1 ПРОЦЕДУРА ОБНОВЛЕНИЯ АППАРАТНО-ПРОГРАММНЫХ ПРОДУКТОВ

1.1 Сравнение функциональных возможностей Криптографических средств 5 поколения и Криптографических средств 6 поколения

Основные отличия функциональных возможностей **Криптографических средств 5 поколения** и **Криптографических средств 6 поколения** приведены в таблице ниже (Таблица 1).

Таблица 1 – Сравнение функциональных возможностей Криптографических средств 5 поколения и Криптографических средств 6 поколения

Функциональные возможности	**Криптографические средства 5 поколения**	**Криптографические средства 6 поколения**
Вычисление хэш-значений по ГОСТ Р 34.11-94	Поддерживается	Поддерживается
Формирование ключей электронной подписи (ЭП) и закрытых ключей шифрования, вычисление и проверка ЭП по ГОСТ Р 34.10-2001	Поддерживается	Поддерживается (исключительно в части проверки архивных ЭП)
Вычисление хэш-значений по ГОСТ Р 34.11-2012 (256 бит)	Поддерживается	Поддерживается
Вычисление хэш-значений по ГОСТ Р 34.11-2012 (512 бит)	Не поддерживается	Поддерживается
Формирование ключей ЭП и закрытых ключей шифрования, вычисление и проверка ЭП по ГОСТ Р 34.10-2012 (256 бит, эллиптические группы RFC 4357 A, B, C)	Поддерживается	Поддерживается
Формирование ключей ЭП и закрытых ключей шифрования, вычисление и проверка ЭП по ГОСТ Р 34.10-2012 (256 бит, эллиптические группы A, B, C, D, ТК№26)	Не поддерживается	Поддерживается
Формирование ключей ЭП, вычисление и проверка ЭП по ГОСТ Р 34.10-2012 (512 бит, эллиптические группы A, B, C, ТК№26)	Не поддерживается	Поддерживается
Шифрование по ГОСТ 28147-89 (узлы замены A, B, C, D, ТК№26)	Поддерживается	Поддерживается
Шифрование по ГОСТ Р 34.12-2015 (блочные шифры «Магма», «Кузнечик») и ГОСТ Р 34.13-2015 (режимы простой замены, гаммирования, выработки имитовставки)	Не поддерживается	Поддерживается
Формирование и обработка сообщений формата PKCS#7 в соответствии с рекомендациями RFC 4357, RFC 4490 и RFC 4491	Поддерживается	Поддерживается
Формирование и обработка сообщений формата Cryptographic Message Syntax (CMS) в соответствии с рекомендациями ТК№26	Не поддерживается	Поддерживается
Формат ключа проверки ЭП и открытого ключа шифрования в сертификатах и запросах	Не поддерживается	Поддерживается

Функциональные возможности	Криптографические средства 5 поколения	Криптографические средства 6 поколения
на сертификат PKCS#10 системы управления сертификатами (СУС)-X.509 в соответствии с рекомендациями ТК№26		
Реализация протокола TLS 1.0, основанная на наборе криптографических алгоритмов на базе ГОСТ 28147-89	Поддерживается	Поддерживается
Реализация протокола TLS 1.2, основанная на наборе криптографических алгоритмов на базе ГОСТ 34.12-2015/ГОСТ 34.13-2015 (блочный шифр «Кузнечик») в соответствии с рекомендациями ТК№26	Не поддерживается	Поддерживается

1.2 Общее описание процедуры обновления Криптографических средств

Перед началом процедуры обновления **Криптографических средств 5 поколения** на **Криптографические средства 6 поколения** необходимо убедиться в том, что все используемые ключи ЭП и закрытые ключи шифрования сформированы по ГОСТ Р 34.10-2012 (256 бит).

Процедура обновления Криптографических средств 5 поколения на Криптографические средства 6 поколения выполняется в два этапа:

– на первом этапе производится обновление Криптографических средств клиентов, при этом **обновление Криптографических средств клиентов, функционирующих за пределами Российской Федерации, должно выполняться в последнюю очередь**;

– на втором этапе производится обновление Криптографических средств Удостоверяющих центров.

Во избежание конфликтов между различными поколениями Криптографических средств, которые функционируют в рамках одной или нескольких, сопряженных друг с другом, автоматизированных систем, до полного завершения обоих этапов обновления запрещается использование любых функциональных возможностей, которые не поддерживаются Криптографическими средствами 5 поколения.

При обновлении Криптографических средств клиентов, функционирующих совместно в рамках клиент-серверных приложений - клиентских библиотек и криптографических серверов, а также клиентов и серверов протоколов TLS и IPsec, необходимо руководствоваться следующим общим правилом: **Криптографические средства серверной**

стороны клиент-серверного приложения должны быть обновлены в первую очередь, только после чего допускается обновлять Криптографические средства клиентских сторон данного приложения.

При обновлении Криптографических средств клиентов и серверов протокола TLS необходимо руководствоваться следующими правилами:

- **непосредственно после обновления Криптографического средства сервера протокола TLS в данном средстве необходимо включить опцию “Поддерживать устаревшие СКЗИ” (при ее наличии);**
- **после завершения процедуры обновления всех Криптографических средств в настройках сервера протокола TLS опцию “Поддерживать устаревшие СКЗИ” можно выключить только после выключения данной опции у всех клиентов протокола TLS (при ее наличии);**
- **переход на использование реализации протокола TLS версия 1.2 (в соответствии с рекомендациями ТК №26) возможен только после завершения процедуры обновления всех Криптографических средств.**

*Примечание – **Криптографические средства 6 поколения** будут гарантированно корректно функционировать совместно с ФКН «Валидата vdToken», при условии использования исключительно функциональных возможностей, поддерживаемых Криптографическими средствами 5 поколения.*

1.3 Внедрение нового формата ключей проверки ЭП и открытых ключей шифрования

В Криптографических средствах 6 поколения ключи проверки ЭП и открытые ключи шифрования формируются в соответствии с рекомендациями ТК№26 тогда, когда для генерации соответствующих ключей ЭП и закрытых ключей шифрования установлены эллиптические группы ТК№26 A, B, C или D (256 бит), или A, B, или C (512 бит).

После завершения обоих этапов процедуры обновления (см. п.2.2) ***рекомендуется*** начать плавное внедрение формата ключа проверки ЭП и открытого ключа шифрования в сертификатах и запросах на сертификат PKCS#10 СУС X.509 в соответствии с рекомендациями ТК№26. Для этого необходимо в соответствующих настройках используемого Криптографического средства указать, что ключи ЭП и закрытые ключи шифрования следует формировать по ГОСТ Р 34.10-2012 (256 бит) с эллиптической группой ТК№26 A, B, C или D.

Аналогично, после завершения обоих этапов процедуры обновления (см. п.2.2), ***можно*** начать плавное внедрение ключей ЭП и закрытых ключей шифрования по ГОСТ Р 34.10-2012 (512 бит). Для этого необходимо в соответствующих настройках используемого Криптографического средства указать, что ключи ЭП и закрытые ключи шифрования следует формировать по ГОСТ Р 34.10-2012 (512 бит) с эллиптической группой ТК№26 A, B, или C.

