ІМПЛЕМЕНТАЦІЙНИЙ РЕГЛАМЕНТ КОМІСІЇ (ЄС) 2015/1502 від 8 вересня 2015 року

про встановлення мінімальних технічних специфікацій та процедур для рівнів надійності засобів електронної ідентифікації відповідно до статті 8(3) Регламенту Європейського Парламенту і Ради (ЄС) № 910/2014 про електронну ідентифікацію та довірчі послуги для електронних транзакцій на внутрішньому ринку

(Текст стосується ЄЕП)

ЄВРОПЕЙСЬКА КОМІСІЯ,

Беручи до уваги Договір про функціонування Європейського Союзу,

Беручи до уваги Регламент Європейського Парламенту і Ради (ЄС) № 910/2014 від 23 липня 2014 року про електронну ідентифікацію та довірчі послуги для електронних транзакцій на внутрішньому ринку та про скасування Директиви 1999/93/ЄС ([1]), зокрема його статтю 8(3),

Оскільки:

(1) Статтею 8 Регламенту (ЄС) № 910/2014 передбачено, що схема електронної ідентифікації, нотифікована відповідно до статті 9(1), повинна встановлювати низький, істотний та високий рівні надійності засобів електронної ідентифікації, випущених відповідно до такої схеми.

(2) Визначення мінімальних технічних специфікацій, стандартів та процедур є важливим для забезпечення спільного розуміння деталей рівнів надійності та забезпечення інтероперабельності під час встановлення відповідності між національними рівнями надійності нотифікованих схем електронної ідентифікації та рівням надійності, зазначеними у статті 8, як передбачено статтею 12(4)(b) Регламенту (ЄС) № 910/2014.

(3) Міжнародний стандарт ISO/IEC 29115 було взято до уваги для цілей специфікацій і процедур, що викладені у цьому імплементаційному акті, як основний міжнародний стандарт, доступний у сфері рівнів надійності засобів електронної ідентифікації. Однак зміст Регламенту (ЄС) № 910/2014 відрізняється від зазначеного міжнародного стандарту, зокрема щодо вимог до підтвердження та верифікації, а також щодо способу врахування відмінностей між механізмами встановлення тотожності особи держав-членів та наявними в ЄС інструментами для такої цілі. Тому у додатку, який базується на цьому міжнародному стандарті, не повинно бути покликань на будь-який конкретний зміст ISO/IEC 29115.

(4) Цей Регламент було розроблено як орієнтований на результат підхід, який є найбільш доречним, що також відтворено в означеннях, використовуваних для позначення термінів та понять. У них враховано ціль Регламенту (ЄС) № 910/2014 щодо рівнів надійності засобів електронної ідентифікації. Тому, необхідно взяти найвищою мірою до уваги великомасштабний пілотний проект STORK, у тому числі специфікації, розроблені у його межах, а також означення та поняття в ISO/IEC 29115 під час встановлення специфікацій та процедур, викладених у цьому імплементаційному акті.

(5) Залежно від контексту, в якому аспект доказу тотожності особи необхідно верифікувати, авторитетні джерела можуть набувати багатьох форм, зокрема таких як реєстри, документи, органи. У різних державах-членах авторитетні джерела можуть відрізнятися одні від одних навіть у схожому контексті.

([1]) OB L 257, 28.08.2014, c. 73.

ІМПЛЕМЕНТАЦІЙНИЙ РЕГЛАМЕНТ КОМІСІЇ (ЄС) 2015/1502

від 8 вересня 2015 року

про встановлення мінімальних технічних специфікацій та процедур для рівнів надійності засобів електронної ідентифікації відповідно до статті 8(3) Регламенту Європейського Парламенту і Ради (ЄС) № 910/2014 про електронну ідентифікацію та довірчі послуги для електронних транзакцій на внутрішньому ринку

(Текст стосується ЄЕП)

ЄВРОПЕЙСЬКА КОМІСІЯ,

Беручи до уваги Договір про функціонування Європейського Союзу,

Беручи до уваги Регламент Європейського Парламенту і Ради (ЄС) № 910/2014 від 23 липня 2014 року про електронну ідентифікацію та довірчі послуги для електронних транзакцій на внутрішньому ринку та про скасування Директиви 1999/93/ЄС ([1]), зокрема його статтю 8(3),

Оскільки:

(1) Статтею 8 Регламенту (ЄС) № 910/2014 передбачено, що схема електронної ідентифікації, нотифікована відповідно до статті 9(1), повинна встановлювати низький, істотний та високий рівні надійності засобів електронної ідентифікації, випущених відповідно до такої схеми.

