Додаток 4
до Технічного регламенту щодо вимог до засобів електронної ідентифікації в контексті схеми електронної ідентифікації та процедури, що застосовуються для визначення рівня довіри до засобів електронної ідентифікації
(пункт 15)

Елементи технічних специфікацій та процедур до управління та організації

№ з/п	Рівні довіри до засобів електронної ідентифікації	Обов'язкові елементи технічних специфікацій та процедур
1	2	3
I. Адміністратори систем*		
1	Низький	1.1. Адміністратори систем повинні бути зареєстрованими відповідно до Закону України «Про державну реєстрацію юридичних осіб, фізичних осіб – підприємців та громадських формувань», мати визначену організаційну структуру та здійснювати діяльність у всіх сегментах, пов'язаних з наданням електронних послуг. 1.2. Адміністратори систем повинні мати повноваження витребувати, перевіряти та обробляти ідентифікаційні дані. 1.3. Адміністратори систем є відповідальними за шкоду заподіяну у сфері електронної ідентифікації, а також повинні мати достатні фінансові ресурси для продовження діяльності з видачі засобів електронної ідентифікації та експлуатації інформаційно-комунікаційних систем схем електронної ідентифікації. 1.4. Адміністратори систем є відповідальними за виконання будь-яких зобов'язань, переданих іншому суб'єкту (представництву), та за дотримання правил функціонування схеми електронної ідентифікації іншими суб'єктами (представництвами). 1.5. Адміністратори систем повинні мати план припинення діяльності, який має містити належний порядок припинення обслуговування або продовження обслуговування користувачів іншим адміністратором системи, способи повідомлення відповідних державних органів та кінцевих користувачів, а також детальну інформацію про захист, зберігання, знищення записів відповідно до правил функціонування схеми.
2	Середній	2.1. Такі самі, як для низького рівня довіри.
3	Високий	3.1. Такі самі, як для низького рівня довіри.
II. Публікація повідомлень та інформація для користувачів		

Продовження додатка 4

1	2	3
1	Низький	1.1. Має бути забезпечено оприлюднення опису процесів та процедур, пов'язаних із видачею та використанням засобів електронної ідентифікації, який має містити усі правила, умови експлуатації та відомості про платежі, у тому числі будь-які обмеження щодо використання засобів. Опис також має містити правила захисту персональних даних. 1.2. Має бути впроваджено відповідну політику та процедури з метою своєчасного (та у надійний спосіб) отримання користувачами інформації про будь-які зміни в описі процесів та процедур, пов'язаних із видачею та використанням засобів електронної ідентифікації, правилах, умовах експлуатації та правилах захисту персональних даних. 1.3. Має бути впроваджено відповідну політику та процедури, які забезпечать надання вичерпних відповідей на запити про надання інформації щодо видачі та використання засобів електронної ідентифікації.
2	Середній	2.1. Такі самі, як для низького рівня довіри.
3	Високий	3.1. Такі самі, як для низького рівня довіри.
III. Управління інформаційною безпекою		
1	Низький	1.1. Впроваджена система управління інформаційною безпекою та контролю за ризиками інформаційної безпеки.
2	Середній	2.1. Такі самі, як для низького рівня довіри. 2.2. Впроваджена система управління інформаційною безпекою та комплексна система захисту інформації відповідно до вимог законодавства у сфері захисту інформації з урахуванням вимог національних стандартів у сфері управління інформаційної безпеки.
3	Високий	3.1. Такі самі, як для середнього рівня довіри.
IV. Зберігання даних		
1	Низький	1.1. Запис та зберігання даних, які обробляються в інформаційно-комунікаційній системі схеми електронної ідентифікації, мають здійснюватися із використанням системи управління записами. 1.2. Зберігання даних, які оброблюються в інформаційно-комунікаційній системі схеми електронної ідентифікації, має здійснюватися протягом строків, визначених законодавством у сфері електронних комунікацій, захисту інформації та персональних даних, впродовж яких вони будуть необхідні для цілей аудиту та розслідування порушень вимог безпеки. 1.3. Після закінчення строку зберігання дані, які оброблялись в інформаційно-комунікаційній системі схеми електронної ідентифікації, мають знищуватись у гарантований спосіб, який забезпечує відсутність можливості відновлення таких даних.
2	Середній	2.1. Такі самі, як для низького рівня.

Продовження додатка 4

1	2	3
3	Високий	3.1. Такі самі, як для низького рівня.

