ЗАТВЕРДЖЕНО
рішенням Правління
АТ «МетаБанк»
від 20.02.2020 року
Реєстраційний № 722

ПОРЯДОК
виявлення змін в електронному документі та змін електронного підпису після підписання електронного документа

м. Запоріжжя
2020

Зміст

1. Загальна частина

Цей Порядок регламентує загальні процедури та дії працівників АТ «МетаБанк» під час виконання перевірок електронних документів на предмет виявлення будь-яких можливих змін після накладання електронного підпису та дії під час виконання перевірок на предмет виявлення будь-яких можливих змін в електронних підписах після підписання електронних документів в АТ «МетаБанк».

Порядок розроблено з урахуванням вимог Законів України «Про електронні довірчі послуги», «Про електронні документи та електронний документообіг», Положення про застосування електронного підпису та електронної печатки в банківській системі України, затвердженого Постановою Правління НБУ №78 від 14.08.2017р. (в редакції постанови Правління НБУ №42 від 25.02.2019р.), інших нормативних документів Національного банку України.

Цей Порядок Правлінням Банку. Банк забезпечує безперешкодний доступ до Порядку своїх клієнтів та інших фізичних і юридичних осіб. шляхом розміщення на Веб-сайті Банку.

2. Ціль документа

Ціль Порядку – встановлення порядку дій при роботі з електронним документом, зокрема в частині виявлення будь-яких змін в електронному документі та будь-яких змін електронного підпису після підписання електронного документа з метою забезпечення належного рівня безпеки інформації та дотримання Банком вимог чинного законодавства України при роботі з іншими суб'єктами електронної взаємодії.

3. Терміни та скорочення

В Порядку використовуються наступні терміни та визначення:

Банк – Акціонерне товариство «МетаБанк»;

Електронні дані – будь-яка інформація в електронній формі;

Електронний документ (ЕД) – документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа (стаття 5 розділ II Закону України «Про електронні документи та електронний документообіг»;

Електронний підпис (ЕП) – електронні дані, які додаються підписувачем до інших електронних даних або логічно з ними пов'язуються і використовуються ним як підпис;

Кваліфікований надавач електронних довірчих послуг – юридична особа незалежно від організаційно-правової форми та форми власності, фізична особа-підприємець, яка надає одну або більше електронних довірчих послуг, діяльність якої відповідає вимогам Закону «Про електронні довірчі послуги» та відомості про яку внесені до Довірчого списку;

Довірчий список – перелік кваліфікованих надавачів електронних довірчих послуг та інформації про послуги, що ними надаються (визначений на сайті Центрального засвідчувального органу Міністерства юстиції України - https://czo.gov.ua/trustedlist);

КЕП Банку – кваліфікована електронна печатка Банку;

НБУ – Національний Банк України;

Підписувач (автор документу) – особа, яка здійснює накладання електронного підпису на електронний документ;

Принцип – при характеристиці різноманітних систем принципи відображають ті суттєві характеристики, що відповідають за правильне функціонування системи, без яких вона не виконувала б свого призначення;

Програмне забезпечення (ПЗ) – сукупність програм системи обробки інформації і програмних документів необхідних для експлуатації цих програм;

Система Автоматизації Банку (САБ) – програмне забезпечення, що обслуговує поточну внутрішньобанківську діяльність (бухгалтерський облік, обслуговування рахунків клієнтів тощо);

СЕД – автоматизована система документообігу та управління бізнес-процесами, розробник АТ «МетаБанк»;

УЕП Банку – удосконалена електронна печатка Банку;

ЦСК АТ «МЕТАБАНК» – «Центр сертифікації ключів», розробник ТОВ «Сайфер»;

Адресат – юридична або фізична особа, на адресу якої направляється електронний або паперовий документ.

