>2) для транскордонного співробітництва з будь-якою метою відповідно до вимог:</p> <p>встановлених національним стандартом, визначеним в пункті 55 Переліку;</p> <p>зазначених у підпункті 1 цього пункту.</p>
<p><b>Пункт відсутній</b></p>	<p><b>4. Міністерству цифрової трансформації України з метою виконання функцій центрального засвідчувального органу, забезпечення</b></p>

інтероперабельності та технологічної нейтральності національних технічних рішень у сфері електронних довірчих послуг, а також недопущення їх дискримінації, взаємного визнання українських та іноземних сертифікатів відкритих ключів та електронних підписів, що використовуються під час надання юридично значущих електронних послуг, забезпечити функціонування програмно-технічного комплексу центрального засвідчувального органу та захисту інформації, що в ньому обробляється, відповідно до вимог законодавства, шляхом впровадження на офіційному вебсайті центрального засвідчувального органу:

1) програмного забезпечення для створення та перевірки уніфікованих форматів удосконалених електронних підписів (CAAdES, PAdES, XAdES), а також контейнерів електронних документів (ASiC), що відповідають вимогам національних стандартів, визначених у пунктах 11-23 Переліку (далі – інструмент створення та перевірки удосконалених електронних підписів).

Функціонал інструменту створення та перевірки удосконалених електронних підписів забезпечує:

створення контейнерів електронних документів (ASiC), перевірку електронних документів, створених у результаті побудови контейнерів електронних документів (ASiC);

створення та перевірку удосконаленого електронного підпису CAAdES;

	<p>створення та перевірку удосконаленого електронного підпису PAdES;</p> <p>створення та перевірку удосконаленого електронного підпису XAdES;</p> <p>інтеграції технічних рішень з інформаційно-телекомунікаційною системою центрального засвідчувального органу, інтегрованою системою електронної ідентифікації та іншими інформаційно-телекомунікаційними системами;</p> <p>2) програмного забезпечення системи моніторингу надання та використання електронних довірчих послуг, що сприятиме підвищенню рівня безпеки електронних довірчих послуг та інтероперабельності технічних засобів, які підпадають під дію вимог цього наказу (далі – інструмент моніторингу сфери електронних довірчих послуг).</p> <p>Функціонал інструменту моніторингу сфери електронних довірчих послуг забезпечує:</p> <p>розповсюдження та своєчасне оновлення кваліфікованих сертифікатів відкритих ключів центрального засвідчувального органу та кваліфікованих надавачів електронних довірчих послуг в інформаційно-телекомунікаційних системах користувачів електронних довірчих послуг;</p> <p>подання повідомлень про зміни в Довірчому списку та заяв на отримання електронних довірчих послуг від центрального засвідчувального органу;</p> <p>обмін тестовими прикладами для перевірки правильності реалізації форматів, протоколів та</p>
--	---

	<p>інтерфейсів технічних засобів, які підпадають під дію вимог цього наказу, між кваліфікованими надавачами електронних довірчих послуг та розробниками таких технічних засобів (зокрема, інтеграція з тестовим програмно-технічним комплексом, створеним на офіційному вебсайті центрального засвідчувального органу, для формування тестових сертифікатів відкритих ключів);</p> <p>автоматизований обмін статистичними даними щодо надання електронних довірчих послуг, в тому числі, пов'язаними з формуванням електронних позначок часу та тестових сертифікатів відкритих ключів, між кваліфікованими надавачами електронних довірчих послуг та центральним засвідчувальним органом;</p> <p>моніторинг у режимі реального часу чинних кваліфікованих сертифікатів відкритих ключів користувачів електронних довірчих послуг за відповідними даними (атрибутами), що містяться в таких кваліфікованих сертифікатах, сформованих для підписувачів або створювачів електронних печаток;</p> <p>запобігання формуванню кваліфікованими надавачами електронних довірчих послуг нових кваліфікованих сертифікатів відкритих ключів за запитами на формування таких сертифікатів, які вже були оброблені раніше.</p>
Пункт відсутній	<p>5. 3 метою забезпечення інтероперабельності та технологічної нейтральності національних технічних</p>

рішень використовуються тестові сертифікати відкритих ключів, призначені для перевірки правильності реалізації форматів, протоколів та інтерфейсів у засобах електронного підпису чи печатки, програмно-технічних комплексах, а також інформаційних та інформаційно-телекомунікаційних системах.

Формування тестових сертифікатів відкритих ключів здійснюється з дотриманням вимог підпункту 6.9.2 пункту 6.9 розділу 6 національного стандарту ДСТУ ETSI EN 319 411-1:2019 (ETSI EN 319 411-1 V1.2.2 (2018-04), IDT) “Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для надавачів довірчих послуг, які видають сертифікати. Частина 1. Загальні вимоги”, затвердженого наказом державного підприємства “Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості” від 27 грудня 2019 року № 515, щодо наявності в такому сертифікаті позначки про те, що він виданий як тестовий сертифікат відкритого ключа.

Власники та розпорядники інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем повинні вживати заходи для недопущення використання тестових сертифікатів відкритих ключів в таких інформаційних та інформаційно-телекомунікаційних системах не за призначенням.

