



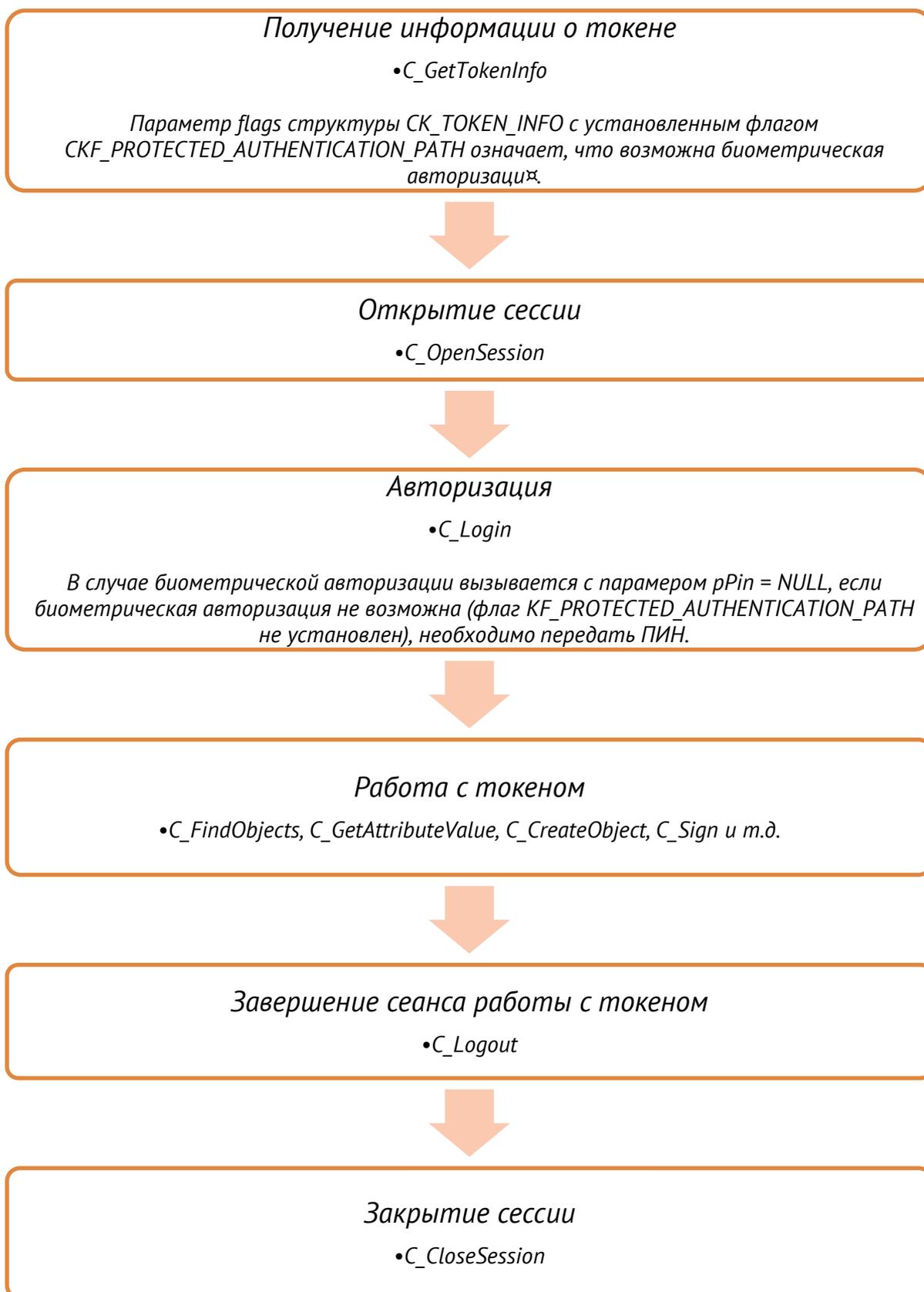
ESMART[®]

ESMART Token BIO – PKCS#11

1. *Сценарий работы с библиотекой PKCS11*



2. Сценарий работы с токеном



3. Особенности

Для алгоритмов ГОСТ поддерживается фиксированный набор параметров в соответствии с RFC 4357, которые можно указывать для атрибутов CKA_GOST28147_PARAMS, CKA_GOSTR3410_PARAMS, CKA_GOSTR3411_PARAMS:

*id_Gost28147_89_CryptoPro_A_ParamSet
id_Gost28147_89_CryptoPro_B_ParamSet
id_Gost28147_89_CryptoPro_C_ParamSet
id_Gost28147_89_CryptoPro_D_ParamSet
id_Gost28147_89_CryptoPro_RIC_1_ParamSet
id_GostR3410_2001_TestParamSet
id_GostR3410_2001_CryptoPro_A_ParamSet
id_GostR3410_2001_CryptoPro_B_ParamSet
id_GostR3410_2001_CryptoPro_C_ParamSet
id_GostR3410_2001_CryptoPro_XchA_ParamSet
id_GostR3410_2001_CryptoPro_XchB_ParamSet
id_GostR3411_94_CryptoProParamSet*

Предполагается, что на карте существуют соответствующие объекты SKO_DOMAIN_PARAMETERS, создание/поиск этих объектов не реализованы.