4. Сфера застосування

Порядок розповсюджується на всіх працівників Банку, які згідно з своїми посадовими обов‘язками працюють з електронним документом, електронним підписом, кваліфікованою електронною печаткою та удосконаленою електронною печаткою, а саме:
– оброблюють електронні документи, які отримано від контрагентів Банку з використанням кваліфікованого електронного підпису, удосконаленого електронного підпису чи електронного підпису Національного банку України;
– використовують в своїй роботі кваліфіковані та/або удосконалені електронні печатки Банку.

5. Опис принципів використання кваліфікованого електронного підпису.

5.1. Види електронного підпису

Використовуючи більш спрощені визначення, не беручі до уваги формальні визначення, види електронних підписів для накладання на електронні документи визначаються наступним чином:
1. Електронний підпис – це будь-яка електронна форма даних, що використовується підписувачем як підпис.
2. Удосконалений електронний підпис – це підпис, сформований з використанням засобів криптографії, але при цьому не обов'язково з використанням сертифіката, а якщо й з використанням, то не обов'язково, щоб сертифікат був кваліфікованим.
3. Кваліфікований електронний підпис – заснований на криптографії відкритий ключ, підтверджений сертифікатом, і сам сертифікат є кваліфікованим. Кваліфікований ЕП накладається з використанням особистого ключа, отриманого виключно у кваліфікованих надавачів електронних довірчих послуг.

Крім електронного підпису Закон України «Про електронні довірчі послуги» запроваджує поняття й електронної печатки. Електронна печатка також може бути удосконаленою та кваліфікованою – критерії видів цих електронних печаток аналогічні відповідним критеріям видів електронних підписів. Відмінність полягає в тому, що електронним підписом може користуватися як юридична, так і фізична особа, а електронною печаткою – тільки юридична особа та фізична особа-підприємець. У функціональному ж змісті суттєвої різниці між електронним підписом і електронною печаткою немає.

5.2. Забезпечення цілісності та автентичності

Застосування кваліфікованого ЕП при електронній взаємодії дозволяє здійснити:
1) Контроль цілісності переданого ЕД – при будь-якій випадковій або навмисній зміні ЕД електронний підпис стане недійсним, тому що він обчислений на підставі вихідного стану початкового ЕД і відповідає лише йому;
2) Захист від змін (підроблення) ЕД – гарантія виявлення підробки при контролі цілісності робить підроблення недоцільним у більшості випадків;
3) Неможливість відмовитись від авторства – створення коректного кваліфікованого ЕП можливе виключно з використанням особистого ключа, а він повинен бути відомим виключно власнику особистого ключа (підписувачу). Відповідно підписувач не може відмовитись від свого ЕП під ЕД;
Електронний підпис є певною послідовністю символів, отриманих в результаті певного перетворення початкового ЕД за допомогою спеціального ПЗ. Будь-яка зміна вихідного ЕД робить ЕП недійсним, а на практиці він є унікальним для кожного ЕД і не може бути перенесений на інший ЕД.

5.3. Забезпечення надійності кваліфікованого електронного підпису

Забезпечення надійності кваліфікованого ЕП здійснюється залученням до процесу отримання особистих ключів, накладання кваліфікованого ЕП та перевірки його дійсності кваліфікованих надавачів електронних довірчих послуг.

Особлива увага приділяється термінам «особистий ключ» та «сертифікат». Криптографічний захист електронних підписів заснований, як правило, на шифруванні, яке передбачає використання пари «відкритий ключ – особистий ключ». Відкритий ключ доступний для кореспондентів і для підписувача, а особистий ключ має перебувати тільки у підписувача (ця асиметрія між ключами лежить в основі терміну «асиметричне криптографічне

перетворення»). При цьому пара цих ключів створюється таким чином, що присвоїти електронному документу електронний підпис можна тільки за допомогою особистого ключа, але перевірити підпис можна за допомогою відкритого ключа, що відповідає особистому ключу. Кореспондент, отримавши документ з удосконаленим ЕП, може у загальному випадку покладатися на те, що це присвоєння було зроблено власником особистого ключа. Крім того, під час створення підпису відбувається співвіднесення даних про документ і даних, що містяться в самому підписі, таким чином, що якщо після підписання змінити в документі що-небудь, то він перестане відповідати підпису й кореспондент має змогу це виявити.

