I. Исполнения носителей ФОРОС-PKCS

Предусмотрены исполнения в виде смарт-карт и USB-ключей реализуемых на базе защищенных микроконтроллеров смарт-карт с защищенной энергонезависимой памятью 80 Кбайт - 160 Кбайт. Потребитель может выбрать исполнение в зависимости от своих потребностей.

II. Конфигурация носителей

Конфигурация носителей ФОРОС-PKCS согласовываются с Заказчиком при выпуске партии изделия, в том числе **максимально возможное количество ключей и размеры областей памяти**, выделяемых в носителе для публичных и приватных объектов данных.

Общее число объектов соответствующей области может достигать 254, а суммарный размер всех атрибутов всех объектов соответствующей области (приватной или публичной) - 32 КБайт.

По умолчанию предлагается конфигурация, обеспечивающая:

А) возможность хранения и применения криптографических объектов PKCS#11 в составе:

- **2-х ключевых пар ГОСТ Р34.10-2012** для функций формирования и проверки электронной подписи;
- **2 отдельных открытых ключей** ГОСТ Р34.10-2012 для функций формирования и проверки подписи.

Б) возможность хранения некриптографических объектов данных PKCS#11:

- область памяти для хранения приватных объектов данных, достаточной, например, для хранения значений **двух сертификатов открытого ключа размером до 4 Кбайт каждый**;
- область памяти для хранения публичных объектов данных.

В) разграничение прав доступа к приватным и публичным объектам:

- Пароль администратора токена (SO PIN)
- Пароль пользователя (User PIN)

Пароли носителя:

Транспортные значения SO PIN и User PIN согласуются с Заказчиком при поставке партий носителей. Число попыток неверного предъявления пароля администратора составляет 5, пароля пользователя также составляет 5 попыток. Эти значения также могут быть согласованы с Заказчиком.

Разблокировка SO PIN невозможна.

Разблокировка User PIN выполняется либо с помощью функций PKCS#11 (функции C_InitToken, C_InitPin, C_SetPin), либо с помощью утилиты UnblockPKCS11.exe (для ОС Windows).

Возможно встраивание в Носитель дополнительных приложений, реализуемых по спецификации Заказчика.

III. Поддерживаемые классы объектов и механизмы

ФОРОС-PKCS поддерживает следующие классы объектов PKCS#11:

- CKO_PRIVATE_KEY
- CKO_PUBLIC_KEY
- CKO_SECRET_KEY
- CKO_DATA
- CKO_CERTIFICATE

ФОРОС-PKCS поддерживает следующие механизмы PKCS#11:

- CKM_GOSTR3410_512_KEY_PAIR_GEN
- CKM_GOSTR3410_256
- CKM_GOSTR3410_WITH_GOSTR3411_12_256
- CKM_GOSTR3411_12_256

Более подробно информация о поддерживаемых классах, объектах и функциях приведена в документе «Руководство программиста» (предоставляется по отдельному запросу).

IV Технические характеристики

Поддерживаемые протоколы: ISO 7816 T=0
Интерфейс подключения (для R301 Форос PKCS): USB 2.0 Full Speed Device, 12 Мбит/сек
Скорость обмена данными: До 323 Кбит/сек, 4 МГц; 500кбит/сек, 6МГц
Перечень поддерживаемых ОС: Windows 7, 8.1, Windows 10, Linux

Перечень поддерживаемых крипто алгоритмов: на аппаратном уровне обеспечивается поддержка современных российских криптографических алгоритмов ГОСТ Р34.11-2012 для хэширования, ГОСТ Р34.10-2012 для формирования и проверки электронной подписи. Обеспечивается поддержка алгоритмов согласования ключей VKO GOST R 34.10-2012, шифрования по ГОСТ Р 34.12-2015 в режимах ГОСТ Р 34.13-2015, а также выработки HMAC согласно ГОСТ Р 50.1.113-2016.

V Информационная безопасность

Носитель Форос-PKCS по умолчанию реализуется на платформе СЗИ ФОРОС 2 (сертификат соответствия ожидается во II кв. 2021). Опционально возможна реализация версии носителя на платформе сертифицированного СКЗИ Форос 2.

Носитель Форос-PKCS обеспечивает неизвлекаемость криптографических ключей, их защиту от несанкционированного доступа в случае утери или хищения Носителя.