(2) Визначення мінімальних технічних специфікацій, стандартів та процедур є важливим для забезпечення спільного розуміння деталей рівнів надійності та забезпечення інтероперабельності під час встановлення відповідності між національними рівнями надійності нотифікованих схем електронної ідентифікації та рівням надійності, зазначеними у статті 8, як передбачено статтею 12(4)(b) Регламенту (ЄС) № 910/2014.

(3) Міжнародний стандарт ISO/IEC 29115 було взято до уваги для цілей специфікацій і процедур, що викладені у цьому імплементаційному акті, як основний міжнародний стандарт, доступний у сфері рівнів надійності засобів електронної ідентифікації. Однак зміст Регламенту (ЄС) № 910/2014 відрізняється від зазначеного міжнародного стандарту, зокрема щодо вимог до підтвердження та верифікації, а також щодо способу врахування відмінностей між механізмами встановлення тотожності особи держав-членів та наявними в ЄС інструментами для такої цілі. Тому у додатку, який базується на цьому міжнародному стандарті, не повинно бути покликань на будь-який конкретний зміст ISO/IEC 29115.

(4) Цей Регламент було розроблено як орієнтований на результат підхід, який є найбільш доречним, що також відтворено в означеннях, використовуваних для позначення термінів та понять. У них враховано ціль Регламенту (ЄС) № 910/2014 щодо рівнів надійності засобів електронної ідентифікації. Тому, необхідно взяти найвищою мірою до уваги великомасштабний пілотний проект STORK, у тому числі специфікації, розроблені у його межах, а також означення та поняття в ISO/IEC 29115 під час встановлення специфікацій та процедур, викладених у цьому імплементаційному акті.

(5) Залежно від контексту, в якому аспект доказу тотожності особи необхідно верифікувати, авторитетні джерела можуть набувати багатьох форм, зокрема таких як реєстри, документи, органи. У різних державах-членах авторитетні джерела можуть відрізнятися одні від одних навіть у схожому контексті.

(6) Вимоги до підтвердження та верифікації тотожності особи повинні враховувати різні

([1]) ОВ L 257, 28.08.2014, с. 73.

системи та практики, забезпечуючи достатньо високий рівень надійності, щоб встановити необхідну довіру. Тому прийняття процедур, які використовувались раніше з відмінною від випуску засобів електронної ідентифікації метою, необхідно здійснювати умовно після підтвердження відповідності таких процедур вимогам, передбаченим для відповідного рівня надійності.

(7) Зазвичай використовують певні чинники автентифікації, такі як спільний секрет, фізичні пристрої та фізичні атрибути. Однак, необхідно сприяти використанню більшої кількості чинників автентифікації, особливо з різних категорій чинників, для того, щоб посилювати безпеку процесу автентифікації.

(8) Дія цього Регламенту не повинна поширюватися на права представлення юридичних осіб. Однак, у додатку необхідно передбачати вимоги до встановлення зв'язку між засобами електронної ідентифікації фізичних та юридичних осіб.

(9) Необхідно визнавати важливість систем управління інформаційною безпекою та послугами, як і важливість використання визнаних методик та застосування принципів, що містяться в стандартах, таких як стандарти серій ISO/IEC 27000 та ISO/IEC 20000.

(10) Необхідно також брати до уваги належну практику щодо застосування рівнів надійності у державах-членах.

(11) Сертифікація безпеки інформаційних технологій на основі міжнародних стандартів є важливим інструментом для верифікації відповідності безпеки продуктів вимогам цього імплементаційного акту.

(12) Комітет, зазначений у статті 48 Регламенту (ЄС) № 910/2014, не надав висновку впродовж терміну, визначеного його головою,

УХВАЛИЛА ЦЕЙ РЕГЛАМЕНТ:

Стаття 1

1. Низький, істотний та високий рівні надійності засобів електронної ідентифікації, випущених відповідно до нотифікованої схеми електронної ідентифікації, встановлюються відповідно до специфікацій та процедур, передбачених у додатку.

2. Специфікації та процедури, передбачені у додатку, необхідно використовувати для визначення рівня надійності засобів електронної ідентифікації, випущених відповідно до нотифікованої схеми електронної ідентифікації, шляхом встановлення надійності та якості таких елементів:

(a) внесення в базу, як передбачено в секції 2.1 додатка до цього Регламенту відповідно до статті 8(3)(a) Регламенту (ЄС) № 910/2014;

(b) управління засобами електронної ідентифікації, як передбачено в секції 2.2 додатка до цього Регламенту відповідно до статті 8(3)(b) та (f) Регламенту (ЄС) № 910/2014;

(c) автентифікація, як передбачено в секції 2.3 додатка до цього Регламенту відповідно до статті 8(3)(c) Регламенту (ЄС) № 910/2014;

(d) управління та організація, як передбачено в секції 2.4 додатка до цього Регламенту відповідно до статті 8(3)(d) та (e) Регламенту (ЄС) № 910/2014.