<p>4. Визнати таким, що втратив чинність, наказ Міністерства юстиції України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 18 листопада 2019 року № 3563/5/610 “Про встановлення вимог до технічних засобів, процесів їх створення, використання та функціонування у складі інформаційно-телекомунікаційних систем під час надання електронних довірчих послуг”, зареєстрований у Міністерстві юстиції України 20 листопада 2019 року за № 1172/34143.</p>	<p>6. Визнати таким, що втратив чинність, наказ Міністерства юстиції України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 18 листопада 2019 року № 3563/5/610 “Про встановлення вимог до технічних засобів, процесів їх створення, використання та функціонування у складі інформаційно-телекомунікаційних систем під час надання електронних довірчих послуг”, зареєстрований у Міністерстві юстиції України 20 листопада 2019 року за № 1172/34143.</p>
<p>5. Адміністратору інформаційно-телекомунікаційної системи центрального засвідчувального органу забезпечити:</p> <p>1) публікацію на офіційному вебсайті центрального засвідчувального органу технічних специфікацій з тестовими прикладами для перевірки правильності реалізації форматів, протоколів та інтерфейсів технічними засобами, визначеними в підпункті 2 пункту 1 цього наказу (кваліфікованого сертифіката електронного підпису, кваліфікованого сертифіката електронної печатки та кваліфікованого сертифіката автентифікації вебсайту, списків відкликаних сертифікатів, кваліфікованої позначки часу, інформації про статус сертифікатів, форматів підписаних даних, переліків об'єктних ідентифікаторів), не пізніше одного місяця з дати набрання чинності цим наказом;</p> <p>2) створення на офіційному вебсайті центрального засвідчувального органу функціонала для оцінки</p>	<p>7. Адміністратору інформаційно-телекомунікаційної системи центрального засвідчувального органу забезпечити:</p> <p>1) публікацію на офіційному вебсайті центрального засвідчувального органу технічних специфікацій з тестовими прикладами для перевірки правильності реалізації форматів, протоколів та інтерфейсів технічними засобами, визначеними в підпункті 2 пункту 1 цього наказу (кваліфікованого сертифіката електронного підпису, кваліфікованого сертифіката електронної печатки та кваліфікованого сертифіката автентифікації вебсайту, списків відкликаних сертифікатів, кваліфікованої позначки часу, інформації про статус сертифікатів, форматів підписаних даних, переліків об'єктних ідентифікаторів), не пізніше одного місяця з дати набрання чинності цим наказом;</p> <p>2) створення на офіційному вебсайті центрального засвідчувального органу функціонала для оцінки</p>

<p>внутрішньої і транскордонної технологічної сумісності технічних засобів, які підпадають під дію вимог цього наказу, та їх здатності взаємодіяти між собою не пізніше 06 листопада 2021 року.</p>	<p><b>внутрішньої та транскордонної технологічної сумісності технічних засобів, які підпадають під дію вимог цього наказу, та їх здатності взаємодіяти між собою шляхом запровадження та здійснення технічної підтримки до 01 січня 2022 року:</b>  <b>інструменту створення та перевірки удосконалених електронних підписів;</b>  <b>інструменту моніторингу сфери електронних довірчих послуг.</b></p>
<p>6. Установити, що об'єктні ідентифікатори алгоритмів криптографічного захисту інформації, визначених у підпункті 2 пункту 1 цього наказу, публікуються на офіційному вебсайті Держспецзв'язку до моменту їх реєстрації національною реєструючою організацією відповідно до законодавства.</p>	<p>8. Установити, що об'єктні ідентифікатори алгоритмів криптографічного захисту інформації, визначених у підпункті 2 пункту 1 цього наказу, публікуються на офіційному вебсайті Держспецзв'язку до моменту їх реєстрації національною реєструючою організацією відповідно до законодавства.</p>
<p>7. Директорату функціонального розвитку цифровізації Міністерства цифрової трансформації України (Халєєва А.П.) подати цей наказ на державну реєстрацію відповідно до Указу Президента України від 03 жовтня 1992 року № 493 “Про державну реєстрацію нормативно-правових актів міністерств та інших органів виконавчої влади”.</p>	<p>9. Директорату функціонального розвитку цифровізації Міністерства цифрової трансформації України (Халєєва А.П.) подати цей наказ на державну реєстрацію відповідно до Указу Президента України від 03 жовтня 1992 року № 493 “Про державну реєстрацію нормативно-правових актів міністерств та інших органів виконавчої влади”.</p>
<p>8. Цей наказ набирає чинності з дня його офіційного опублікування.</p>	<p>10. Цей наказ набирає чинності з дня його офіційного опублікування.</p>



<p>9. Контроль за виконанням цього наказу покласти на заступника Міністра цифрової трансформації України та заступника Голови Державної служби спеціального зв'язку та захисту інформації України відповідно до розподілу функціональних обов'язків.</p>	<p><b>11.</b> Контроль за виконанням цього наказу покласти на заступника Міністра цифрової трансформації України та заступника Голови Державної служби спеціального зв'язку та захисту інформації України відповідно до розподілу функціональних обов'язків.</p>
--	--

**Заступник Міністра цифрової  
трансформації України**

**Людмила РАБЧИНСЬКА**

\_\_\_\_\_ 2021 р.