ПОРЯДОК ПРИМЕНЕНИЯ ТЕХНОЛОГИИ МОБИЛЬНОЙ ЭЦП

Мобильная ЭЦП – технология, которая позволяет использовать мобильный телефон в качестве средства ЭЦП, а также для идентификации пользователя в подсистеме «Интернет-клиент» СДБО «BS-Client».

Для подписания документов используются специальные зашифрованные сообщения – бинарные SMS, а совершение подписи, как и SIM-карта, защищено PIN-кодом.

В настоящее время в Республике Беларусь воспользоваться технологией мобильной ЭЦП могут абоненты мобильного оператора «Велком» при условии подключения услуги SIMiD.

Для подключения данной услуги абонент УП «Велком» должен обратиться в уполномоченный центр обслуживания клиентов для смены SIM на специализированную SIM с функцией ЭЦП, при этом телефонный номер сохраняется за абонентом.

Владелец SIM с подключенной услугой SIMiD может обратиться в любой регистрационный центр Государственной системы управления открытыми ключами, имеющий подключение к системе мобильной ЭЦП, для генерации ключей ЭЦП и выпуска сертификата открытого ключа (на платной основе).

ШАГ 1. Авторизация

Порядок использования сервера авторизации для идентификации и аутентификации пользователя приведен на Рис. 1.

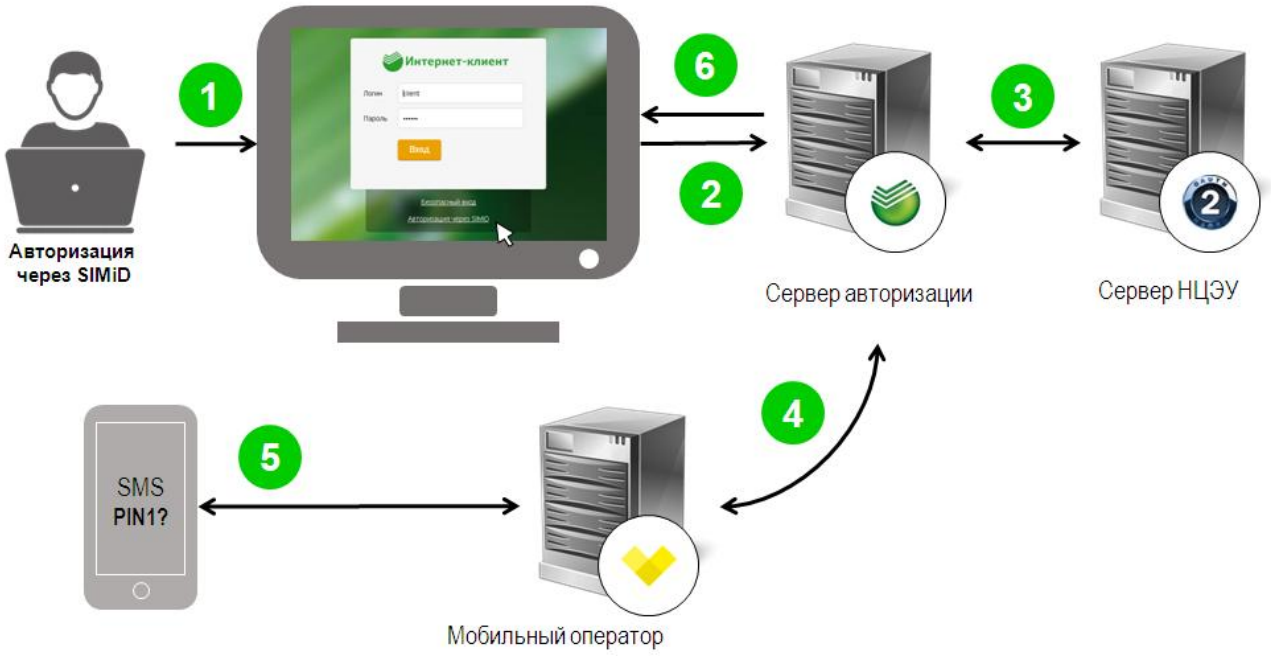

Рис. 1 – Идентификация и аутентификация пользователя

1. Пользователь, который является владельцем SIM с ЭЦП, заходит на сайт подсистемы «Интернет-клиент» и выполняет вход через пункт «Авторизация через SIMiD».
2. Банк перенаправляет пользователя на сервер авторизации с обращением к сервису идентификации и аутентификации сервера. Пользователь указывает серверу свой телефонный номер.
3. Сервер определяет сертификат, выпущенный на данный телефонный номер, и проверяет его статус.
4. Сервер выполняет протокол аутентификации пользователя путем обмена с SIM бинарными SMS.
5. Для подтверждения согласия на прохождение идентификации и аутентификации на сервере с последующей передачей своих идентификационных данных Банку владелец SIM вводит на телефоне PIN1.
6. Сервер возвращает Банку результат аутентификации пользователя и подлинные идентификационные данные пользователя: Ф.И.О., паспортные данные, сертификат открытого ключа ЭЦП и др. Пользователь выбирает свою организацию и выполняет вход на рабочее место подсистемы «Интернет-клиент».