3. Якщо засоби електронної ідентифікації, випущені відповідно до нотифікованої схеми електронної ідентифікації, відповідають вимогам, передбаченим для високого рівня надійності, то припускають, що ці засоби відповідають аналогічним вимогам до низького рівня надійності.

4. Якщо інше не зазначено у відповідній частині додатка, всі елементи, передбачені у додатку для певного рівня надійності засобів електронної ідентифікації, випущених відповідно до нотифікованої схеми електронної ідентифікації, необхідно виконати, щоб відповідати заявленому рівню надійності.

Стаття 2

Цей Регламент набуває чинності на двадцятий день після його публікації в *Офіційному віснику Європейського Союзу*.

Цей Регламент обов'язковий у повному обсязі та підлягає прямому застосуванню у всіх державах-членах.

Вчинено у Брюсселі 8 вересня 2015 року.

За Комісію

Президент

Jean-Claude JUNCKER

ДОДАТОК

Технічні специфікації та процедури щодо низького, істотного та високого рівнів надійності засобів електронної ідентифікації, випущених відповідно до нотифікованої схеми електронної ідентифікації

1. Застосовні терміни та означення

Для цілей цього додатку застосовують такі терміни та означення:

(1) «авторитетне джерело» означає будь-яке незалежно від його форми джерело, на яке можна покластися як на таке, що надає точні дані, інформацію та/або відомості, які можуть бути використані для доказу тотожності особи.

(2) «чинник автентифікації» означає чинник, який підтверджено як такий, що пов’язаний з особою, та поділяється на такі категорії:

(a) «чинник автентифікації на підставі володіння» означає чинник автентифікації, коли від суб’єкта вимагають продемонструвати свої володіння;

(b) «чинник автентифікації на підставі знання» означає чинник автентифікації, коли від суб’єкта вимагають продемонструвати свої знання;

(c) «чинник автентифікації на підставі властивості» означає чинник автентифікації, що базується на фізичному атрибуті фізичної особи, у межах якого від суб’єкта вимагають продемонструвати, що він має такий фізичний атрибут;

(3) «динамічна автентифікація» означає електронний процес з використанням криптографії та інших методів для забезпечення засобу створення на вимогу електронного доказу, що ідентифікаційні дані знаходяться під контролем суб’єкту або у його володінні та який змінюється за кожної автентифікації між суб’єктом та системою верифікації особи суб’єкту.

(4) «система управління інформаційною безпекою» означає низку процесів і процедур, призначених для управління прийнятними рівнями ризиків, пов’язаних з інформаційною безпекою.

2. Технічні специфікації та процедури

Елементи технічних специфікацій та процедур, наведені у цьому додатку, повинні використовуватись для визначення способів застосування вимог та критеріїв, передбачених у статті 8 Регламенту (ЄС) № 910/2014, до засобів електронної ідентифікації, випущених відповідно до схеми електронної ідентифікації.

2.1. *Внесення в базу*

2.1.1. Подання заявки та реєстрація

Рівень надійності	Необхідні елементи
Низький	1. Забезпечення того, що заявник знає умови, пов’язані з використанням засобів електронної ідентифікації. 2. Забезпечення того, що заявник знає рекомендовані заходи безпеки, пов’язані з використанням засобів електронної ідентифікації. 3. Збір відповідних ідентифікаційних даних, необхідних для підтвердження та верифікації тотожності особи.
Істотний	Такі самі, як для низького рівня.
Високий	Такі самі, як для низького рівня.

2.1.2. Підтвердження та верифікація тотожності особи (фізичної особи)