Примечание – Следует учитывать тот факт, что производительность криптографических преобразований по ГОСТ Р 34.10-2012 (512 бит) значительно ниже (примерно в 4 раза), чем по ГОСТ Р 34.10-2012 (256 бит). В связи с этим, внедрение ключей ЭП и закрытых ключей шифрования по ГОСТ Р 34.10-2012 (512 бит) следует проводить в тех случаях, когда требуется повышенная криптографическая стойкость, а снижение производительности криптографических преобразований не является критичным.

2 ПРОЦЕДУРА ДОРАБОТКИ ПРИКЛАДНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

В ***Криптографических средствах 6 поколения*** (в инструментариях разработчика) реализовано множество новых программных интерфейсов – типов, констант, структур и функций. Эти интерфейсы позволяют оперировать защищенными сообщениями формата CMS, а также использовать канальное шифрование по протоколу TLS версия 1.2 на базе ГОСТ Р 34.12-2015 (блочные шифры «Магма», «Кузнечик») и ГОСТ Р 34.13-2015 (в режимах простой замены, гаммирования, выработки имитовставки) в соответствии с рекомендациями ТК№26.

Некоторые программные интерфейсы, реализованные в ***Криптографических средствах 5 поколения*** (в частности те, которые позволяют оперировать защищенными сообщениями простого формата и формата PKCS#7), объявляются ***устаревшими*** и ***будут удалены*** в последующих поколениях Криптографических средств.

Примечание – Устаревшие программные интерфейсы не описаны в документации, включаемой в инструментарии разработчика ***Криптографических средств 6 поколения****. Для получения детального описания устаревших программных интерфейсов необходимо обратиться к документации, включаемой в инструментарии разработчика* ***Криптографических средств 5 поколения.***

Необходимо выполнить доработку прикладного программного обеспечения в части проверки пригодности сертификатов для шифрования. Согласно разделу ***5.3 Область использования ключа*** Рекомендации по стандартизации «Использование алгоритмов ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012 в сертификате, списке аннулированных сертификатов (CRL) и запросе на сертификат PKCS #10 инфраструктуры открытых ключей X.509» (***Р 1323565.1.023-2018***), пригодность сертификата для шифрования определяется наличием флага ***keyAgreement*** в расширении ***KeyUsage***. Указанный флаг соответствует маске ***KEYUSAGE_KEY_AGREEMENT*** (согласование ключей), задаваемой в поле ***keyUsage*** структуры ***certificate_t***. ***Не допускается*** использовать при проверке пригодности сертификата для шифрования маски ***KEYUSAGE_KEY_ENCIPHERMENT*** и ***KEYUSAGE_DATA_ENCIPHERMENT***.

Следует выполнить доработку прикладного программного обеспечения в части перевода на использование новых программных интерфейсов, поддерживающих ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015 и реализованных в ***Криптографических средствах 6 поколения***.

В следующих ниже подразделах приведены перечни устаревших программных интерфейсов с указанием актуальных интерфейсов для замены (при их наличии), предоставляемых ***Криптографическими средствами 6 поколения***.

В заголовочных файлах ***vcert1.h*** и ***vcerterr.h***, поставляемых в инструментариях разработчика ***Криптографических средств 6 поколения***, устаревшие программные интерфейсы помечены макросом ***_VD_DIS_DEPR***. Для проверки того, что устаревшие программные интерфейсы не используются прикладным программным обеспечением, последнее следует перекомпилировать со значением макроса ***_VD_DIS_DEPR***, установленным в ***1*** – перекомпиляция должна завершиться успешно.

2.1 Типы и общие флаги криптографических функций

Перечень типов, констант и общих флагов криптографических функций, в том числе устаревших, приведен ниже в таблице (Таблица 2).

Таблица 2 – Перечень типов и общих флагов криптографических функций

Устаревший прикладной интерфейс (заменяемый)	**Новый прикладной интерфейс (заменяющий)**	**Примечание**
Тип strsign_t	Тип strcms_t	Унифицирован тип контекстов выполнения потоковых функций, оперирующих защищенными сообщениями в формате CMS
Тип strverify_t	Тип strcms_t	Унифицирован тип контекстов выполнения потоковых функций, оперирующих защищенными сообщениями в формате CMS
Тип strencrypt_t	Тип strcms_t	Унифицирован тип контекстов выполнения потоковых функций, оперирующих защищенными сообщениями в формате CMS
Тип strdecrypt_t	Тип strcms_t	Унифицирован тип контекстов выполнения потоковых функций, оперирующих защищенными сообщениями в формате CMS
Флаг FLAG_SIMPLE	Отсутствует	Новые программные интерфейсы формируют защищенные сообщения в формате CMS в соответствии с рекомендациями ТК№26
Флаг FLAG_PKCS7	Отсутствует	Новые программные интерфейсы формируют защищенные сообщения в формате CMS в соответствии с рекомендациями ТК№26
Флаг FLAG_DETACHED	Отсутствует	Для подписанных CMS сообщений с присоединенными ЭП и с отсоединенными ЭП используются различные наборы функций

2.2 Функции инициализации и деинициализации

Перечень функций инициализации и деинициализации, в том числе устаревших, приведен ниже в таблице (Таблица 3).

Таблица 3 – Функции инициализации и деинициализации

Устаревший прикладной интерфейс (заменяемый)	Новый прикладной интерфейс (заменяющий)	Примечание
Флаг FLAG_INIT_NOCRLUPDATE	Флаг FLAG_INIT_DISABLECRLUPDATE	Замена произведена для повышения читаемости идентификатора
Флаг FLAG_INIT_CHECKEXPIRED	Флаг FLAG_INIT_EXPIRINGOBJECTUI	Замена произведена для повышения читаемости идентификатора
Флаг FLAG_INIT_NOLDAP	Флаг FLAG_INIT_DISABLELDAPUSAGE	Замена произведена для повышения читаемости идентификатора
Флаг FLAG_INIT_NOKEYUNLOAD	Отсутствует	В Криптографических средствах 6 поколения отсутствует возможность хранения ключей ЭП и закрытых ключей шифрования в хранилище, общем для различных процессов
Флаг FLAG_INIT_NOSAVECACHE	Флаг FLAG_INIT_DISABLECACHESAVE	Замена произведена для повышения читаемости идентификатора
Флаг FLAG_INIT_REGISTRY	Флаг FLAG_INIT_CERTSTOREPROFILE	Замена произведена для повышения читаемости идентификатора
Флаг FLAG_INIT_FORCE_CACHE_CERTS	Флаг FLAG_INIT_FORCECERTCACHING	Замена произведена для повышения читаемости идентификатора
Флаг FLAG_INIT_ALLOW_RA_IN_CHAIN	Отсутствует	В Криптографических средствах 6 поколения возможность использования сертификатов регистрации для инициализации контекста библиотеки является устаревшей
Флаг FLAG_INIT_LDAP_CHAIN_SEARCH	Отсутствует	В Криптографических средствах 6 поколения построение цепочек производится исключительно с

Устаревший прикладной интерфейс (заменяемый)	Новый прикладной интерфейс (заменяющий)	Примечание
		использованием точек доступа к Центру (AIA) и точек распространения CAC (CDP)
Флаг FLAG_INIT_USE_AIA_CDP	Флаг FLAG_INIT_ALLOWAIACDPUSAGE	Замена произведена для повышения читаемости идентификатора
Флаг FLAG_INIT_SILENT_KEYLOAD	Флаг FLAG_INIT_USESILENTKEYLOAD	Замена произведена для повышения читаемости идентификатора
Флаг FLAG_INIT_VERIFYCONTEXT	Флаг FLAG_INIT_USEVERIFYCONTEXT	Замена произведена для повышения читаемости идентификатора

2.3 Функции вычисления хэш-значений

Перечень функций вычисления хэш-значений, в том числе устаревших, приведен ниже в таблице (Таблица 6).

