USB-токен «MS_KEY K»

Устройство «MS_KEY_K» - средство криптографической защиты информации (СКЗИ), имеет **сертификат соответствия ФСБ** РФ № СФ/124-2673 по классам КС1 и КС2.

Устройство **USB-токен «MS_KEY_K»** предназначено для ***безопасной работы*** в системе ДБО ***Клиент-Банк*** *iBank2* с ***ключами электронной подписи***:

- *генерации*,

- *неизвлекаемого хранения ключей электронной подписи,*

- *выполнения функций подписи внутри устройства*.

Формирование ЭП в соответствии с ГОСТ Р34.10-2001 происходит непосредственно внутри USB-токена «MS_KEY_K». На вход токен принимает электронный документ, на выходе выдает ЭП под данным документом. Ключ ЭП генерируется самим «MS_KEY_K», хранится в защищенной памяти «MS_KEY_K». Никогда, никем и ни при каких условиях не может быть считан из «MS_KEY_K».

USB-токен «MS_KEY_K» позволяет хранить ключи ЭП ответственных сотрудников одного клиента или нескольких клиентов. В одном токене могут содержаться ключи ЭП ответственных сотрудников разных корпоративных клиентов, обслуживаемых в разных банках с системами Клиент-Банк iBank2. В каждом USB-токене может храниться 50 ключей электронной подписи.

Для обеспечения дополнительной защиты от несанкционированного доступа к ключам ЭП, хранящимся на USB-токене «MS_KEY_K», реализована возможность задавать PIN-код доступа к ключу. До момента ввода корректного PIN-кода отсутствует возможность действий с ключами.

Для работы в системе электронного банкинга iBank2 с USB-токенами «MS_KEY_K» необходим драйвер. Операционная система может содержать в своем составе драйвер и устройство будет доступно без отдельной установки драйвера на компьютере. Драйвер токена устанавливается до подключения устройства. Для установки нужный драйвер необходимо скачайте с портала iBank2.RU.

КБ «ОБР» (ООО) рекомендует своим **клиентам для безопасной работы** в системе **Клиент-Банк** iBank2 и **безопасного хранения ключей** электронной подписи **USB-токены «MS_KEY_K».**

Ориентировочная стоимость одного USB-токена «MS_KEY_K» на 17.10.2016г. 3000р.

По всем возникающим вопросам обращайтесь в отдел автоматизации по телефону (8352) 34-44-41

Краткая памятка по безопасности работы с USB-токеном «MS_KEY_K»

1. Не передавайте USB-токены третьим лицам! Не сообщайте третьим лицам пароли от ключей ЭП!

2. Подключайте USB-токен к компьютеру только на время работы с системой «iBank 2».

3. В случае утери (хищения) или повреждения USB-токена немедленно свяжитесь с Банком.

4. Не допускается непрерывное функционирование USB-токена более суток (24 часов).

5. Не разбирайте USB-токены, так как это ведет к потере гарантии!

6. Необходимо избегать скачков напряжения питания компьютера и USB-шины при подключенном USB-порте, а также не извлекать USB-токен из USB-порта во время записи и считывания.

7. В случае неисправности или неправильного функционирования USB-токенов обращайтесь в Банк.

8. Пароль на ключ, заданный при генерации секретного ключа, не должен состоять из одних цифр.

9. Пароль не должен быть слишком коротким и простым, быть легко запоминающимся.

10. Пароль должен содержать как заглавные, так и строчные буквы, цифры и знаки препинания.

11. Пароль не должен быть значимым словом (имя, дата рождения, девичья фамилия жены и т.д.), которое можно легко подобрать или угадать.

12. Неправильно ввести пароль к ключу ЭП, который находится на USB-токене «MS_KEY K», можно не более 10 раз подряд. После этого ключ ЭП блокируется навсегда.

13. PIN-код должен состоять не менее чем из 8 символов и может содержать любую комбинацию из букв, цифр и знаков препинания (рекомендации аналогичные как для пароля к ключу, см.выше).

14. Назначенный PIN-код к «MS_KEY K» удалить нельзя, его можно лишь сменить.

15. Неправильно ввести PIN-кода доступа к «MS_KEY K» можно не более 10 раз подряд. После этого «MS_KEY K» блокируется для использования.

16. Если ключ ЭП удалить из Хранилища ключей, восстановить его будет невозможно. Поэтому удалять можно ключи, которые в дальнейшем не будут использоваться при работе с системой (ключи с истекшим сроком действия, скомпрометированные ключи и т.д.).

По всем возникающим вопросам обращайтесь в отдел автоматизации по телефону (8352) 34-44-41