ІМПЛЕМЕНТАЦІЙНЕ РІШЕННЯ КОМІСІЇ (ЄС) 2016/650

від 25 квітня 2016 року

щодо стандартів оцінки безпеки засобів для створення кваліфікованих підпису та печатки відповідно до статей 30(3) та 39(2) 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 статті 30(3) та 39(2),

Оскільки:

(1) У додатку II до Регламенту (ЄС) № 910/2014 встановлено вимоги до засобів для створення кваліфікованого електронного підпису та засобів для створення кваліфікованої електронної печатки.

(2) Завдання складання технічних специфікацій, необхідних для виробництва та введення в обіг продуктів, беручи до уваги поточний стан технологій, виконується організаціями, компетентними в сфері стандартизації.

(3) ISO/IEC (Міжнародна організація зі стандартизації/Міжнародна електротехнічна комісія) встановлює загальні поняття та принципи інформаційної безпеки та визначає загальну модель оцінки, яка використовуватиметься як основа для оцінки властивостей безпеки продуктів інформаційних технологій.

(4) Відповідно до мандату M/460 на стандартизацію, виданого Комісією, Європейський комітет зі стандартизації (CEN) розробив стандарти для засобів для створення кваліфікованих електронних підпису та печатки, де дані для створення електронного підпису або дані для створення електронної печатки зберігаються в середовищі, керованому повністю, але не обов'язково лише, користувачем. Ці стандарти вважаються доцільними для оцінки відповідності таких засобів належним вимогам, викладеним у додатку II Регламенту (ЄС) № 910/2014.

(5) У додатку II до Регламенту (ЄС) № 910/2014 встановлено, що лише кваліфікований постачальник довірчих послуг може управляти даними для створення електронного підпису від імені підписувача. Вимоги до безпеки та їх відповідні специфікації щодо сертифікації є різними для випадків, коли підписувач фізично володіє продуктом, та для випадків, коли кваліфікований постачальник довірчих послуг діє від імені підписувача. Для задоволення вимог обох ситуацій, а також для сприяння подальшому розвитку продуктів та стандартів оцінки, необхідних для конкретних потреб, у додатку до цього Рішення зазначаються стандарти, що охоплюють обидві ситуації.

(6) Після ухвалення цього Рішення Комісії декілька постачальників довірчих послуг вже пропонують рішення для управління даними для створення електронного підпису від імені своїх клієнтів. Сертифікація продуктів на цей момент обмежена апаратними модулями безпеки, які

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

ІМПЛЕМЕНТАЦІЙНЕ РІШЕННЯ КОМІСІЇ (ЄС) 2016/650

від 25 квітня 2016 року

щодо стандартів оцінки безпеки засобів для створення кваліфікованих підпису та печатки відповідно до статей 30(3) та 39(2) 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 статті 30(3) та 39(2),

Оскільки:

(1) У додатку II до Регламенту (ЄС) № 910/2014 встановлено вимоги до засобів для створення кваліфікованого електронного підпису та засобів для створення кваліфікованої електронної печатки.

(2) Завдання складання технічних специфікацій, необхідних для виробництва та введення в обіг продуктів, беручи до уваги поточний стан технологій, виконується організаціями, компетентними в сфері стандартизації.

(3) ISO/IEC (Міжнародна організація зі стандартизації/Міжнародна електротехнічна комісія) встановлює загальні поняття та принципи інформаційної безпеки та визначає загальну модель оцінки, яка використовуватиметься як основа для оцінки властивостей безпеки продуктів інформаційних технологій.

(4) Відповідно до мандату M/460 на стандартизацію, виданого Комісією, Європейський комітет зі стандартизації (CEN) розробив стандарти для засобів для створення кваліфікованих електронних підпису та печатки, де дані для створення електронного підпису або дані для створення електронної печатки зберігаються в середовищі, керованому повністю, але не обов'язково лише, користувачем. Ці стандарти вважаються доцільними для оцінки відповідності таких засобів належним вимогам, викладеним у додатку II Регламенту (ЄС) № 910/2014.

