Описание функциональных характеристик программного обеспечения «Эникриптер».

Программное обеспечение «Эникриптер» соответствует всем требованиям российского законодательства в части обеспечения юридически значимого статуса и может использоваться для подписания котировочных заявок, банковских гарантий, межевых планов, алкогольных деклараций, различных соглашений, договоров, контрактов и других документов.

Поддерживаемый набор функций ПО «Эникриптер»:

ПО «Эникриптер» позволяет шифровать и расшифровывать любое количество файлов любого размера.

ПО «Эникриптер» позволяет осуществлять электронную подпись файлов.

ПО «Эникриптер» применяется в том случае, когда требуется защитить данные от постороннего доступа, обеспечить доказательства подлинности и авторства электронных документов, согласовывать электронные документы, гарантировать целостность данных при отправке по каналам связи и т.д.

В настоящее время программой поддерживается следующие технологии, параметры и алгоритмы защиты:

– ГОСТ 34.11-94/34.10-2001, 34.11/34.10-2012

– ГОСТ 28147-89

– штампы времени, CAdES, ocsp.

Шифрование

– ГОСТ 28147-89/ ТК 26 Z

– шифрование и расшифрование отдельных файлов, пакетов и архивов данных;

– размер шифруемых данных ограничен только файловой системой и доступным свободным местом;

– одновременное шифрование множества файлов;

– удаление исходного файла после шифрования;

– шифрование данных по стандарту PKCS#7, CMS;

– задание расширений выходных шифрованных файлов (по умолчанию - *.cr);

– задание расширений выходных расшифрованных файлов (по умолчанию - *.decr);

– специальная функция Сейф для создания списков защищённых файлов, зашифрованных на два ключа. Файлы могут быть восстановлены по специальному резервному ключу в случае утраты аппаратного.

Электронная подпись

– ГОСТ 3411/3410-2001, 3411/3410-2012

– поддержка улучшенной подписи CAdES;

– формирование подписи с использованием штампов времени (tsp/ocsp);

– электронная подпись отдельных файлов, пакетов данных и архивов;

– варианты электронной подписи: первичная, дополнительная (подпись документа несколькими лицами);

– классический формат электронной подписи;

– электронная подпись, отделенная от подписываемых данных и совмещенная с данными;

– размер подписываемых данных ограничен только файловой системой и доступным свободным местом;

– одновременная обработка множества файлов;

– задание расширений выходных файлов (по умолчанию - *.sgn и *.cosgn).

Возможности автоматизации работы с программой

– индивидуальные настройки, которые могут ускорить выполнение однотипных операций;

– криптографические операции «одним кликом»;

– возможность удаленного администрирования рабочего места в PKI инфраструктуре.

Модуль «Сейф» и его возможности

– удобный менеджер защиты собственных файлов на компьютере;

– расшифровка только при наличии закрытого ключа, например, брелка Рутокен;

Создание рабочих мест в инфраструктуре pki

– поддержка работы с Microsoft Certificate Authority и ПАК «КриптоПро УЦ»;

– использование в качестве рабочего места для взаимодействия с Удостоверяющим центром;

– просмотр информации и проверка текущего статуса цифрового сертификата;

– обновление списков отозванных сертификатов;

– импорт и экспорт сертификатов, запросов на сертификат, списков отзывов сертификатов;

– просмотр списка ключевых контейнеров.

Управление контейнерами и отчуждаемыми ключевыми носителями

– программа «Эникриптер» позволяет инициализировать ключевой носитель (ФКН), сменить пароль пользователя, сменить пароль администратора, сбросить счетчик неверных вводов PIN-кода пользователя.

При работе с CSP (КриптоПро, VipNet) данный функционал не доступен. CSP имеют свои интерфейсы для работы с ключевой информацией.

Модульная архитектура

– модуль «Клиент УЦ» включен в состав базового дистрибутива;

– модуль «Сейф» включен в состав базового дистрибутива;

– модуль «Управление отчуждаемыми ключевыми носителями» включен в состав базового дистрибутива.