Требования к аппаратному ключу

Определение

Аппаратный ключ (смарт-карта) – компактный носитель информации, содержащий в себе защищенный микропроцессор и операционную систему, контролирующую устройство, доступ к оперативной и долговременной памяти. Аппаратный ключ также содержит программу (апплет), выполняющую все необходимые криптографические операции внутри устройства и без использования внешних ресурсов.

Требования к аппаратному ключу

Ключ должен:

1. Генерировать и содержать с защищенном виде закрытые ключи ГОСТ и RSA, а также соответствующие им открытые ключи.
2. Обеспечивать безусловную защиту закрытых ключей от копирования во внешнюю вычислительную систему
3. Обеспечить защиту оперативной и долговременной памяти от клонирования и НСД
4. Соответствовать стандарту PKCS-11
5. Удовлетворять всем требованиям законодательства Российской Федерации для создания квалифицированной электронной подписи.
6. Реализовать функционирование следующих криптоалгоритмов:
    a. AES (длины ключей 128, 192, 256 бит);
    b. 3DES (длины ключей 168 бит);
    c. RSA (длины 1024, 2048);
    d. криптография на эллиптических кривых (длины ключей 512 бит);
    e. аппаратная генерация ключей для RSA и криптографии на эллиптических кривых (ГОСТ);
    f. аппаратная генерация случайных чисел
    g. алгоритмы согласования ключей: алгоритм Диффи-Хеллмана, алгоритм Диффи-Хеллмана на эллиптических кривых;
    h. функции хэширования: SHA-1, SHA-256;
    i. ГОСТ Р 34.10-2001 (генерация ключевых пар, формирование и проверка ЭП);
    j. ГОСТ Р 34.11-94 (функция хэширования);
7. Реализовывать функциональность монотонного защищенного счетчика в объеме, изложенном в Приложении 1.

Требования к библиотеке связи

Аппаратный ключ должен содержать библиотеку связи, реализующую стандарт PKCS-11 (включая ГОСТ). Библиотека и прочее необходимое для работы ПО должно поддерживать работу на оборудовании со следующими операционными системами:

- Windows 10 (32/64-бит)
- Windows 8.1 (32/64-бит)
- Windows 7 SP1 (32/64-бит)
- Red Hat Linux Enterprise Linux 6.3 Desktop (32/64-бит)
- OpenSUSE 12.2 (32/64-бит)
- Ubuntu Desktop 12.04.1 LTS и 15.04 (32/64-бит)
- CentOS 6,7 (32/64-бит)

Приложение 1

Монотонно-возрастающий счетчик

Встроенное программное обеспечение смарт-карты должно обеспечивать функциональность неубывающего счетчика. Каждое ЭП, успешно рассчитанная смарт-картой, должна обеспечивать увеличение значения счетчика на единицу.

Встроенное программное обеспечение НЕ ДОЛЖНО содержать никаких открытых программных интерфейсов, с помощью которых можно изменить значение счетчика. Счетчик не должен терять свое значение при переформатировании карты. Счетчик должен выдаваться только на чтение. Выдаваемое на чтение значение счетчика должно сопровождаться криптографической контрольной суммой.

Криптографическая контрольная сумма

Криптографическая контрольная сумма должна представлять собой результат расчета ЭП от следующих параметров:

- Аппаратный номер карты
- Значение дайджеста последних данных, от которых рассчитывалась ЭП
- Значение счетчика

Значение ЭП вычисляется с использованием СПЕЦИАЛЬНОЙ ключевой пары. Пара МОЖЕТ содержать сигнальный атрибут и / или иные средства, препятствующие использованию этой пары в других процедурах подписания помимо расчета контрольной суммы.