(5) У додатку II до Регламенту (ЄС) № 910/2014 встановлено, що лише кваліфікований постачальник довірчих послуг може управляти даними для створення електронного підпису від імені підписувача. Вимоги до безпеки та їх відповідні специфікації щодо сертифікації є різними для випадків, коли підписувач фізично володіє продуктом, та для випадків, коли кваліфікований постачальник довірчих послуг діє від імені підписувача. Для задоволення вимог обох ситуацій, а також для сприяння подальшому розвитку продуктів та стандартів оцінки, необхідних для конкретних потреб, у додатку до цього Рішення зазначаються стандарти, що охоплюють обидві ситуації.

(6) Після ухвалення цього Рішення Комісії декілька постачальників довірчих послуг вже пропонують рішення для управління даними для створення електронного підпису від імені своїх клієнтів. Сертифікація продуктів на цей момент обмежена апаратними модулями безпеки, які сертифіковані відповідно до різних стандартів, але ще не сертифіковані згідно з вимогами до засобів для створення кваліфікованих підпису та печатки. Однак поки відсутні опубліковані

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

стандарти, такі як EN 419 211 (застосовувані до електронного підпису, створеного в середовищі, керованому повністю, але не обов'язково лише, користувачем) для рівною мірою важливого ринку сертифікованих продуктів віддаленого доступу. Оскільки стандарти, які можуть підходити для цих цілей, перебувають на стадії розробки, то Комісія доповнить це Рішення після того, як ці стандарти стануть доступні та будуть оцінені як такі, що відповідають вимогам, викладеним у додатку II до Регламенту (ЄС) № 910/2014. До того моменту, коли буде встановлено список таких стандартів, може використовуватися альтернативний процес для оцінки відповідності таких продуктів на умовах, передбачених у пункті (b) статті 30(3) Регламенту (ЄС) № 910/2014.

(7) У додатку наведено стандарт EN 419 211, який складається з різних частин (від 1 до 6), що охоплюють різні ситуації. Частина 5 EN 419 211 та частина 6 EN 419 211 містять розширення, що стосуються середовища засобу для створення кваліфікованого підпису, як, наприклад, зв'язок з надійними програмами створення підпису. Виробники продуктів вільно застосовують такі розширення. Відповідно до пункту 56 преамбули Регламенту (ЄС) № 910/2014 сфера сертифікації згідно зі статтями 30 та 39 зазначеного Регламенту обмежена до захисту даних для створення підпису, а програми створення підпису виключені зі сфери сертифікації.

(8) Для того, щоб забезпечити, що електронні підписи та печатки, генеровані засобами для створення кваліфікованих підпису та печатки, надійно захищені від підробки відповідно до вимог додатка II до Регламенту (ЄС) № 910/2014, відповідні криптографічні алгоритми, довжини ключів та функції гешування є необхідними умовами для забезпечення безпеки сертифікованих продуктів. Оскільки це питання не було гармонізовано на європейському рівні, держави-члени повинні співпрацювати для узгодження криптографічних алгоритмів, довжин ключів та функцій гешування, які повинні використовуватись у сфері електронних підписів та печаток.

(9) У зв'язку з ухваленням цього Рішення, Рішення Комісії 2003/511/ЄС ([2]) втрачає актуальність. Тому його необхідно скасувати.

(10) Заходи, передбачені цим Рішенням, відповідають висновку Комітету, визначеного у статті 48 Регламенту (ЄС) № 910/2014,

УХВАЛИЛА ЦЕ РІШЕННЯ:

Стаття 1

1. Стандарти для оцінки безпеки продуктів інформаційних технологій, які застосовуються до сертифікації засобів для створення кваліфікованого електронного підпису або засобів для створення кваліфікованої електронної печатки відповідно до пункту (a) статті 30(3) або 39(2) Регламенту (ЄС) № 910/2014, де дані для створення електронного підпису та дані для створення електронної печатки, зберігаються в середовищі, керованому повністю, але не обов'язково лише, користувачем, зазначено в додатку до цього Рішення.