Таблица 4 – Функции вычисления хэш-значений

Устаревший прикладной интерфейс (заменяемый)	Новый прикладной интерфейс (заменяющий)	Примечание
Функция VCERT_HashMem()	Функция VCERT_BlkHashMem()	Новая функция позволяет задавать алгоритм для вычисления хэш-значения
Функция VCERT_HashFile()	Функция VCERT_BlkHashFile()	Новая функция позволяет задавать алгоритм для вычисления хэш-значения

2.4 Функции получения информации о CMS/PKCS#7 сообщениях

Перечень функций получения информации о CMS/PKCS#7 сообщениях, в том числе устаревших, приведен ниже в таблице (Таблица 7).

Таблица 5 – Функции получения информации о CMS/PKCS#7 сообщениях

Устаревший прикладной интерфейс (заменяемый)	Новый прикладной интерфейс (заменяющий)	Примечание
Структура signed_info_result_t	Структура cms_msginf_t	Структура cms_msginf_t является общей для подписанных и зашифрованных CMS/PKCS#7 сообщений
Структура encrypted_info_result_t	Структура cms_msginf_t	Структура cms_msginf_t является общей для подписанных и зашифрованных

Устаревший прикладной интерфейс (заменяемый)	Новый прикладной интерфейс (заменяющий)	Примечание
		CMS/PKCS#7 сообщений
Структура pkcs7_info_t	Структура cms_msginf_t	Структура cms_msginf_t поддерживает большее количество способов идентификации сертификатов, и большее количество типов структур получателей
Функция VCERT_SignedInfoMem()	Функция VCERT_CmsBlkMsgInfMem()	Блочное получение информации о подписанном CMS/PKCS#7 сообщении
Функция VCERT_SignedInfoFile()	Функция VCERT_CmsBlkMsgInfFile()	Блочное получение информации о подписанном CMS/PKCS#7 сообщении
Функция VCERT_FreeSignedInfoResult()	Функция VCERT_CmsFreeMsgInf()	-
Функция VCERT_EncryptedInfoMem()	Функция VCERT_CmsBlkMsgInfMem()	Блочное получение информации о зашифрованном CMS/PKCS#7 сообщении
Функция VCERT_EncryptedInfoFile()	Функция VCERT_CmsBlkMsgInfFile()	Блочное получение информации о зашифрованном CMS/PKCS#7 сообщении
Функция VCERT_StrEncryptedInfoMem()	Функции VCERT_CmsStrMsgInfInitMem() VCERT_CmsStrMsgInfUpdateMem() VCERT_CmsStrMsgInfFinalMem()	Потоковое получение информации о зашифрованном CMS/PKCS#7 сообщении. Следует последовательно вызывать функции Init, Update (возможно, несколько раз), Final
Функция VCERT_StrEncryptedInfoFile()	Функция VCERT_CmsStrMsgInfFile()	Потоковое получение информации о зашифрованном CMS/PKCS#7 сообщении
Функция VCERT_FreeEncryptedInfoResult()	Функция VCERT_CmsFreeMsgInf()	
Функция VCERT_GetPkcs7InfoMem()	Функция VCERT_CmsBlkMsgInfMem()	Блочное получение информации о CMS/PKCS#7 сообщении
Функция VCERT_GetPkcs7InfoFile()	Функция VCERT_CmsBlkMsgInfFile()	Блочное получение информации о CMS/PKCS#7 сообщении
Отсутствует	Функции VCERT_CmsStrMsgInfInitMem() VCERT_CmsStrMsgInfUpda	Потоковое получение информации о CMS/PKCS#7 сообщении. Следует последовательно вызывать

Устаревший прикладной интерфейс (заменяемый)	Новый прикладной интерфейс (заменяющий)	Примечание
	teMem() VCERT_CmsStrMsgInfFinalMem()	функции Init, Update (возможно, несколько раз), Final
Отсутствует	Функция VCERT_CmsStrMsgInfFile()	Потоковое получение информации о CMS/PKCS#7 сообщении
Функция VCERT_FreePkcs7Info()	Функция VCERT_CmsFreeMsgInf()	

2.5 Функции вычисления ЭП

Перечень функций вычисления ЭП, в том числе устаревших, приведен ниже в таблице (Таблица 8).

Таблица 6 – Функции вычисления ЭП

Устаревший прикладной интерфейс (заменяемый)	Новый прикладной интерфейс (заменяющий)	Примечание
Флаг FLAG_SIGN_SENDCERT	Флаг FLAG_CMS_SIGN_ADDSIGNER	Замена произведена для повышения читаемости идентификатора
Отсутствует	Флаг FLAG_CMS_SIGN_SUBJKEYID	Использовать для идентификации сертификата подписанта расширение Идентификатор ключа владельца. *Полученная ЭП не сможет быть проверена с использованием Криптографического средства 5 поколения*
Отсутствует	Флаг FLAG_CMS_SIGN_ENVELOPE	Подписание поверх переданных данных, без проверки наличия существующих ЭП
Отсутствует	Флаг FLAG_CMS_SIGN_CADESBES	Добавить в ЭП обязательные подписываемые атрибуты в соответствии со стандартом CAdES-BES
Функция VCERT_SignMem()	Функция VCERT_CmsBlkAttSignMem()	Вычисление блочной присоединенной ЭП
Функция VCERT_SignFile()	Функция VCERT_CmsBlkAttSignFile()	Вычисление блочной присоединенной ЭП
Функция	Функция	Вычисление блочной

Устаревший прикладной интерфейс (заменяемый)	Новый прикладной интерфейс (заменяющий)	Примечание
VCERT_SignMem()	VCERT_CmsBlkDetSignMem()	отсоединенной ЭП
Функция VCERT_SignFile()	Функция VCERT_CmsBlkDetSignFile()	Вычисление блочной отсоединенной ЭП
Отсутствует	Функции VCERT_CmsStrAttSignInitMem() VCERT_CmsStrAttSignUpdateMem() VCERT_CmsStrAttSignFinalMem()	Вычисление потоковой присоединенной ЭП. Следует последовательно вызывать функции Init, Update (возможно, несколько раз), Final
Отсутствует	Функция VCERT_CmsStrAttSignFile()	Вычисление потоковой присоединенной ЭП
Функции VCERT_StrSignInitMem() VCERT_StrSignUpdateMem() VCERT_StrSignFinalMem()	Функции VCERT_CmsStrDetSignInitMem() VCERT_CmsStrDetSignUpdateMem() VCERT_CmsStrDetSignFinalMem()	Вычисление потоковой отсоединенной ЭП. Следует последовательно вызывать функции Init, Update (возможно, несколько раз), Final
Функция VCERT_StrSignFile()	Функция VCERT_CmsStrDetSignFile()	Вычисление потоковой отсоединенной ЭП

2.6 Функции проверки ЭП

Перечень функций проверки ЭП, в том числе устаревших, приведен ниже в таблице (Таблица 9).