Для мінімізації такого ризику регламентом щодо забезпечення надійності ЕП введено ще один елемент: третя сторона, яка перевіряє особу підписувача й, упевнившись, що дані відкритого ключа відповідають особистим даним підписувача, видає «сертифікат» – спеціальний набір даних, асоційований із відкритим ключем, що засвідчується Кваліфікованим надавачем електронних довірчих послуг. В цьому разі кореспондент, одержавши підписаний електронний документ, який пов'язаний не тільки з відкритим ключем, а й з сертифікатом, може покладатися на те, що особа, яка застосувала кваліфікований електронний підпис, є тим, чий є цей електронний підпис. При цьому якщо згадана третя сторона - засвідчувач внесена до спеціального Довірчого списку, то сертифікат, що видається нею, є кваліфікованим сертифікатом, і сама вона має статус кваліфікованого надавача електронних довірчих послуг. Законом України «Про електронні довірчі послуги» передбачена обов'язкова ідентифікація, якщо відповідна послуга є кваліфікованою.

5.4. Принцип створення електронного документа з накладанням кваліфікованого електронного підпису

При підписанні ЕД його початковий зміст не змінюється, а додається блок даних, так званий «Електронний підпис». Отримання цього блоку розподіляється на два етапи:
1) На першому етапі за допомогою програмного забезпечення і спеціальної математичної функції обчислюється так званий «відбиток документу». Цей відбиток має такі властивості:
– фіксовану довжину, незалежно від довжини документу;
– унікальність відбитку для кожного документу;
– неможливість відновлення документу за його відбитком.

Таким чином, якщо ЕД був модифікований, то зміниться і його відбиток, що відобразиться при перевірці накладеного кваліфікованого ЕП (розділи 5.5, 7.2 Порядку).
2) На другому етапі відбиток електронного документа шифрується за допомогою програмного забезпечення і особистого ключа підписувача (автора). Розшифрувати кваліфікований ЕП і одержати початковий відбиток, який відповідатиме даному документу, можливо тільки використовуючи «сертифікат» відкритого ключа підписувача.

Таким чином, обчислення відбитку документу захищає його від модифікації сторонніми особами після підписання, а шифрування особистим ключем підписувача підтверджує авторство електронного документа.

5.5. Принцип перевірки кваліфікованого електронного підпису створеного електронного документа

Перевірка кваліфікованого ЕП створеного ЕД в результаті виконання процедури підписання ЕД проводиться за наступними етапами:
1) На першому етапі адресат за допомогою спеціалізованого програмного забезпечення «сертифікатом» відкритого ключа підписувача розшифровує підписаний відбиток документу і одержує відбиток початкового документа (оригінального ЕД, на який підписувач власноручно з використанням особистого ключа наклав кваліфікований ЕП);
2) За допомогою спеціального програмного забезпечення і спеціальної математичної функції з документа, який був одержаний (електронний документ з накладеним кваліфікованим ЕП), обчислюється його відбиток;
3) При перевірці кваліфікованого ЕП порівнюються відбитки початкового і одержаного електронних документів. Результат виконання такої перевірки може бути лише одна з відповідей: «вірний» чи «невірний».
Для повноцінного функціонування системи електронної взаємодії, у т.ч. перевірки належності відкритого ключа відповідному підписувачу, Банк використовує спеціальні захищені довідники

сертифікатів відкритих ключів, які ведуться кваліфікованими надавачами електронних довірчих послуг, як то АЦСК Органів Юстиції України, АЦСК «Україна», АЦСК ІДД ДФС, АЦСК ПАТ «НДУ», тощо.

