КОМПАНІЯ CS

2FA

ДВОФАКТОРНА АУТЕНТИФІКАЦІЯ З ВИКОРИСТАННЯМ ЕЦП «CRYPTOLIBV3»

Двофакторна аутентифікація з використанням ЕЦП «CryptoLibV3»

Механізм двофакторної аутентифікації користувачів в АБС Б2 і JetB2 з використанням бібліотек **CryptolibV3** компанії «**Автор**» призначений для підвищення рівня безпеки входу в систему (АБС Б2 і JetB2) завдяки послідовному порівнянню двох факторів аутентифікації користувача:

- фактора знання логіна і пароля;
- фактора наявності у користувача токена компанії «Автор», а також знання пароля особистого ключа, який на ньому зберігається (за допомогою особистого ключа користувача накладається електронно-цифровий підпис (ЕЦП) на згенеровану випадкову послідовність, після чого підпис перевіряється на стороні сервера аутентифікації).

Відповідність

Протокол аутентифікації відповідає схемі №2 стандарту ДСТУ ISO/IEC 9798 3 2002 «Інформаційні технології. Методи захисту. Автентифікація суб'єктів. Частина 3. Механізми з Використання методу цифрового підпису».

Використання механізму забезпечує виконання умов вимог по аутентифікації, викладених в Постанові НБУ №95 від 28.09.2017 «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України».

Використання механізму дозволяє:

- Використовувати двофакторну аутентифікацію з використанням бібліотек CryptolibV3 компанії «Автор» окремо для кожного користувача;
- Здійснювати валідацію другого фактора аутентифікації користувача на сервері аутентифікації;
- Налаштовувати і зберігати параметри другого фактора аутентифікації користувача в базі даних (БД) сервера аутентифікації;
- Зберігати дані всіх запитів на аутентифікацію в БД сервера аутентифікації;
- Взаємодіяти з сервером аутентифікації:
  - Для клієнта АБС Б2 — через БД АБС Б2;
  - Для клієнта JetB2 — через сервер застосунків;
- Взаємодіяти з апаратними носіями (токенами) компанії «Автор» (SecureToken-337, SecureToken-338) за допомогою бібліотек CryptolibV3. CryptolibV3.