Рівень надійності	Необхідні елементи
Низький	1. Можна припустити, що особа володіє відомостями, які визнано державою-членом, у якій зроблено заявку на засоби електронного встановлення тотожності особи, та які представляють заявлену особу. 2. Можна припустити, що такі відомості є справжніми або такими, існування яких підтверджено авторитетним джерелом і які виявляються дійсними. 3. Авторитетному джерелу відомо, що заявлена особа існує, і можна припустити, що особа, яка заявляє про тотожність з нею, є цією особою.
Істотний	Елементи низького рівня та виконання додатково однієї з вимог, зазначених у пунктах 1–4: 1. Особу верифікували, як таку, що володіє відомостями, які визнано державою-членом, в якій зроблено заявку на засоби електронного встановлення тотожності особи, та які представляють заявлену особу, та здійснюється перевірка відомостей, щоб визначити, чи вони є справжнім; або відомо, відповідно до авторитетного джерела, що такі відомості існують та відносяться до реальної особи, та вжито заходів, щоб мінімізувати ризик відсутності тотожності особи з заявленою особою, беручи до уваги, наприклад, ризик втрати, викрадення, призупинення дії, відкликання чи закінчення терміну дії відомостей; або 2. Посвідчення особи пред'являють під час процесу реєстрації у державі-члені, у якій його було видано, і виявляється, що таке посвідчення стосується особи, яка його пред'являє, та вжито заходів, щоб мінімізувати ризик відсутності тотожності особи з заявленою особою, беручи до уваги, наприклад, ризик втрати, викрадення, призупинення дії, відкликання чи закінчення терміну дії документів; або 3. Якщо процедури, що використовувались раніше публічними або приватними суб'єктами у тій самій державі-члені для цілей, відмінних від випуску засобів електронної ідентифікації, забезпечують надійність, рівноцінну надійності процедур, визначених у секції 2.1.2 для істотного рівня надійності, то суб'єкт, відповідальний за реєстрацію, не повинен повторно виконувати попередні процедури за умови, що їхню рівноцінну надійність підтверджено органом оцінки відповідності, зазначеним у статті 2(13) Регламенту Європейського Парламенту і Ради (ЄС) № 765/2008 ([1]), або аналогічним органом; або 4. Якщо засоби електронної ідентифікації випущено на основі дійсних нотифікованих засобів електронної ідентифікації, які мають істотний або високий рівень надійності, та, беручи до уваги ризики зміни даних персональної ідентифікації, немає необхідності повторно здійснювати процеси підтвердження та верифікації тотожності особи. Якщо засоби електронної ідентифікації, які взято за основу, не було нотифіковано, необхідно, щоб орган оцінки відповідності, зазначений у статті 2(13) Регламенту (ЄС) № 765/2008, або аналогічний орган підтвердив істотний або високий рівень надійності.

Високий	Необхідно виконати вимоги пунктів 1 або 2: 1. Елементи істотного рівня та виконання додатково однієї з вимог, зазначених у пунктах (a) – (c): (a) Якщо особу верифікували, як таку, що володіє фотографічними або біометричними ідентифікаційними відомостями, які визнано державою-членом, в якій зроблено заявку на засоби електронного встановлення тотожності особи, і ці відомості представляють заявлену особу, такі відомості перевіряються для встановлення їх дійсності відповідно до авторитетного джерела; та заявника ідентифікують як заявлену особу шляхом зіставлення однієї або більше фізичних характеристик особи з авторитетним джерелом; або (b) Якщо процедури, що використовувались раніше публічними або приватними суб'єктами у тій самій державі-члені для цілей, відмінних від випуску засобів електронної ідентифікації, забезпечують надійність, рівноцінну надійності процедур, визначених у секції 2.1.2 для високого рівня надійності, то суб'єкт, відповідальний за реєстрацію, не повинен повторно виконувати попередні процедури за умови, що їхню рівноцінну надійність підтверджено органом оцінки відповідності, зазначеним у статті 2(13) Регламенту (ЄС) № 765/2008, або аналогічним органом та вжито заходів, щоб показати, що результати попередніх процедур залишаються дійсними; або (c) Якщо засоби електронної ідентифікації випущено на основі дійсних нотифікованих засобів електронної ідентифікації, які мають високий рівень надійності, та, беручи до уваги ризики зміни даних персональної ідентифікації, немає необхідності повторно здійснювати процеси підтвердження та верифікації тотожності особи. Якщо засоби електронної ідентифікації, які взято за основу, не було нотифіковано, потрібно, щоб орган оцінки відповідності, зазначений у статті 2(13) Регламенту (ЄС) № 765/2008, або аналогічний орган підтвердив високий рівень надійності та вжито заходів, щоб показати, що результати попередньої процедури випуску нотифікованих засобів електронної ідентифікації залишаються дійсними. АБО 2. Якщо заявник не надає будь-які визнані фотографічні або біометричні ідентифікаційні відомості, застосовують такі самі процедури, що використовуються на національному рівні державою-членом суб'єкта, відповідального за реєстрацію, щоб отримати такі визнані фотографічні або біометричні ідентифікаційні відомості.

([1]) Регламент Європейського Парламенту і Ради (ЄС) № 765/2008 від 9 липня 2008 року щодо вимог до акредитації та ринкового нагляду у сфері реалізації продуктів та про скасування Регламенту (ЄЕС) № 339/93 (OB L 218, 13.08.2008, с. 30).