Перевірка актуальності накладеного на ЕД кваліфікованого ЕП та правильність проставлених параметрів часової мітки здійснюється з використанням спеціалізованого програмного забезпечення та/або он-лайн сервісу одного із кваліфікованих надавачів електронних довірчих послуг (наприклад, інтернет-сторінка АЦСК Органів Юстиції України - https://ca.informjust.ua/verify).

6. Порядок виявлення будь-яких змін в електронному документі

Перевірка цілісності електронного документа проводиться шляхом перевірки електронного підпису підписувача.

Процес виявлення наявності будь-яких змін в ЕД у разі необхідності здійснюється Банком з використанням спеціального програмного забезпечення, в якому є відповідні «інструменти» для виконання такої перевірки. Процедури використання таких «інструментів» визначаються розробником програмного забезпечення.

За допомогою «інструментів» виконується перевірка ЕП (в друкованій копії ЕД це поле може мати назву «штамп», «сертифікат» чи відображатись як інша унікальна послідовність символів), що має наступні особливості:

– ЕП має фіксовану довжину незалежно від обсягу інформації в ЕД. Довжина підпису визначається розробником програмного забезпечення;

– унікальність ЕП для кожного ЕД всередині всієї інформаційної системи електронної взаємодії. ЕП нерозривно пов‘язаний з конкретним документом і тільки з ним;

– неможливість відновлення секретного ключа чи інших таємних компонентів по ЕП на ЕД.

Накладений ЕП дозволяє здійснити контроль цілісності кожного ЕД, оскільки при будь-якій випадковій або навмисній зміні електронного документа ЕП стане недійсним, тому що він (електронний підпис) обчислений на підставі вихідного стану документа і відповідає лише йому.

Відповідно, якщо ЕД був модифікований, то перевірка цілісності цього ЕД виявить невідповідність накладеному ЕП, що буде свідчить про негативний результат – відповідь «невірний» (пункт 3 розділу 5.5. Порядку). Такий ЕД буде вважатися не дійсним. Позитивний результат перевірки цілісності ЕД – відповідь «вірний» (пункт 3 розділу 5.5. Порядку) буде підтвердженням відсутності будь-яких змін у створеному і підписаному(за допомогою електронного підпису) електронному документі.

7. Порядок виявлення будь-яких змін ЕП після підписання ЕД

7.1 Принципи виявлення будь-яких змін ЕП після підписання ЕД

Оскільки ЕП є якоюсь послідовністю символів, які отримані в результаті певного перетворення початкового документа (або будь-якої іншої інформації в електронному вигляді) за допомогою спеціального програмного забезпечення, то будь-яка зміна вихідного документа робить ЕП недійсним, а на практиці він є унікальним для кожного ЕД і не може бути перенесений на інший ЕД. Неможливість підробки ЕП забезпечується дуже великим обсягом математичних обчислень, необхідних для його підбору. Таким чином, при отримані документу, підписаного ЕП, одержувач може бути впевненим у авторстві і незмінності змісту даного документа.

Особистий ключ є найбільш вразливим компонентом всієї криптосистеми ЕП. Шахрай, який може заволодіти особистим ключем підписувача, може створити дійсний цифровий підпис будь-якого ЕД від імені цього підписувача, але при умові що знатиме пароль доступу до особистого ключа. Тому в Банку особлива увага приділяється засобам зберігання особистих ключів – всі особисті ключі які використовуються Банком, зберігаються на захищених носіях ключової інформації, а паролі доступу до особистих ключів відомі виключно власникам таких ключів.