Таблица 7 – Функции проверки ЭП

Устаревший прикладной интерфейс (заменяемый)	Новый прикладной интерфейс (заменяющий)	Примечание
Флаг FLAG_VERIFY_DELSIGN	Флаг FLAG_CMS_VERIFY_DELETESIGNATURES	Замена произведена для повышения читаемости идентификатора
Флаг FLAG_VERIFY_KEYUSAGE	Флаг FLAG_CMS_VERIFY_SIGNERKEYUSAGES	Замена произведена для повышения читаемости идентификатора
Флаг FLAG_VERIFY_POLICY	Флаг FLAG_CMS_VERIFY_SIGNERPOLICIES	Замена произведена для повышения читаемости идентификатора
Флаг FLAG_VERIFY_EXTKEYUSAGE	Флаг FLAG_CMS_VERIFY_SIGNEREXTKEYUSAGES	Замена произведена для повышения читаемости идентификатора
Флаг FLAG_VERIFY_MINSIGNS	Флаг FLAG_CMS_VERIFY_MINIMUMSIGNATURES	Замена произведена для повышения читаемости

Устаревший прикладной интерфейс (заменяемый)	Новый прикладной интерфейс (заменяющий)	Примечание
		идентификатора
Флаг FLAG_VERIFY_NOTIMECHECK	Флаг FLAG_CMS_VERIFY_DONOTCHECKTIMES	Замена произведена для повышения читаемости идентификатора
Флаг FLAG_VERIFY_NOCACHECERT	Флаг FLAG_CMS_VERIFY_DONOTADDSIGNER	Замена произведена для повышения читаемости идентификатора
Флаг FLAG_VERIFY_NOATTACHEDCERT	Флаг FLAG_CMS_VERIFY_IGNOREATTACHEDSIGNER	Замена произведена для повышения читаемости идентификатора
Флаг FLAG_VERIFY_USEREVTIME	Флаг FLAG_CMS_VERIFY_USEREVOCATIONTIME	Замена произведена для повышения читаемости идентификатора
Флаг FLAG_VERIFY_NOADDCER_FRM_PKCS7	Флаг FLAG_CMS_VERIFY_DONOTADDATTACHEDSIGNER	Замена произведена для повышения читаемости идентификатора
Флаг FLAG_VERIFY_REQUIREATTACHEDSIGNER	Флаг FLAG_CMS_VERIFY_REQUIREATTACHEDSIGNER	Замена произведена для повышения читаемости идентификатора
Отсутствует	Флаг FLAG_CMS_VERIFY_USEATTACHEDCHAIN	Использовать сертификаты и CAC из CMS сообщения при проверке цепочек сертификатов подписантов
Функция VCERT_VerifyMem()	Функция VCERT_CmsBlkAttVerifyMem()	Проверка блочной присоединенной ЭП
Функция VCERT_VerifyFile()	Функция VCERT_CmsBlkAttVerifyFile()	Проверка блочной присоединенной ЭП
Функция VCERT_VerifyMem()	Функция VCERT_CmsBlkDetVerifyMem()	Проверка блочной отсоединенной ЭП
Функция VCERT_VerifyFile()	Функция VCERT_CmsBlkDetVerifyFile()	Проверка блочной отсоединенной ЭП
Отсутствует	Функции VCERT_CmsStrAttVerifyInitMem() VCERT_CmsStrAttVerifyUpdateMem() VCERT_CmsStrAttVerifyFinalMem()	Проверка потоковой присоединенной ЭП. Следует последовательно вызывать функции Init, Update (возможно, несколько раз), Final
Отсутствует	Функция VCERT_CmsStrAttVerifyFile()	Проверка потоковой присоединенной

Устаревший прикладной интерфейс (заменяемый)	Новый прикладной интерфейс (заменяющий)	Примечание
		ЭП
Функции VCERT_StrVerifyInitMem() VCERT_StrVerifyUpdateMem() VCERT_StrVerifyFinalMem()	Функции VCERT_CmsStrDetVerifyInitMem() VCERT_CmsStrDetVerifyUpdateMem() VCERT_CmsStrDetVerifyFinalMem()	Проверка потоковой отсоединенной ЭП. Следует последовательно вызывать функции Init, Update (возможно, несколько раз), Final
Функция VCERT_StrVerifyFile()	Функция VCERT_CmsStrDetVerifyFile()	Проверка потоковой отсоединенной ЭП

2.7 Функции зашифрования

Перечень функций зашифрования, в том числе устаревших, приведен ниже в таблице (Таблица 10).

Таблица 8 – Функции зашифрования

Устаревший прикладной интерфейс (заменяемый)	Новый прикладной интерфейс (заменяющий)	Примечание
Флаг FLAG_ENCRYPT_REMOTE	Флаг FLAG_CMS_ENCRYPT_USEREMOTESEARCH	Замена произведена для повышения читаемости идентификатора
Флаг FLAG_ENCRYPT_NOTIMECHECK	Флаг FLAG_CMS_ENCRYPT_DONOTCHECKTIMES	Замена произведена для повышения читаемости идентификатора
Флаг FLAG_ENCRYPT_NOVERIFY	Флаг FLAG_CMS_ENCRYPT_DONOTVERIFYCHAIN	Замена произведена для повышения читаемости идентификатора
Флаг FLAG_ENCRYPT_ADD_LDAP2LOCAL	Флаг FLAG_CMS_ENCRYPT_ADDREMOTETOLOCAL	Замена произведена для повышения читаемости идентификатора
Флаг FLAG_ENCRYPT_NOKEYTIMECHECK	Флаг FLAG_CMS_ENCRYPT_DONOTCHECKKEYTIME	Замена произведена для повышения читаемости идентификатора
Флаг FLAG_ENCRYPT_PARTIAL_SUBJECT	Флаг FLAG_CMS_ENCRYPT_SUBJECTISPARTIAL	Замена произведена для повышения читаемости идентификатора
Флаг FLAG_ENCRYPT_IGNORE_CACHED	Флаг FLAG_CMS_ENCRYPT_IGNORESTORECACHE	Замена произведена для повышения читаемости идентификатора
Флаг FLAG_ENCRYPT_IGNORE_LOCAL	Флаг FLAG_CMS_ENCRYPT_IGNORESTORELOCAL	Замена произведена для повышения читаемости идентификатора
Флаг FLAG_ENCRYPT_SUBJECT_ATTRIBUTE	Флаг FLAG_CMS_ENCRYPT_SUBJECTATTRIBUTE	Замена произведена для повышения читаемости идентификатора
Отсутствует	Флаг FLAG_CMS_ENCRYPT_SUBJKEYID	Использовать для идентификации сертификатов получателей расширение