2. До встановлення Комісією списку стандартів для оцінки безпеки продуктів інформаційних технологій, які застосовуються до сертифікації засобів для створення кваліфікованого електронного підпису або засобів для створення кваліфікованої електронної печатки, де кваліфікований постачальник довірчих послуг управляє даними для створення електронного підпису або даними для створення електронної печатки від імені підписувача або розробника печатки, основою для сертифікації таких продуктів є процес, у межах якого відповідно до статті 30(3)(b) використовуються рівні безпеки, аналогічні рівням, передбаченим у статті 30(3)(a), про що Комісії повідомляє публічний або приватний орган, зазначений у параграфі 1 статті 30 Регламенту (ЄС) № 910/2014.

([2]) Рішення Комісії 2003/511/ЄС від 14 липня 2003 року про публікацію реєстраційних номерів загальновизнаних стандартів для продуктів з електронним підписом відповідно до Директиви Європейського Парламенту і Ради 1999/93/ЄС (OB L 175, 15.07.2003, с. 45).

Стаття 2

Рішення 2003/511/ЄС скасувати.

Стаття 3

Це Рішення набуває чинності на двадцятий день після його публікації в *Офіційному віснику Європейського Союзу*.

Вчинено у Брюсселі 25 квітня 2016 року.

За Комісію

Президент

Jean-Claude JUNCKER

ДОДАТОК

СПИСОК СТАНДАРТІВ, ЗАЗНАЧЕНИХ У СТАТТІ 1(1)

— ISO/IEC 15408 — Інформаційні технології — Методи забезпечення безпеки — Критерії оцінки безпеки інформаційних технологій, частини 1–3, як зазначено нижче:

  — ISO/IEC 15408-1:2009 — Інформаційні технології — Методи забезпечення безпеки — Критерії оцінки безпеки інформаційних технологій — Частина 1. ISO, 2009.

  — ISO/IEC 15408-2:2008 — Інформаційні технології — Методи забезпечення безпеки — Критерії оцінки безпеки інформаційних технологій — Частина 2. ISO, 2008.

  — ISO/IEC 15408-3:2008 — Інформаційні технології — Методи забезпечення безпеки — Критерії оцінки безпеки інформаційних технологій — Частина 3. ISO, 2008.

та

— ISO/IEC 18045:2008: Інформаційні технології — Методи забезпечення безпеки — Методика оцінки безпеки інформаційних технологій,

та

— EN 419 211 — Профілі захисту для засобу для створення захищеного підпису, частини 1–6 — у відповідних випадках — як зазначено нижче:

  — EN 419211-1:2014 — Профілі захисту для засобу для створення захищеного підпису — Частина 1: Огляд

  — EN 419211-2:2013 — Профілі захисту для засобу для створення захищеного підпису — Частина 2: Засіб з генерацією ключів

  — EN 419211-3:2013 — Профілі захисту для засобу для створення захищеного підпису — Частина 3: Засіб з імпортуванням ключів

  — EN 419211-4:2013 — Профілі захисту для засобу для створення захищеного підпису — Частина 4: Розширення для засобу з генерацією ключів і надійним каналом зв’язку з програмою генерації сертифікатів

  — EN 419211-5:2013 — Профілі захисту для засобу для створення захищеного підпису — Частина 5: Розширення для засобу з генерацією ключів і надійним каналом зв’язку з програмою створення підписів

  — EN 419211-6:2014 — Профілі захисту для засобу для створення захищеного підпису — Частина 6: Розширення для засобу з імпортуванням ключів і надійним каналом зв’язку з програмою створення підписів