V. Об’єктовий контроль та персонал (у розділі зазначено вимоги щодо об’єктів (будівель і приміщень) та працівників, обов’язки яких безпосередньо пов’язані із забезпеченням функціонування інформаційно-комунікаційної системи схеми електронної ідентифікації та випуском засобів електронної ідентифікації)		
1	Низький	1.1. Визначення адміністратором системи процедур, які забезпечують перевірку наявності у працівників належної підготовки, кваліфікації та досвіду, необхідних для виконання ними своїх обов’язків. 1.2. Наявність кількості працівників, які належно забезпечать функціонування інформаційно-комунікаційної системи схеми електронної ідентифікації та видача засобів електронної ідентифікації відповідно до прийнятих вимог, принципів та процедур. 1.3. Об’єкти (будівлі та приміщення), які використовуються для забезпечення функціонування інформаційно-комунікаційної системи схеми електронної ідентифікації та видача засобів електронної ідентифікації, підлягають постійному моніторингу та захисту від пошкоджень, спричинених техногенними катастрофами, несанкціонованим доступом та іншими чинниками, які можуть вплинути на безпеку функціонування. 1.4. На об’єктах (у будівлях та приміщеннях), які використовуються для забезпечення функціонування інформаційно-комунікаційної системи схеми електронної ідентифікації та видача засобів електронної ідентифікації, доступ до зон, у яких зберігаються та оброблюються персональні дані, ключова інформація (криптографічний матеріал) або інша вразлива інформація надається виключно уповноваженим адміністратором системи працівникам.
2	Середній	2.1. Такі самі, як для низького рівня довіри.
3	Високий	3.1. Такі самі, як для низького рівня довіри.
VI. Технічний контроль		
1	Низький	1.1. Наявність пропорційного технічного контролю для управління ризиками, які загрожують безпеці обслуговування, захисту конфіденційності, цілісності та доступності інформації, що оброблюється в інформаційно-комунікаційній системі. 1.2. Канали зв’язку, які використовуються для обміну персональними даними та вразливою інформацією, захищено від несанкціонованого ознайомлення, модифікації та повторного відтворення інформації. 1.3. Доступ до ключової інформації (криптографічного матеріалу), якщо така (такий) використовується для видачі засобів електронної

Продовження додатка 4

1	2	3
		ідентифікації та в інших сегментах інформаційно-комунікаційної системи схеми електронної ідентифікації, обмежено програмами, які чітко вимагають доступу залежно від кола посадових обов'язків. Забезпечується зберігання такого матеріалу у встановленому законодавством порядку. 1.4. Існують формалізовані процедури, які забезпечують підтримку безпеки впродовж визначеного терміну і можливість реагувати на зміни рівнів ризику, інциденти та порушення безпеки. 1.5. Усі засоби, що містять персональні дані, ключову інформацію (криптографічний матеріал) або іншу вразливу інформацію, зберігаються, передаються та знищуються у встановлений законодавством спосіб.
2	Середній	2.1. Такі самі, як для низького рівня довіри. 2.2. Ключову інформацію (криптографічний матеріал), якщо така (такий) використовується для видачі засобів електронної ідентифікації та в інших сегментах інформаційно-комунікаційної системи схеми електронної ідентифікації, захищено від несанкціонованого доступу та копіювання.
3	Високий	3.1. Такі самі, як для низького рівня довіри. 3.2. Ключова інформація (криптографічний матеріал), яка (який) використовується для видачі засобів електронної ідентифікації та в інших сегментах інформаційно-комунікаційної системи схеми електронної ідентифікації, захищається завдяки вбудованим апаратно-програмним засобам, що забезпечують захист записаних на них даних від несанкціонованого доступу, безпосереднього ознайомлення із значенням параметрів особистих ключів та їх копіювання.
VII. Аудит на відповідність цим вимогам		
1	Низький	1.1. Проведення внутрішніх аудитів інформаційної безпеки, які охоплюють усі сегменти інформаційно-комунікаційної системи схеми електронної ідентифікації, з метою забезпечення дотримання встановлених вимог, принципів та процедур у визначені строки.
2	Середній	2.1. Такі самі, як для низького рівня довіри. 2.2. Періодичне проведення незалежних зовнішніх аудитів інформаційної безпеки, які охоплюють усі складові інформаційно-комунікаційної системи схеми електронної ідентифікації, з метою забезпечення дотримання прийнятих вимог, принципів та процедур.
3	Високий	3.1. Систематичне проведення незалежних зовнішніх аудитів інформаційної безпеки, які охоплюють усі складові інформаційно-комунікаційної системи схеми електронної ідентифікації, з метою забезпечення дотримання встановлених вимог, принципів та процедур. 3.2. Проведення заходів державного контролю за станом технічного та криптографічного захисту інформації в інформаційно-комунікаційній системі схеми електронної ідентифікації.

* Адміністратори систем – юридичні особи, фізичні особи – підприємці, що здійснюють технічне та технологічне забезпечення функціонування інформаційно-комунікаційних систем.