Устаревший прикладной интерфейс (заменяемый)	Новый прикладной интерфейс (заменяющий)	Примечание
		Идентификатор ключа владельца. *Полученное зашифрованное сообщение не сможет быть расшифровано с использованием Криптографического средства 5 поколения*
Отсутствует	Флаг FLAG_CMS_ENCRYPT_GOST_R_34_12_15MG	Использовать для зашифрования CMS сообщения ГОСТ Р 34.12-2015 (блочный шифр «Магма»). *Полученное зашифрованное сообщение не сможет быть расшифровано с использованием Криптографического средства 5 поколения*
Отсутствует	Флаг FLAG_CMS_ENCRYPT_GOST_R_34_12_15GH	Использовать для зашифрования CMS сообщения ГОСТ Р 34.12-2015 (блочный шифр «Кузнечик»). *Полученное зашифрованное сообщение не сможет быть расшифровано с использованием Криптографического средства 5 поколения*
Отсутствует	Флаг FLAG_CMS_ENCRYPT_ADDOMACATTRIBUTE	Вычислять и добавлять в зашифрованное CMS сообщение имитовставку. *Полученное зашифрованное сообщение не сможет быть расшифровано с использованием Криптографического средства 5 поколения*
Отсутствует	Флаг FLAG_CMS_ENCRYPT_RECIPKEYAGREEMENT	Использовать в CMS сообщении структуры получателей типа KeyAgreement. *Полученное зашифрованное сообщение не сможет быть расшифровано с использованием Криптографического средства 5 поколения*
Функция VCERT_EncryptMem()	Функция VCERT_CmsBlkEncryptMem()	Блочное зашифрование
Функция VCERT_EncryptFile()	Функция VCERT_CmsBlkEncryptFile()	Блочное зашифрование
Функции VCERT_StrEncryptInitMem() VCERT_StrEncryptUpdateMem() VCERT_StrEncryptFinalMem()	Функции VCERT_CmsStrEncryptInitMem() VCERT_CmsStrEncryptUpdateMem() VCERT_CmsStrEncryptFinalMem()	Потоковое зашифрование. Следует последовательно вызывать функции Init, Update (возможно, несколько раз), Final
Функция VCERT_StrEncryptFile()	Функция VCERT_CmsStrEncryptFile()	Потоковое зашифрование

2.8 Функции расшифрования

Перечень функций расшифрования, в том числе устаревших, приведен ниже в таблице (Таблица 11).

Таблица 9 – Функции расшифрования

Устаревший прикладной интерфейс (заменяемый)	Новый прикладной интерфейс (заменяющий)	Примечание
Флаг FLAG_DECRYPT_NOCACHE	Отсутствует	В Криптографических средствах 6 поколения используется анонимное шифрование, поэтому сертификат отправителя зашифрованного CMS сообщения не определен
Флаг FLAG_DECRYPT_NOCRLCHECK	Отсутствует	В Криптографических средствах 6 поколения используется анонимное шифрование, поэтому сертификат отправителя зашифрованного CMS сообщения не определен
Флаг FLAG_DECRYPT_ADD_LDAP2LOCAL	Отсутствует	В Криптографических средствах 6 поколения используется анонимное шифрование, поэтому сертификат отправителя зашифрованного CMS сообщения не определен
Функция VCERT_DecryptMem()	Функция VCERT_CmsBlkDecryptMem()	Блочное расшифрование
Функция VCERT_DecryptFile()	Функция VCERT_CmsBlkDecryptFile()	Блочное расшифрование
Функции VCERT_StrDecryptInitMem() VCERT_StrDecryptUpdateMem() VCERT_StrDecryptFinalMem()	Функции VCERT_CmsStrDecryptInitMem() VCERT_CmsStrDecryptUpdateMem() VCERT_CmsStrDecryptFinalMem()	Потоковое расшифрование. Следует последовательно вызывать функции Init, Update

Устаревший прикладной интерфейс (заменяемый)	Новый прикладной интерфейс (заменяющий)	Примечание
		(возможно, несколько раз), Final
Функция VCERT_StrDecryptFile()	Функция VCERT_CmsStrDecryptFile()	Потоковое расшифрование

2.9 Совмещенные (комплексные) функции

Перечень совмещенных (комплексных) функций, в том числе устаревших, приведен ниже в таблице (Таблица 12).

Таблица 10 – Совмещенные (комплексные) функции

Устаревший прикладной интерфейс (заменяемый)	Новый прикладной интерфейс (заменяющий)	Примечание
Функция VCERT_VerifyAndSignMem()	Функции VCERT_CmsBlkAttVerifyMem() и VCERT_CmsBlkAttSignMem()	Проверка и вычисление блочных присоединенных ЭП. Последовательный вызов функций Verify и Sign
Функция VCERT_VerifyAndSignFile()	Функции VCERT_CmsBlkAttVerifyFile() и VCERT_CmsBlkAttSignFile()	Проверка и вычисление блочных присоединенных ЭП. Последовательный вызов функций Verify и Sign
Функция VCERT_VerifyAndSignMem()	Функции VCERT_CmsBlkDetVerifyMem() и VCERT_CmsBlkDetSignMem()	Проверка и вычисление блочных отсоединенных ЭП. Последовательный вызов функций Verify и Sign
Функция VCERT_VerifyAndSignFile()	Функции VCERT_CmsBlkDetVerifyFile() и VCERT_CmsBlkDetSignFile()	Проверка и вычисление блочных отсоединенных ЭП. Последовательный вызов функций Verify и Sign
Функция VCERT_SignAndEncryptMem()	Функции VCERT_CmsBlkAttSignMem() и VCERT_CmsBlkEncryptMem()	Вычисление блочной ЭП и зашифрование. Последовательный вызов функций Sign и Encrypt
Функция VCERT_SignAndEncryptFile()	Функции VCERT_CmsBlkAttSignFile() и VCERT_CmsBlkEncryptFile()	Вычисление блочной присоединенной ЭП и зашифрование.

Устаревший прикладной интерфейс (заменяемый)	Новый прикладной интерфейс (заменяющий)	Примечание
		Последовательный вызов функций Sign и Encrypt
Функция VCERT_DecryptAndVerifyMem()	Функции VCERT_CmsBlkDecryptMem() и VCERT_CmsBlkAttVerifyMem()	Расшифрование и проверка блочной присоединенной ЭП. Последовательный вызов функций Decrypt и Verify
Функция VCERT_DecryptAndVerifyFile()	Функции VCERT_CmsBlkDecryptFile() и VCERT_CmsBlkAttVerifyFile()	Расшифрование и проверка блочной присоединенной ЭП. Последовательный вызов функций Decrypt и Verify

2.10 Функции преобразования формата ЭП

Перечень функций преобразования формата ЭП, в том числе устаревших, приведен ниже в таблице (Таблица 13).

