

*І.С. Кудрявцев, А.О. Оріхон
(Національний авіаційний університет, Україна)*

Оптимізація авіаційного документообігу через буферизацію електронних підписів в умовах нестабільного зв'язку

У статті розглядається проблема використання електронних підписів в авіаційній галузі за умов нестабільного або відсутнього інтернет-з'єднання. Впровадження електронного підпису є критично важливим для забезпечення швидкого, безпечного та ефективного документообігу, однак специфіка авіаційної діяльності часто обмежує можливості таких систем. Запропоноване рішення – система буферизації електронних підписів, яка дозволяє підписувати документи офлайн з подальшою синхронізацією при доступі до мережі, що забезпечує цілісність, юридичну силу підписів та безперервність робочих процесів.

Вступ. У сучасних умовах стрімкого розвитку цифрових технологій, які проникають у всі аспекти життя, авіаційна галузь стикається з новими викликами в області електронного документообігу. Електронні підписи сприяють швидкому, безпечному та ефективному обміну документами, проте робота в умовах обмеженого або нестабільного інтернет-з'єднання створює серйозні перешкоди для традиційних систем підписання. В епоху цифрової трансформації зростає потреба в новаторських рішеннях, які забезпечували б надійну і безпечну роботу з документами навіть при нестабільному зв'язку. У цій роботі пропонується впровадження системи буферизації підписів, що дозволить авіаційній індустрії ефективно долати ці труднощі та покращувати свої операційні процеси.

Розглянемо основні виклики, з якими стикається авіаційна галузь у сфері електронного підписання. Перша проблема — це нестабільне інтернет-з'єднання в різних умовах авіаційної діяльності. Літаки перетинають різноманітні географічні зони, такі як океани, пустелі, гірські райони, де якість інтернет-зв'язку може варіюватися від високої до повністю відсутньої. Друга — необхідність забезпечення безперервності робочих процесів. В авіації кожна хвилина має значення, і затримки через неможливість підписати важливі документи можуть призвести до серйозних фінансових втрат та підвищення ризиків для безпеки. Третя — це суворі вимоги до безпеки та автентичності електронних підписів, оскільки в авіаційній галузі кожен підпис є критичним, будь то затвердження плану польоту, підтвердження технічного обслуговування або внесення змін у розклад екіпажу.

Наявні традиційні системи електронного підпису, які вимагають постійного інтернет-з'єднання, виявляються неефективними в умовах нестабільного зв'язку. Водночас офлайн-системи не можуть забезпечити

миттєву синхронізацію, що може спричинити невідповідність даних і призвести до потенційних помилок у процесах. Варіант з рішенням наявної проблеми за допомогою системи буферизації підписів спирається на концепцію локального збереження даних із подальшою відкладеною синхронізацією.

Механізм роботи системи (рис.1) виглядає наступним чином: після підписання документа користувачем, на його пристрої формується локальна копія цього документа. На неї накладається електронний підпис, для чого використовуються криптографічні ключі, що зберігаються локально. Дані ключі генеруються і оновлюються за допомогою спеціальних алгоритмів, що гарантуватиме їх унікальність і захищеність, навіть при роботі в офлайн-режимі. Підписаний документ зберігається у локальному сховищі з використанням методів шифрування, що забезпечить конфіденційність та цілісність даних. Паралельно до цього формуватиметься запис у черзі синхронізації — це структура даних у вигляді черги, яка містить інформацію про всі підписані документи, що чекають синхронізації з центральним сервером. Елементи оброблятимуться в порядку їх додавання (FIFO - First In, First Out).

Ключовими компонентами системи буферизації є:

- Модуль локального збереження даних: Це компонент, що відповідатиме за створення записів на пристрої користувача і шифруватиме їх для захисту даних від несанкціонованого доступу.
- Модуль електронного підписання: Цей компонент відповідає за накладання електронного підпису на документ. Він використовує криптографічні алгоритми.
- Черга синхронізації: Це структура даних, яка керує процесом синхронізації. Вона забезпечує, що всі підписані документи будуть відправлені на сервер у правильному порядку, як тільки з'явиться стабільне інтернет-з'єднання.
- Модуль синхронізації з центральним сервером: Цей модуль відповідає за встановлення зв'язку з центральним сервером та передачу даних як тільки з'явиться стабільне інтернет-з'єднання.
- Центральний сервер: Даний елемент буде приймати дані від системи буферизації.
- Модуль валідації даних: Цей компонент забезпечуватиме перевірку документів, які передаються між системою буферизації та центральним сервером, на зміни або пошкодження під час передачі.