ШАГ 2. Подписание электронного документа

Порядок использования сервера авторизации для выработки ЭЦП приведен на Рис. 2.

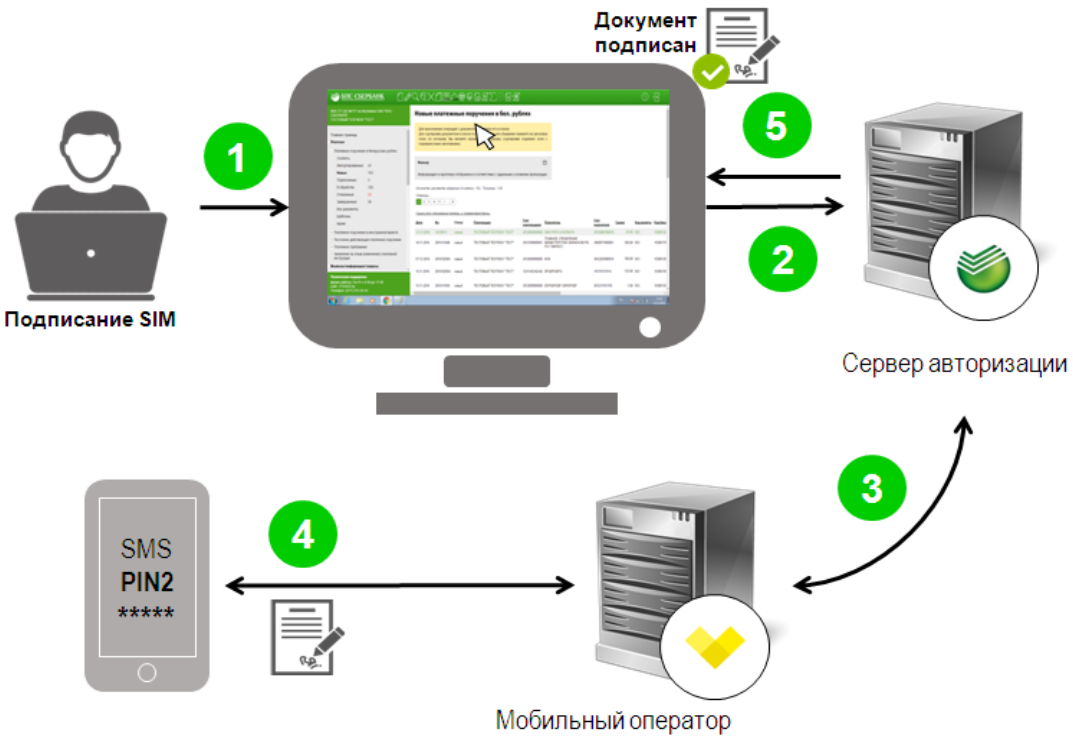

Рис. 2 – Подписание документа ЭЦП пользователя

1. Пользователь оформляет электронный документ в подсистеме «Интернет-клиент», выделяет его в списке и выбирает пункт «Подписать мобильной ЭЦП» или «Отправить/Подписать и отправить документ в банк».
2. Банк перенаправляет пользователя на сервер авторизации с обращением к сервису выработки ЭЦП в рамках защищенного соединения, установленного между сервером и SIM: передается хэш-значение документа.
3. Сервер выполняет протокол выработки ЭЦП пользователя путем отправки бинарной SMS с хэш-значением документа и получения бинарной SMS с выработанной ЭЦП.
4. Для подтверждения своего согласия на выработку ЭЦП владелец SIM вводит на телефоне PIN2.
5. Сервер формирует электронный документ согласно СТБ 34.101.23, проверяет его подлинность и возвращает системе ДБО сформированный подлинный электронный документ (документ в статусе «Подписан» или «Принят»).

   Таким образом, сервер авторизации во взаимодействии с SIM с функцией ЭЦП реализует сервис идентификации и аутентификации владельца SIM, а также сервис выработки ЭЦП с соблюдением требований Закона Республики Беларусь «Об электронном документе и электронной цифровой подписи».