Таблица 11 – Функции преобразования формата ЭП

Устаревший прикладной интерфейс (заменяемый)	Новый прикладной интерфейс (заменяющий)	Примечание
Функция VCERT_AttachSignMem()	Функция VCERT_CmsBlkSignAttachMem()	Присоединение блочной ЭП к подписанному CMS сообщению
Функция VCERT_AttachSignFile()	Функция VCERT_CmsBlkSignAttachFile()	Присоединение блочной ЭП к подписанному CMS сообщению
Функция VCERT_DetachSignMem()	Функция VCERT_CmsBlkSignDetachMem()	Отсоединение блочной ЭП от подписанного CMS сообщения
Функция VCERT_DetachSignFile()	Функция VCERT_CmsBlkSignDetachFile()	Отсоединение блочной ЭП от подписанного CMS сообщения
Отсутствует	Функции VCERT_CmsStrSignDetachInitMem() VCERT_CmsStrSignDetachUpdateMem() VCERT_CmsStrSignDetachFinalMem()	Отсоединение потоковой ЭП от подписанного CMS сообщения. Следует последовательно вызывать функции Init, Update (возможно, несколько раз), Final

Устаревший прикладной интерфейс (заменяемый)	Новый прикладной интерфейс (заменяющий)	Примечание
Отсутствует	Функция VCERT_CmsStrSignDetachFile()	Отсоединение потоковой ЭП от подписанного CMS сообщения

2.11 Функции импорта и экспорта

Перечень функций импорта и экспорта, в том числе устаревших, приведен ниже в таблице (Таблица 14).

Таблица 12 – Функции импорта и экспорта

Устаревший прикладной интерфейс (заменяемый)	Новый прикладной интерфейс (заменяющий)	Примечание
Флаг FLAG_IMPORT_UI	Флаг FLAG_IMPORT_DISPLAYOBJECTUI	Замена произведена для повышения читаемости идентификатора
Флаг FLAG_IMPORT_CERTIFICATE	Флаг FLAG_IMPORT_CERTDERPEMFORMAT	Замена произведена для повышения читаемости идентификатора
Флаг FLAG_IMPORT_CRL	Флаг FLAG_IMPORT_CRLDERPEMFORMAT	Замена произведена для повышения читаемости идентификатора
Флаг FLAG_IMPORT_MY_CERTIFICATE	Флаг FLAG_IMPORT_CERTWITHPRIVATE	Замена произведена для повышения читаемости идентификатора
Флаг FLAG_IMPORT_UPDATE	Флаг FLAG_IMPORT_SIGNEDCARAUPDATE	Замена произведена для повышения читаемости идентификатора
Отсутствует	Флаг FLAG_IMPORT_DONOTVERIFYCHAIN	Импортировать объект (сертификат или САС) без построения и проверки его цепочки
Отсутствует	Флаг FLAG_IMPORT_FORCEREMOTESTORE	Импортировать объект (сертификат или САС) в сетевой справочник сертификатов
Структура add_param_t	Структура import_param_t	В структуре import_param_t следует установить флаг в зависимости от типа импортируемого

Устаревший прикладной интерфейс (заменяемый)	**Новый прикладной интерфейс (заменяющий)**	**Примечание**
		объекта
Функция VCERT_AddCertificate()	Функция VCERT_ImportMem()	Задать флаг импорта FLAG_IMPORT_CERTDERPEMFORMAT
Функция VCERT_AddCRL()	Функция VCERT_ImportMem()	Задать флаг импорта FLAG_IMPORT_CRLDERPEMFORMAT
Флаг FLAG_EXPORT_UI	Флаг FLAG_EXPORT_SHOWREQUESTUI	Замена произведена для повышения читаемости идентификатора
Флаг FLAG_EXPORT_ASN1	Флаг FLAG_EXPORT_PUREDERFORMAT	Замена произведена для повышения читаемости идентификатора
Флаг FLAG_EXPORT_NEWREQUEST	FLAG_EXPORT_PKCS10REQUEST	Замена произведена для повышения читаемости идентификатора
Флаг FLAG_EXPORT_REVREQUEST	FLAG_EXPORT_REVOKEREQUEST	Замена произведена для повышения читаемости идентификатора
Флаг FLAG_EXPORT_GOST_R_34_10_2001	Отсутствует	В Криптографических средствах 6 поколения генерация ключей ЭП и закрытых ключей шифрования по ГОСТ Р 34.10-2001 запрещена
Флаг FLAG_EXPORT_GOST_R_34_10_2012	Флаг FLAG_EXPORT_GOST_R_34_10_12_256	Замена произведена для повышения читаемости идентификатора
Отсутствует	Флаг FLAG_EXPORT_GOST_R_34_10_12_512	Выполнить генерацию ключа ЭП и/или закрытого ключа шифрования по ГОСТ Р 34.10-2012 (512 бит)
Отсутствует	Флаг FLAG_EXPORT_CARRIER_GENERATION	При генерации ключа ЭП и/или закрытого ключа шифрования на ФКН «Валидата vdToken» формировать закрытый ключ внутри ФКН ***«Валидата***

Устаревший прикладной интерфейс (заменяемый)	Новый прикладной интерфейс (заменяющий)	Примечание
		vdToken» с датчиком случайных чисел. ***Поддерживается только для ключевого носителя ФКН «Валидата vdToken» версия 2***

2.12 Функции поиска сертификатов

Перечень функций поиска сертификатов, в том числе устаревших, приведен ниже в таблице (Таблица 15).

Таблица 13 – Функции поиска сертификатов

Устаревший прикладной интерфейс (заменяемый)	Новый прикладной интерфейс (заменяющий)	Примечание
Флаг FLAG_FIND_MY	Флаг FLAG_FIND_CERTWITHPRIVATE	Замена произведена для повышения читаемости идентификатора
Флаг FLAG_FIND_REMOTE	Флаг FLAG_FIND_USEREMOTESEARCH	Замена произведена для повышения читаемости идентификатора
Флаг FLAG_FIND_SELECTUI	Флаг FLAG_FIND_SHOWUISELECTOR	Замена произведена для повышения читаемости идентификатора
Флаг FLAG_FIND_NOTIMECHECK	Флаг FLAG_FIND_DONOTCHECKTIMES	Замена произведена для повышения читаемости идентификатора
Флаг FLAG_FIND_NOVERIFY	Флаг FLAG_FIND_DONOTVERIFYCHAIN	Замена произведена для повышения читаемости идентификатора
Флаг FLAG_FIND_ADD_LDAP2LOCAL	Флаг FLAG_FIND_ADDREMOTETOLOCAL	Замена произведена для повышения читаемости идентификатора
Флаг FLAG_FIND_NOKEYTIMECHECK	Флаг FLAG_FIND_DONOTCHECKKEYTIME	Замена произведена для повышения читаемости идентификатора
Флаг FLAG_FIND_PARTIAL_SUBJECT	Флаг FLAG_FIND_SUBJECTISPARTIAL	Замена произведена для повышения читаемости идентификатора

Устаревший прикладной интерфейс (заменяемый)	Новый прикладной интерфейс (заменяющий)	Примечание
Флаг FLAG_FIND_IGNORE_CACHED	Флаг FLAG_FIND_IGNORESTORECACHE	Замена произведена для повышения читаемости идентификатора
Флаг FLAG_FIND_IGNORE_LOCAL	Флаг FLAG_FIND_IGNORESTORELOCAL	Замена произведена для повышения читаемости идентификатора
Флаг FLAG_FIND_SUBJECT_ATTRIBUTE	Флаг FLAG_FIND_SUBJECTATTRIBUTE	Замена произведена для повышения читаемости идентификатора

2.13 Функции построения и проверки цепочек

Перечень функций построения и проверки цепочек, в том числе устаревших, приведен ниже в таблице (Таблица 16).