2.1.4. Підтвердження та верифікація тотожності особи (фізичної особи)

Рівень надійності	Необхідні елементи
Низький	1. Заявлену юридичну особу представлено на основі відомостей, визнаних державою-членом, в якій зроблено заявку на засоби електронного встановлення тотожності особи. 2. Відомості виявляються дійсним, і можна припустити, що вони є

	справжніми або такими, існування яких підтверджено авторитетним джерелом, якщо занесення юридичної особи до авторитетного джерела є добровільним та регулюється домовленістю між юридичною особою та авторитетним джерелом. 3. Авторитетному джерелу не відомо статус юридичної особи, який би перешкоджав їй діяти як зазначеній юридичній особі.
Істотний	Елементи низького рівня та виконання додатково однієї з вимог, зазначених у пунктах 1–3: 1. Заявлену юридичну особу представлено на основі відомостей, визнаних державою-членом, в якій зроблено заявку на засоби електронного встановлення тотожності особи, у тому числі назва юридичної особи, організаційно-правова форма і (за наявності) її реєстраційний номер, та здійснюється перевірка відомостей, щоб визначити, чи вони є справжніми; або відомо, відповідно до авторитетного джерела, що такі відомості існують, якщо занесення юридичної особи до авторитетного джерела необхідно для того, щоб юридична особа діяла у межах свого сектору, та вжито заходів, щоб мінімізувати ризик відсутності тотожності особи з заявленою юридичною особою, беручи до уваги, наприклад, ризик втрати, викрадення, призупинення дії, відкликання чи закінчення терміну дії документів; або 2. Якщо процедури, що використовувались раніше публічними або приватними суб'єктами у тій самій державі-члені для цілей, відмінних від випуску засобів електронної ідентифікації, забезпечують надійність, рівноцінну надійності процедур, визначених у секції 2.1.3 для істотного рівня надійності, то суб'єкт, відповідальний за реєстрацію, не повинен повторно виконувати попередні процедури за умови, що їхню рівноцінну надійність підтверджено органом оцінки відповідності, зазначеним у статті 2(13) Регламенту (ЄС) № 765/2008, або аналогічним органом; або 3. Якщо засоби електронної ідентифікації випущено на основі дійсних нотифікованих засобів електронної ідентифікації, які мають істотний або високий рівень надійності, немає необхідності повторно здійснювати процеси підтвердження та верифікації тотожності особи. Якщо засоби електронної ідентифікації, які взято за основу, не було нотифіковано, необхідно, щоб орган оцінки відповідності, зазначений у статті 2(13) Регламенту (ЄС) № 765/2008, або аналогічний орган підтвердив істотний або високий рівень надійності.
Високий	Елементи істотного рівня та виконання додатково однієї з вимог, зазначених у пунктах 1–3: 1. Заявлену юридичну особу представлено на основі відомостей, визнаних державою-членом, в якій зроблено заявку на засоби електронного встановлення тотожності особи, у тому числі назва юридичної особи, організаційно-правова форма і щонайменше один унікальний ідентифікатор, що представляє юридичну особу та застосовується в національному контексті та здійснюється перевірка відомостей, щоб визначити, чи вони є дійсними відповідно до авторитетного джерела; або 2. Якщо процедури, що використовувались раніше публічними або приватними суб'єктами у тій самій державі-члені для цілей, відмінних від випуску засобів електронної ідентифікації, забезпечують надійність, рівноцінну надійності процедур, визначених у секції 2.1.3 для високого рівня надійності, то суб'єкт, відповідальний за реєстрацію, не повинен повторно виконувати попередні процедури за умови, що їхню рівноцінну надійність підтверджено органом оцінки відповідності, зазначеним у статті 2(13) Регламенту (ЄС) № 765/2008, або аналогічним органом

	та вжито заходів, щоб показати, що результати попередніх процедур залишаються дійсними; або 3. Якщо засоби електронної ідентифікації випущено на основі дійсних нотифікованих засобів електронної ідентифікації, які мають високий рівень надійності, немає необхідності повторно здійснювати процеси підтвердження та верифікації тотожності особи. Якщо засоби електронної ідентифікації, які взято за основу, не було нотифіковано, потрібно, щоб орган оцінки відповідності, зазначений у статті 2(13) Регламенту (ЄС) № 765/2008, або аналогічний орган підтвердив високий рівень надійності та вжито заходів, щоб показати, що результати попередньої процедури випуску нотифікованих засобів електронної ідентифікації залишаються дійсними.

2.1.4. Встановлення зв’язку між засобами електронної ідентифікації фізичних та юридичних осіб

У відповідних випадках, для встановлення зв’язку між засобами електронної ідентифікації фізичної особи та засобами електронної ідентифікації юридичної особи («встановлення зв’язку») застосовують такі умови:

(1) Необхідно передбачити можливість призупинення та/або відкликання встановлення зв’язку. Управління терміном дії зв’язку (наприклад, активація, призупинення, поновлення, відкликання) здійснюється відповідно до національно визнаних процедур.

