Требования к защищенному устройству для хранения ключей и сертификатов электронной цифровой подписи Научно-информационного центра «Новые технологии»

Защищенное устройство (USB-токен, SAM-карта) должно быть оснащено контроллером безопасности.

Защищенное устройство должно поддерживать T=0 и T=1 – протоколы коммуникации и криптографические алгоритмы, 3DES, AES, RSA, SHA-1, SHA-224, SHA-256, ECC over GF(p) и Random number generation и функции шифрования.

Защищенное устройство должно соответствовать стандартам Java Card 2.2.2 или Java Card 3.0.3, Global Platform 2.1.1 и выше.

Защищенное устройство в форм факторе SAM-карты должно иметь размеры ISO/IEC 7810:2003, ID-1 (Standart SIM 1FF) с прорезями для получения размера ISO/IEC 7810:2003, ID-000 (Mini SIM 2FF);

Скорость работы алгоритмов защищенного устройства по O'zDSt1092-2009 не должна превышать 600 миллисекунд, скорость работы апплета защищенного устройства не должна превышать 2 секунды, объем памяти, выделяемой для хранения данных, должен быть не менее 100 килобайт и объем оперативной памяти защищенного устройства должен быть не менее 8 килобайт.

Износостойкость не менее 500,000 циклов перезаписи.

Срок хранения данных не менее 10 лет.

Интерфейс ISO 7816, CCID.

Сопроцессор должен быть доступен Java-апплету для реализации стандарта OzDST 1092:2009 алгоритм II. В SDK должен быть реализован Java-класс BigNumberEx с методами реализующими математику с большими числами и математику на эллиптических кривых.

Защищенное устройство должно иметь ATR, внутренний уникальный не менее 18-байтный заводской номер CPLC доступный специальной APDU командой и внешне напечатанный серийный номер в виде баркод и серийный номер в формате BBNNNNNNNNNNN.

Должен быть предоставлен список со связкой CPLC и серийного номера защищенного устройства в электронном формате CSV.

Должны быть предоставлены коды аутентификации ENC, MAC, DEK для загрузки скомпилированного Java-апплета в защищенное устройство.

Должна быть возможность замены стандартных кодов аутентификации ENC, MAC, DEK на другие.