Таблица 14 – Функции построения и проверки цепочек

Устаревший прикладной интерфейс (заменяемый)	Новый прикладной интерфейс (заменяющий)	Примечание
Флаг FLAG_POLICY_NOTIMECHECK	Флаг FLAG_POLICY_DONOTCHECKTIMES	Замена произведена для повышения читаемости идентификатора
Флаг FLAG_POLICY_VERIFY_CRL	Флаг FLAG_POLICY_DOCRLVERIFICATION	Замена произведена для повышения читаемости идентификатора
Флаг FLAG_POLICY_NOKEYTIMECHECK	Флаг FLAG_POLICY_DONOTCHECKKEYTIME	Замена произведена для повышения читаемости идентификатора

2.14 Функции штампов времени

Перечень функций штампов времени, в том числе устаревших, приведен ниже в таблице (Таблица 17).

Таблица 15 – Функции штампов времени

Устаревший прикладной интерфейс (заменяемый)	Новый прикладной интерфейс (заменяющий)	Примечание
Флаг FLAG_TSP_REQUEST_ADD_NONCE	Флаг FLAG_TSP_REQUEST_INCLUDENONCE	Замена произведена для повышения читаемости

Устаревший прикладной интерфейс (заменяемый)	Новый прикладной интерфейс (заменяющий)	Примечание
		идентификатора
Флаг FLAG_TSP_REQUEST_CERT_REQUEST	Флаг FLAG_TSP_REQUEST_ATTACHEDSIGNER	Замена произведена для повышения читаемости идентификатора
Флаг FLAG_TSP_RESPONSE_ADD_TSA_NAME	Флаг FLAG_TSP_RESPONSE_INCLUDETSANAME	Замена произведена для повышения читаемости идентификатора
Флаг FLAG_TSP_VERIFY_NOATTACHEDCERT	Флаг FLAG_TSP_VERIFY_IGNOREATTACHEDSIGNER	Замена произведена для повышения читаемости идентификатора
Функция VCERT_TspRequestFromPkcs7()	Функция VCERT_TspBlkRequestFromCmsMem()	Создание запроса на получение штампа времени для блочной ЭП
Функция VCERT_TspUrlStampPkcs7Mem()	Функция VCERT_TspBlkUrlStampCmsMem()	Получение штампа времени для блочной ЭП на указанном сервере
Функция VCERT_TspUrlStampPkcs7File()	Функция VCERT_TspBlkUrlStampCmsFile()	Получение штампа времени для блочной ЭП на указанном сервере
Отсутствует	Функции VCERT_TspStrUrlStampCmsInitMem() VCERT_TspStrUrlStampCmsUpdateMem() VCERT_TspStrUrlStampCmsFinalMem()	Получение штампа времени для потоковой ЭП на указанном сервере. Следует последовательно вызывать

Устаревший прикладной интерфейс (заменяемый)	Новый прикладной интерфейс (заменяющий)	Примечание
		функции Init, Update (возможно, несколько раз), Final
Отсутствует	Функция VCERT_TspStrUrlStampCmsFile()	Получение штампа времени для потоковой ЭП на указанном сервере
Функция VCERT_TspVerifyPkcs7Mem()	Функция VCERT_TspBlkVerifyCmsMem()	Проверка штампа времени для блочной ЭП
Функция VCERT_TspVerifyPkcs7File()	Функция VCERT_TspBlkVerifyCmsFile()	Проверка штампа времени для блочной ЭП
Отсутствует	Функции VCERT_TspStrVerifyCmsInitMem() VCERT_TspStrVerifyCmsUpdateMem() VCERT_TspStrVerifyCmsFinalMem	Проверка штампа времени для потоковой ЭП. Следует последовательно вызывать функции Init, Update (возможно, несколько раз), Final
Отсутствует	Функция VCERT_TspStrVerifyCmsFile()	Проверка штампа времени для потоковой ЭП

2.15 Функции протокола TLS

Перечень функций протокола TLS, в том числе устаревших, приведен ниже в таблице (Таблица 18).

Таблица 16 – Функции протокола TLS

Устаревший прикладной интерфейс (заменяемый)	Новый прикладной интерфейс (заменяющий)	Примечание
Флаг FLAG_TLS_CLIENT_SESSION	Флаг FLAG_TLS_CREAT_CLIENT_SESSION	Замена произведена для повышения читаемости идентификатора
Флаг FLAG_TLS_NO_RESUME_ON_RENEGO	Флаг FLAG_TLS_NO_RENEGO_RESUMPTION	Замена произведена для повышения читаемости идентификатора
Флаг FLAG_TLS_ALLOW_UNSAFE_RENEGO	Флаг FLAG_TLS_ENABLE_UNSAFE_RENEGO	Замена произведена для повышения читаемости идентификатора
Константа VCERT_TLS_QUERY_PEER_CERTIF	Константа VCERT_TLS_QRY_PEER_CERTIF_BLOB	Замена произведена для повышения читаемости идентификатора

2.16 Вспомогательные функции

Перечень вспомогательных функций, в том числе устаревших, приведен ниже в таблице (Таблица 19).

Таблица 17 – Вспомогательные функции

Устаревший прикладной интерфейс (заменяемый)	Новый прикладной интерфейс (заменяющий)	Примечание
Функция VCERT_GetErrorLine()	Функция VCERT_GetErrorLineEx()	Заменяющая функция позволяет получать дополнительные диагностические данные, связанные с возникшей ошибкой

2.17 Коды ошибок

Перечень кодов ошибок, в том числе устаревших, приведен ниже в таблице (Таблица 20).