(2) Фізична особа, чиї засоби електронної ідентифікації пов’язані з засобами електронної ідентифікації юридичної особи, може делегувати встановлення зв’язку іншій фізичній особі на основі національно визнаних процедур. Однак фізична особа, яка делегує свої повноваження, залишається відповідальною.

(3) Встановлення зв’язку повинно відбуватись у такий спосіб:

Рівень надійності	Необхідні елементи
Низький	1. Підтвердження тотожності фізичної особи, яка діє від імені юридичної особи, верифіковано як таке, що було виконано на низькому або вищому рівні. 2. Зв’язок встановлено на основі національно визнаних процедур. 3. Авторитетному джерелу не відомо статус фізичної особи, який би перешкоджав їй діяти від імені такої юридичної особи.
Істотний	Пункт 3 необхідних елементів низького рівня, а також: 1. Підтвердження тотожності фізичної особи, яка діє від імені юридичної особи, верифіковано як таке, що було виконано на істотному або високому рівні. 2. Зв’язок встановлено на основі національно визнаних процедур, що привело до його реєстрації в авторитетному джерелі. 3. Встановлення зв’язку верифіковано на основі інформації з авторитетного джерела.
Високий	Пункт 3 необхідних елементів низького рівня та пункт 2 необхідних елементів істотного рівня, а також: 1. Підтвердження тотожності фізичної особи, яка діє від імені юридичної особи, верифіковано як таке, що було виконано на високому рівні. 2. Встановлення зв’язку було верифіковано на основі унікального ідентифікатора, що представляє юридичну особу та застосовується у національному контексті, та на основі інформації, яка однозначно представляє фізичну особу з авторитетного джерела.

2.2. *Управління засобами електронної ідентифікації*

2.2.1. Характеристика та дизайн засобів електронної ідентифікації

Рівень надійності	Необхідні елементи
Низький	1. Засоби електронної ідентифікації використовують щонайменше один чинник автентифікації. 2. Засоби електронної ідентифікації розроблено таким чином, щоб орган, який їх випускає, вживав необхідних заходів для перевірки того, чи вони використовуються тільки під контролем або у межах володіння особи, якій такі засоби належать.
Істотний	1. Засоби електронної ідентифікації використовують щонайменше два чинники автентифікації різних категорій. 2. Засоби електронної ідентифікації розроблено таким чином, щоб можна було припустити, що вони використовуються тільки під контролем або у межах володіння особи, якій такі засоби належать.
Високий	Істотний рівень, а також: 1. Засоби електронної ідентифікації захищено від дублювання та неправомірного втручання, а також від зловмисників з високою імовірністю здійснення нападу. 2. Засоби електронної ідентифікації розроблено таким чином, що особа, якій вони належать, може надійно захистити їх від використання іншими.

2.2.2. Випуск, доставка та активація

Рівень надійності	Необхідні елементи
Низький	Після випуску засоби електронної ідентифікації доставляють шляхом застосування механізму, за допомогою якого, можна припустити, вони дістануться тільки призначеній особі.
Істотний	Після випуску засоби електронної ідентифікації доставляють шляхом застосування механізму, за допомогою якого, можна припустити, вони передаються у володіння тільки особи, якій вони належать.
Високий	У процесі активації здійснюється верифікація передання засобів електронної ідентифікації тільки у володіння особі, якій вони належать.

2.2.3. Випуск, доставка та активація

Рівень надійності	Необхідні елементи
Низький	1. Існує можливість призупинення та/або відкликання засобу електронної ідентифікації вчасно та ефективно. 2. Існують заходи для запобігання несанкціонованим призупиненню, відкликанню та/або повторній активації. 3. Повторна активація повинна здійснюватися тільки за умови продовження дотримання тих самих вимог до надійності, які було встановлено перед призупиненням або відкликанням.
Істотний	Такі самі, як для низького рівня.
Високий	Такі самі, як для низького рівня.

2.2.4. Поновлення та заміна

Рівень надійності	Необхідні елементи
Низький	Беручи до уваги ризики зміни даних персональної ідентифікації, необхідно, щоб процеси поновлення або заміни відповідали тим самим вимогам до надійності, що й початковий процес підтвердження та верифікації тотожності особи, або базувались на дійсних засобах електронної ідентифікації того самого або вищого рівня надійності.
Істотний	Такі самі, як для низького рівня.
Високий	Низький рівень, а також: Якщо поновлення та заміна базується на дійсних засобах електронної ідентифікації, здійснюється верифікація тотожності особи з авторитетним джерелом.

2.3. *Автентифікація*

У цій секції розглядаються загрози, пов'язані з використанням механізму автентифікації, та передбачено вимоги до кожного рівня надійності. У цій секції засоби контролю вважаються такими, що відповідають ризикам на зазначеному рівні.