7.2 Порядок виявлення будь-яких змін електронного підпису після підписання електронного документа з використанням сертифікату відкритого ключа підписувала

У Банку при роботі з електронними документами, на які накладено кваліфікований електронний підпис, встановлений наступний порядок виявлення будь-яких змін ЕП після підписання ЕД:

1) При роботі з ЕД, якими обмінюються через інформаційну систему «Мій електронний документ» (ІС «M.E.Doc») відповідальні працівники Банку, за допомогою штатних «інструментів» у ІС «M.E.Doc» перевіряють, чи дійсно ЕП відповідає документу та відкритому ключу, зазначеному у сертифікаті. За наявності будь-яких змін в ЕП результати перевірки вважаються негативними і такий ЕД визначається Банком не дійсним. Позитивний результат підтверджує цілісність ЕП;

2) При роботі з ЕД, якими обмінюються із використанням звичайного файлообміну відповідальні працівники Банку, за допомогою штатних «інструментів» офіційного Інтернет-ресурсу «АЦСК Органів Юстиції України» https://ca.informjust.ua/verify або спеціалізованого ПЗ «Користувач АЦСК ІДД ДФС», наданого АЦСК ІДД ДФС, перевіряється, чи дійсно ЕП відповідає документу та відкритому ключу, зазначеному у сертифікаті. За наявності будь-яких змін в ЕП результати перевірки вважаються негативними і такий ЕД визначається Банком не дійсним. Позитивний результат підтверджує цілісність ЕП;

4) При роботі з ЕД в системі дистанційного банківського обслуговування «Клієнт-Банк» достовірність електронного підпису перевіряється штатними «інструментами» в автоматичному режимі. При цьому перевірка відповідності ЕП відкритому ключу здійснюється з використанням довідника сертифікатів відкритих ключів серверу ЦСК Банку.

7.3 Порядок виявлення будь-яких змін ЕП після підписання ЕД без використання сертифікату відкритого ключа підписувача

Банк за допомогою «інструментів» у спеціалізованому програмному забезпеченні здійснює перевірку простого ЕП підписувача в автоматичному режимі згідно з процедурою, передбаченою в договорі між Банком і підписувачем. За результатами перевірки підтверджується відповідність простого ЕП певному ЕД.

За допомогою програмно-технічних комплексів, в яких здійснюється створення, обробка та зберігання ЕД клієнтів Банку, Банк забезпечує цілісність, достовірність та авторство електронного документа, на який накладено простий ЕП, що забезпечує однозначну ідентифікацію особи підписувача. У разі необхідності за допомогою «інструментів» у спеціалізованому програмному забезпеченні в будь-який час виконується перевірка відповідності простого ЕП конкретному ЕД з визначенням дати та часу накладання простого ЕП та ідентифікації особи підписувача.

Вся службова інформація (електронні дані в базах даних, лог-файли, протоколи, тощо), що стосується створення, оброблення і зберігання таких ЕД надійно захищена від модифікації та доступність до неї регламентується вимогами Системи управління інформаційною безпекою Банку.

8. Ролі та відповідальності

Всі працівники Банку, які обробляють ЕД з накладеними ЕП для виконання своїх посадових обов‘язків, повинні дотримуватись процедур даного Порядку, інших внутрішніх нормативних документів Банку та чинного законодавства України і несуть особисту відповідальність за їх порушення.

Працівники Управління інформаційної безпеки відповідають за виконання належного контролю за дотриманням працівниками Банку вимог даного Порядку для забезпечення своєчасного виявлення недоліків чи слабких місць та їх швидке усунення.

Керівники Банку здійснюють всебічну підтримку для забезпечення стабільного та безвідмовного функціонування інформаційних систем, в яких виконується робота з ЕД, для забезпечення необхідного рівня конфіденційності та інформаційної безпеки відповідно до вимог Системи управління інформаційною безпекою Банку.

9. Перегляд документу

Цей Порядок переглядається за необхідністю. Причинами внесення змін до Порядку є зміни в інформаційній інфраструктурі та/або впровадженні нових інформаційних технологій, а також зміни в законодавчих, регуляторних та інших нормах, що стосуються застосування ЕП та обігу ЕД.

10. Історія змін

Дата	Автор	Зміст змін
09.01.2020	Начальник Управління інформаційної безпеки Курінной О.Д.	Початкова редакція