Таблица 18 – Коды ошибок

Устаревший прикладной интерфейс (заменяемый)	Новый прикладной интерфейс (заменяющий)	Примечание
Константа VCERT_E_HASH	Константа VCERT_E_DIGEST	Замена произведена для повышения

Устаревший прикладной интерфейс (заменяемый)	Новый прикладной интерфейс (заменяющий)	Примечание
		читаемости идентификатора
Константа VCERT_E_PKCS7_SET_TYPE	Отсутствует	Данный код ошибки не возвращается в Криптографических средствах 6 поколения
Константа VCERT_E_PKCS7_ADD_SIGNATURE	Константа VCERT_E_CMS_ADD_SIGNATURE	Замена произведена для повышения читаемости идентификатора
Константа VCERT_E_PKCS7_ADD_CERTIFICATE	Отсутствует	Данный код ошибки не возвращается в Криптографических средствах 6 поколения
Константа VCERT_E_PKCS7_CONTENT_NEW	Отсутствует	Данный код ошибки не возвращается в Криптографических средствах 6 поколения
Константа VCERT_E_PKCS7_D2I	Константа VCERT_E_CMS_ASN1_DECODE	Замена произведена для повышения читаемости идентификатора
Константа VCERT_E_PKCS7_I2D	Константа VCERT_E_CMS_ASN1_ENCODE	Замена произведена для повышения читаемости идентификатора
Константа VCERT_E_PKEY_NOT_GOST	Отсутствует	Данный код ошибки не возвращается в Криптографических средствах 6 поколения
Константа VCERT_E_SIGN	Константа VCERT_E_SIGN_HASH	Замена произведена для повышения читаемости идентификатора
Константа VCERT_E_PKCS7_READ	Отсутствует	Данный код ошибки не возвращается в

Устаревший прикладной интерфейс (заменяемый)	Новый прикладной интерфейс (заменяющий)	Примечание
		Криптографических средствах 6 поколения
Константа VCERT_E_REQ_DAMAGED	Константа VCERT_E_PKCS10_DAMAGED	Замена произведена для повышения читаемости идентификатора
Константа VCERT_E_VERIFY_FORMAT	Отсутствует	Данный код ошибки не возвращается в Криптографических средствах 6 поколения
Константа VCERT_E_DELETE_SIGN	Отсутствует	Данный код ошибки не возвращается в Криптографических средствах 6 поколения
Константа VCERT_E_PKCS7_SET_CIPHER	Отсутствует	Данный код ошибки не возвращается в Криптографических средствах 6 поколения
Константа VCERT_E_PKCS7_SET_CIPHER_INFO	Отсутствует	Данный код ошибки не возвращается в Криптографических средствах 6 поколения
Константа VCERT_E_PKCS7_ADD_RECIPIENT	Отсутствует	Данный код ошибки не возвращается в Криптографических средствах 6 поколения
Константа VCERT_E_PKCS7_ENCRYPT	Отсутствует	Данный код ошибки не возвращается в Криптографических средствах 6 поколения
Константа VCERT_E_PKCS7_WRONG_TYPE	Константа VCERT_E_CMS_INVALID_TYPE	Замена произведена для повышения читаемости

Устаревший прикладной интерфейс (заменяемый)	Новый прикладной интерфейс (заменяющий)	Примечание
		идентификатора
Константа VCERT_E_EVP_GET_CIPHER	Отсутствует	Данный код ошибки не возвращается в Криптографических средствах 6 поколения
Константа VCERT_E_DECRYPT_NO_RECIPIENTS	Константа VCERT_E_CMS_NO_RECIPIENTS	Замена произведена для повышения читаемости идентификатора
Константа VCERT_E_DECRYPT_NO_SENDER	Отсутствует	Данный код ошибки не возвращается в Криптографических средствах 6 поколения
Константа VCERT_E_DECRYPT_NO_RECIPIENT	Константа VCERT_E_CMS_NOT_RECIPIENT	Замена произведена для повышения читаемости идентификатора
Константа VCERT_E_PKCS7_DECRYPT	Константа VCERT_E_CMS_KEY_DECRYPT	Замена произведена для повышения читаемости идентификатора
Константа VCERT_E_DECRYPT	Константа VCERT_E_DATA_DECRYPT	Замена произведена для повышения читаемости идентификатора
Константа VCERT_E_OPEN_PSE	Константа VCERT_E_OPEN_PSESTORE	Замена произведена для повышения читаемости идентификатора
Константа VCERT_E_NO_STREAM_DATA	Отсутствует	Данный код ошибки не возвращается в Криптографических средствах 6 поколения
Константа VCERT_E_BAD_STREAM_EOC	Отсутствует	Данный код ошибки не возвращается в Криптографических средствах 6

Устаревший прикладной интерфейс (заменяемый)	Новый прикладной интерфейс (заменяющий)	Примечание
		поколения
Константа VCERT_E_OPENKEY_NOT_FOUND	Константа VCERT_E_PUBKEY_NOT_FOUND	Замена произведена для повышения читаемости идентификатора
Константа VCERT_E_REQ_NOT_FOUND	Отсутствует	Данный код ошибки не возвращается в Криптографических средствах 6 поколения
Константа VCERT_E_PKCS7_WRONG_ALGORITHM	Отсутствует	Данный код ошибки не возвращается в Криптографических средствах 6 поколения
Константа VCERT_E_SIGNLEN	Отсутствует	Данный код ошибки не возвращается в Криптографических средствах 6 поколения
Константа VCERT_E_DECRYPT_FORMAT	Константа VCERT_E_CMS_NOT_ENCRYPTED	Замена произведена для повышения читаемости идентификатора
Константа VCERT_E_FILE_MAPPING	Отсутствует	Данный код ошибки не возвращается в Криптографических средствах 6 поколения
Константа VCERT_E_INSUFFICIENT_SIGNS	Константа VCERT_E_TOO_FEW_SIGNATURES	Замена произведена для повышения читаемости идентификатора
Константа VCERT_E_VERIFY_CRL	Отсутствует	Данный код ошибки не возвращается в Криптографических средствах 6 поколения
Константа VCERT_E_REQ_NEW	Константа VCERT_E_PKCS10_CREATE	Замена произведена для повышения

Устаревший прикладной интерфейс (заменяемый)	Новый прикладной интерфейс (заменяющий)	Примечание
		читаемости идентификатора
Константа VCERT_E_REQ_SIGN	Константа VCERT_E_PKCS10_SIGN	Замена произведена для повышения читаемости идентификатора
Константа VCERT_E_MAKE_REVREQ	Константа VCERT_E_REVREQ_CREATE	Замена произведена для повышения читаемости идентификатора
Константа VCERT_E_SIGN_REVREQ	Константа VCERT_E_REVREQ_SIGN	Замена произведена для повышения читаемости идентификатора
Константа VCERT_E_PKCS7_DATA_INIT	Отсутствует	Данный код ошибки не возвращается в Криптографических средствах 6 поколения
Константа VCERT_E_BIO_WRITE	Отсутствует	Данный код ошибки не возвращается в Криптографических средствах 6 поколения
Константа VCERT_E_RESIGN_PROHIBIT	Отсутствует	Данный код ошибки не возвращается в Криптографических средствах 6 поколения
Константа VCERT_E_TSP_RESP_D2I	Константа VCERT_E_TSP_RESP_ASN1_DECODE	Замена произведена для повышения читаемости идентификатора
Константа VCERT_E_OCSP_RESP_D2I	Константа VCERT_E_OCSP_RESP_ASN1_DECODE	Замена произведена для повышения читаемости идентификатора