2.3.1. Механізм автентифікації

У наведеній нижче таблиці встановлено вимоги для кожного рівня надійності щодо механізму автентифікації, за допомогою якого фізична або юридична особа використовує засоби електронної ідентифікації для підтвердження своєї тотожності зі стороною-користувачем.

Рівень надійності	Необхідні елементи
Низький	1. Випуску даних персональної ідентифікації передують надійна верифікація засобів електронної ідентифікації та встановлення їх дійсність. 2. Якщо дані персональної ідентифікації зберігаються як частина механізму автентифікації, захист такої інформації здійснюють для того, щоб запобігти втратам та компрометації, у тому числі аналізу у режимі офлайн. 3. У межах механізму автентифікації впроваджують засоби контролю безпеки для верифікації засобів електронної ідентифікації, тому надзвичайно малоймовірним є те, що такі дії, як вгадування, підслуховування, повторне відтворення повідомленням та маніпулювання ним зловмисником з підвищеною базовою ймовірністю здійснення нападу, зможуть дестабілізувати механізми автентифікації.
Істотний	Низький рівень, а також: 1. Випуску даних персональної ідентифікації передують надійна верифікація засобів електронної ідентифікації та встановлення їх дійсність за допомогою динамічної автентифікації. 2. У межах механізму автентифікації впроваджують засоби контролю безпеки для верифікації засобів електронної ідентифікації, тому надзвичайно малоймовірним є те, що такі дії, як вгадування, підслуховування, повторне відтворення повідомленням та маніпулювання ним з середньою ймовірністю здійснення нападу, зможуть дестабілізувати механізми автентифікації.
Високий	Істотний рівень, а також: У межах механізму автентифікації впроваджують засоби контролю безпеки для верифікації засобів електронної ідентифікації, тому надзвичайно малоймовірним є те, що такі дії, як вгадування, підслуховування, повторне відтворення повідомленням та маніпулювання ним зловмисником з високою ймовірністю здійснення нападу, зможуть дестабілізувати механізми автентифікації.

2.4. *Управління та організація*

Усі учасники, які надають послугу, пов’язану з електронною ідентифікацією, в транскордонному контексті («постачальники») повинні мати у розпорядженні задокументовані порядок управління інформаційною безпекою, принципи, підходи до управління ризиками та інших визнані засоби контролю для запевнення відповідних органів управління, відповідальних за схеми електронної ідентифікації у відповідній державі-члені, що чинні порядки знаходяться в їхньому розпорядженні. У секції 2.4 усі вимоги та елементи повинні вважатися такими, що відповідають ризикам на зазначеному рівні.

2.4.1. Загальні положення

Рівень надійності	Необхідні елементи
Низький	1. Постачальники, які забезпечують будь-яке експлуатаційне обслуговування, охоплене цим Регламентом, є публічним органом або юридичною особою, які визнано національним законодавством держави-члена, мають засновану організацію та повною мірою діють у всіх сегментах, пов’язаних з наданням таких послуг. 2. Постачальники відповідають будь-яким законним вимогам, покладеним на них у зв’язку з діяльністю та наданням послуг, у тому числі види інформації, яка може бути затребувана, способи підтвердження тотожності особи, види інформації, яку можна зберігати, та термін зберігання такої. 3. Постачальники можуть продемонструвати свою здатність приймати ризик відповідальності за збитки, а також наявність достатніх фінансових ресурсів для продовження діяльності та надання послуг. 4. Постачальники несуть відповідальність за виконання будь-яких зобов’язань, переданих іншому суб’єкту, та дотримання принципів схеми так, ніби самі постачальники виконували такі обов’язки. 5. Схеми електронної ідентифікації, не передбачені національним законодавством, повинні охоплювати чинний план щодо припинення дії. Такий план повинен містити належний порядок припинення обслуговування або продовження обслуговування іншим постачальником, спосіб повідомлення відповідних органів та кінцевих користувачів, а також детальну інформацію про захист, зберігання, знищення записів відповідно до принципів схеми.
Істотний	Такі самі, як для низького рівня.
Високий	Такі самі, як для низького рівня.

2.4.2. Оприлюднені повідомлення та інформація про користувача

Рівень надійності	Необхідні елементи
Низький	1. Наявність оприлюдненого означення послуги, яке містить усі застосовні терміни, умови та збори, у тому числі будь-які обмеження щодо її використання. Означення послуги повинно містити принципи приватності. 2. Необхідно ввести в дію відповідні принципи та процедури, щоб забезпечити, що користувачі послуги отримують своєчасно та у надійний спосіб інформацію про будь-які зміни до означення послуги та до будь-яких застосовних термінів, умов та принципів приватності для зазначеної послуги. 3. Необхідно ввести в дію відповідні принципи та процедури, що забезпечать надання повних та правильних відповідей на запити про надання інформації.
Істотний	Такі самі, як для низького рівня.
Високий	Такі самі, як для низького рівня.

