

ВИТЯГ

з Положення про криптографічний захист інформації в АТ «ТАСКОМБАНК»

8. ВИЯВЛЕННЯ БУДЬ-ЯКИХ ЗМІН В ЕЛЕКТРОННОМУ ДОКУМЕНТІ, В ЕЛЕКТРОННІЙ КОПІЇ З ПАПЕРОВОГО ДОКУМЕНТА ТА ЗМІН ЕЛЕКТРОННОГО ПІДПISУ/ПЕЧАТКИ ПІСЛЯ ПІДПISАННЯ

8.1. Для виявлення змін в ЕД, в електронній копії з паперового документа та змін ЕП/ЦВП після підписання електронного документа проводиться перевірка цілісності електронного документа та ЕП/Печатки/ЦВП.

8.2. Перевірка цілісності ЕД чи електронних копій з паперового документа підписаних КЕП/УЕП/Печаткою виконується за допомогою ПЗ, WEB ресурсів, ПЗ що використовує криптобібліотеки що мають експертний висновок ДССЗЗІУ.

8.3. Для перевірки цілісності ЕД чи електронних копій з паперового документа підписаних КЕП/УЕП/Печаткою також можна використовувати Державні онлайн ресурси, ПЗ, яке використовує крипто-бібліотеки, що мають експертний висновок ДССЗЗІУ.

8.4. Для уніфікації процесу перевірки КЕП на електронному документі, перевірки цілісності документу, наявності всіх необхідних реквізитів та властивостей підписаного документа, працівник Банку повинен скористатися, наприклад, WEB-ресурсом Центрального засвідчувального органу Міністерства цифрової трансформації України (далі – ЦЗО): <https://czo.gov.ua/verify>.

8.5. Під час перевірки документу у WEB-ресурсі ЦЗО працівник Банку встановлює, що документ підписаний, цілісний, підписаний кваліфікованим ЕП і є можливість вивантажити протокол перевірки.

8.5.1. В протоколі перевірки має обов'язково значитися інформація:

- Дата та час перевірки;
- Назва файлу з підписом;
- Розмір файлу з підписом;
- Назва файлу без підпису;
- Розмір файлу без підпису;
- Результат перевірки підпису: «Файл успішно перевірено. Усі дані цілі»;
- П.І.Б. підписувача.

8.5.2. Якщо підписувач (контрагент Банку) діє від імені юридичної особи, протокол перевірки має додатково містити:

- РНОКПП і назву юридичної особи
- Код ЄДРПОУ юридичної особи;
- Час підпису (має бути підтверджено кваліфікованою позначкою часу для підпису від Надавача);
- Тип носія на якому був КЕП/Печатка;
- Ким виданий кваліфікований сертифікат (назву КНЕДП де підписувач отримав КЕП/Печатку); Серійний номер сертифікату;
- Застосований алгоритм підпису (наприклад ДСТУ-4145);

- Тип підпису, наприклад кваліфікований або удосконалений;
- Тип контейнера, наприклад: підпис та дані в одному файлі (CAAdES enveloped);
- Формат підпису: З повними даними ЦСК для перевірки (CAAdES-X Long);
- Тип Сертифікату, наприклад «Кваліфікований».

8.6. Здійснивши перевірку працівник повинен вивантажити протокол перевірки підпису і долучити його до загального пакету документів по тій угоді (правочину) в рамках якої відбулося підписання електронних документів сторонами угоди. Наявність такого протоколу в загальному пакеті документів є свідченням того що перевірка документу проведена.

8.7. Якщо електронний документ підписується не фізичною особою, а представником/працівником юридичної особи, працівник Банку повинен з'ясувати, чи вповноважений підписувач діяти від імені юридичної особи, про що запросити від підписувача Довіреність на право підписувати угоди. Таким чином Банк уникає ризику укладання угод і операцій за цими угодами підписаних посадовими особами які мали в користуванні КЕП/Печатку юридичної особи, але не мали повноважень підписувати угоди на співпрацю з Банком.

8.8. Перевірка цілісності електронних документів підписаних ЦВП, простим ЕП, удосконаленим ЕП, кваліфікованим ЕП, Печаткою забезпечується засобами інформаційної системи, у якій здійснюється створення, оброблення, зберігання електронних документів.