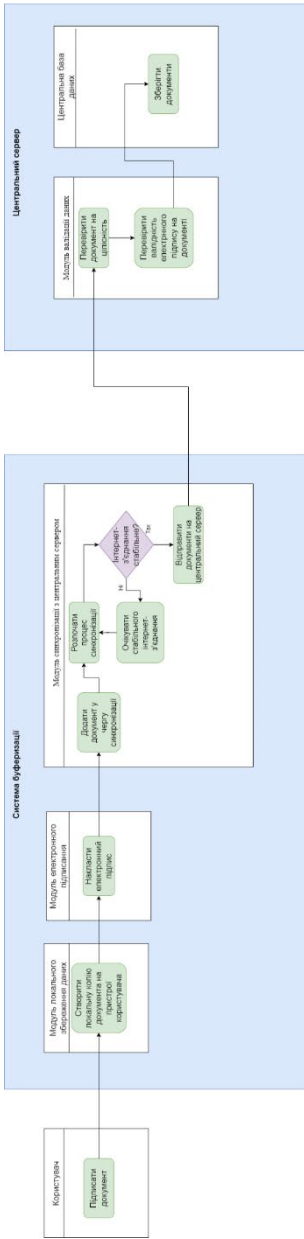


Рис. 1. Механізм роботи системи буферизації підписів

Процес синхронізації запускається автоматично при наявності стабільного інтернет-з'єднання. Після встановлення з'єднання, документи, що знаходяться у черзі синхронізації, передаються на центральний сервер у тому порядку, в якому вони були створені. Центральний сервер виконує низку перевірок: спочатку він верифікує цілісність документів, переконуючись, що під час передачі вони не зазнали змін. Далі здійснюється перевірка валідності електронних підписів за допомогою публічних ключів, пов'язаних з кожним користувачем. Ця перевірка включає як перевірку статусу сертифіката користувача, щоб гарантувати, що він не був відкликаний або термін його дії не закінчився. Після завершення всіх перевірок підтверджені документи зберігаються в центральній базі даних. Ця база є розподіленою системою з високим рівнем доступності, що гарантує надійне зберігання даних і забезпечує оперативний доступ до них незалежно від географічного розташування.

Механізм буферизації підписів дозволить забезпечити безперервність робочих процесів, що має ключове значення для авіаційної індустрії. Завдяки цьому пілоти та інженери зможуть виконувати свої завдання без очікувань на стабільне інтернет-з'єднання для підписання необхідних документів, що підвищить загальну ефективність операцій і мінімізує ризики помилок, спричинених роботою в умовах обмеженого часу.

Ця система суттєво підвищує рівень безпеки документообігу. Використання локальних методів шифрування та захищених сховищ значно знижує ймовірність несанкціонованого доступу до конфіденційної інформації. Механізм відкладеної синхронізації гарантує цілісність даних, забезпечуючи збереження кожного підписаного документа навіть у разі перебоїв зі зв'язком. Впровадження такої системи відкриває нові можливості для оптимізації внутрішніх процесів авіакомпаній. Наприклад, вона дозволяє швидко реагувати на зміни в розкладі польотів або технічних вимогах, навіть якщо літак перебуває в повітрі або в віддаленому аеропорту, що підвищує гнучкість операцій і здатність швидко адаптуватися до непередбачуваних ситуацій.

Проте, впровадження буферизації підписів має й свої виклики. Серед них — необхідність забезпечення сумісності з існуючими системами авіакомпаній, щоб інтеграція відбувалася плавно і не впливала на поточні робочі процеси. Крім того, важливим аспектом є навчання персоналу для ефективного використання нової системи. Ще один важливий виклик стосується правових аспектів. Необхідно гарантувати, що електронні підписи, створені в офлайн-режимі, будуть юридично рівноцінними традиційним підписам. Це потребує узгодження з міжнародними авіаційними регуляторами та, ймовірно, внесення змін до чинного законодавства.

Впровадження системи буферизації підписів має можливість суттєво вплинути на авіаційну галузь. Її потенціал полягає у підвищенні загальної ефективності операцій, зниженні затримок і супутніх витрат. Окрім того, посилена безпека і надійність документообігу сприятимуть зростанню довіри між учасниками авіаційного сектору. У перспективі така система може стати новим стандартом в авіації, підтримуючи подальшу цифровізацію та автоматизацію процесів. Це може призвести до виникнення нових бизнес-моделей і сервісів, заснованих на більш гнучкому та безпечному обміні даними.

Таким чином, система буферизації підписів не тільки вирішує поточні проблеми з електронними підписами в авіації, але й створює умови для інновацій і подальшого розвитку галузі в цілому.

Висновок. Запропонована система буферизації електронних підписів є ефективним інструментом для авіаційної галузі, яка стикається з проблемами через нестабільне інтернет-з'єднання. Вона дозволяє підтримувати безперервність робочих процесів, покращує безпеку документообігу та знижує ризики, пов'язані із затримками у підписанні критично важливих документів. Завдяки використанню локального шифрування та механізму відкладеної синхронізації система гарантує збереження цілісності та конфіденційності даних, що є важливим для авіаційних операцій. Впровадження таких рішень сприятиме цифровій трансформації галузі, підвищенню операційної ефективності, безпеки польотів і відкриттю нових можливостей для оптимізації бізнес-процесів. У перспективі ця система може стати галузевим стандартом, забезпечуючи надійний і гнучкий документообіг навіть в умовах складної інфраструктури.

Список літератури

1. Дуда Г. Електронний цифровий підпис: сутність, принципи дії та порядок отримання // Львів: ЛНУП, 2024. 579 с. – С. 209.
2. Кашапов А. А., Немкова О. А. Розроблення електронного цифрового підпису на основі динамічних шаблонів автентифікації // Науково-технічний журнал “Сучасний захист інформації. -2024. №. 2. - С. 59-68”
3. Рогачевський Д., Каплун В. Захист файлів з використанням електронно-цифрового підпису (ЕЦП) // ВНТУ, 2023.