2.4.3. Управління інформаційною безпекою

Рівень надійності	Необхідні елементи

Низький	Існує ефективна система управління інформаційною безпекою для управління ризиками інформаційної безпеки та контролю за такими.
Істотний	Низький рівень, а також: Система управління інформаційною безпекою відповідає затвердженим стандартам або принципам управління ризиками інформаційної безпеки та контролю за такими.
Високий	Такі самі, як для істотного рівня.

2.4.4. Ведення обліку

Рівень надійності	Необхідні елементи
Низький	1. Запис та зберігання відповідної інформації шляхом використання ефективної системи управління записами, беручи до уваги застосовне законодавство та належну практику щодо захисту даних та збереження даних. 2. Зберігання, наскільки це дозволяє національне законодавство або інші національні адміністративні домовленості, та захист записів на періоду, протягом якого вони будуть необхідні для цілей аудиту та розслідування порушень безпеки, після чого усі записи безпечно знищуються.
Істотний	Такі самі, як для низького рівня.
Високий	Такі самі, як для низького рівня.

2.4.5. Об’єкти та персонал

У наведеній нижче таблиці представлено вимоги щодо об’єктів, персоналу і субпідрядників, за наявності таких, які беруть на себе зобов’язання, зазначені у цьому Регламенті. Дотримання всіх вимог здійснюється пропорційно рівню ризику, пов’язаного з передбаченим рівнем надійності.

Рівень надійності	Необхідні елементи
Низький	1. Наявність процедур, які забезпечують, що персонал та субпідрядники мають належну підготовку, кваліфікацію та досвід стосовно умінь, які необхідні для виконання ними своїх ролей. 2. Наявність відповідного персоналу та субпідрядників, які належно працюють та забезпечують надання послуг відповідно до принципів та процедур. 3. Об’єкти, які використовують для надання послуг, підлягають постійному моніторингу та захисту від пошкоджень, спричинених екологічними подіями, несанкціонованим доступом та іншими чинниками, які можуть вплинути на безпеку обслуговування. 4. Об’єкти, які використовують для надання послуг, забезпечують, що доступ до зон, у яких зберігають та обробляють персональну, криптографічну або іншу вразливу інформацію, мають лише уповноважені персонал або субпідрядники.
Істотний	Такі самі, як для низького рівня.
Високий	Такі самі, як для низького рівня.

2.4.6. Технічний контроль

Рівень надійності	Необхідні елементи

Низький	1. Наявність пропорційного технічного контролю для управління ризиками, які загрожують безпеці обслуговування, захисту конфіденційності, цілісності та доступності інформації, що обробляється. 2. Канали електронного зв'язку, які використовують для обміну особистою та вразливою інформацією, захищено від підслуховування, маніпуляцій та повторного відтворення. 3. Доступ до вразливого криптографічного матеріалу, якщо такий використовується для випуску засобів електронної ідентифікації та автентифікації, обмежено ролями та програмами, які чітко вимагають доступу. Необхідно забезпечити, щоб такий матеріал ніколи не зберігався у формі простого тексту. 4. Існують процедури, які забезпечують підтримку безпеки впродовж певного часу і можливість реагувати на зміни рівнів ризику, інциденти та порушення безпеки. 5. Усі засоби, що містять особисту, криптографічну або іншу вразливу інформацію, зберігаються, передаються та знищуються у безпечний та захищений спосіб.
Істотний	Такі самі, як для низького рівня. Вразливий криптографічний матеріал, якщо такий використовується для випуску засобів електронної ідентифікації та автентифікації, захищено від неправомірного втручання.
Високий	Такі самі, як для істотного рівня.

2.4.7. Відповідність вимогам та аудит

Рівень надійності	Необхідні елементи
Низький	Періодичне проведення внутрішніх аудитів, які охоплюють усі сегменти, пов'язані з постачанням наданих послуг, з метою забезпечення дотримання відповідних принципів.
Істотний	Періодичне проведення незалежних внутрішніх та зовнішніх аудитів, які охоплюють усі сегменти, пов'язані з постачанням наданих послуг, з метою забезпечення дотримання відповідних принципів.
Високий	1. Періодичне проведення незалежних зовнішніх аудитів, які охоплюють усі сегменти, пов'язані з постачанням наданих послуг, з метою забезпечення дотримання відповідних принципів. 2. Якщо схемою безпосередньо управляє державний орган, її аудит здійснюється відповідно до національного законодавства.