КАРМА

Описание назначения и применение

©Электронные Офисные Системы. 2019 г.

Область применения КАРМА

Криптографический комплекс КАРМА (далее - КАРМА) - программное решение для использования криптографических функций, таких как шифрование, установка и проверка электронной цифровой подписи, в прикладных функциональных системах. КАРМА позволяет применять в прикладном программном обеспечении криптографические методы защиты информации, используя высокоуровневый интерфейс, не требующий специальных знаний в области криптографии, учёта особенностей использования различных криптографических провайдеров и оперирования специальными криптографическими объектами, такими как ключевые контейнеры, хэш-функции и прочее. Визуальная оболочка позволяет использовать КАРМА в качестве персонального АРМ для криптографической обработки файлов.

Системные требования

КАРМА предназначена для функционирования в операционных системах Microsoft Windows 2000SP4/XP/2003/Vista/7/8.1/10. Для установки и работы системы КАРМА необходимо также наличие Microsoft .NET Framework версии не ниже 4.0 (+ версия 3.5 для поддержка совместимости с приложениями CLR 2.0).

КАРМА обеспечивает работу со всеми криптопровайдерами, поддерживающими спецификацию Microsoft CryptoAPI 2.0, в том числе Microsoft Strong Cryptographic Provider, КриптоПро CSP, SignalCOM CSP, Верба-OW, Генкей SMARTCRYPTO CSP, Домен-К, Авест и другие.

Состав и назначение компонентов КАРМА

КАРМА состоит из следующих компонентов:

- сервис взаимодействия с криптопровайдером;
- библиотека объекта COM-интерфейса криптографических функций;
- библиотека объекта COM-интерфейса функций взаимодействия с инфраструктурой открытых ключей (PKI);
- библиотека .Net сборка CarmaCryptographySupport;
- графическая оболочка;
- функциональные расширения;
- сервисные утилиты (настройка, диагностика платформы);
- локальный веб-сервер(страницы настройки и тестирования функционала)

Сервис взаимодействия с криптопровайдером

Сервис взаимодействия с криптопровайдером представляет собой исполняемое приложение, непосредственно обращающееся к функциям криптопровайдера, обеспечивая корректный вызов последовательности криптографических операций для выполнения поставленной задачи. Сервис взаимодействия с криптопровайдером может работать в двух режимах – как запускаемое приложение и как системная служба (В режиме системной службы функциональность модуля ограничена функциями, не требующими предъявления секретного ключа, например: проверка подписи, получение реквизитов сертификата и т.п.). Сервис запускается и работает в системном

контексте, не зависимом от контекста прикладного ПО, использующего КАРМА, и может быть запущен от имени другого пользователя.

Библиотеки объектов COM-интерфейсов

Библиотеки объектов COM-интерфейсов криптографических функций и функций взаимодействия с инфраструктурой открытых ключей обеспечивают регистрацию в системе и использование прикладным программным обеспечением набора высокоуровневых функций для выполнения шифрования и расшифровывания данных, установку и проверку электронной цифровой подписи, работу с сертификатами открытых ключей. Функции библиотек вызываются посредством стандартного механизма COM через обращение к объектам EosCryptoSvc и EosPKISvc. Библиотеки объектов не содержат в себе механизмов обработки данных, они лишь формируют запрос к сервису взаимодействия с криптопровайдером, передают и получают данные. Обмен между библиотеками и сервисом производится по собственному протоколу, базирующемуся на механизме именованных каналов (Named Pipes), что позволяет сервису взаимодействия с криптопровайдером быть запущенным на произвольной удаленной машине (В данном режиме функциональность модуля ограничена функциями, не требующими предъявления секретного ключа, например: проверка подписи, получение реквизитов сертификата и т.п.).

Библиотека .Net сборка CarmaCryptographySupport

CarmaCryptographySupport является сборкой .Net (версии CLR 2.0 и 4.0), которая использует крипто-интерфейсы КАРМА и реализует работу с криптографическими данными, XmlDsig и XAdES подписями с поддержкой ГОСТ алгоритмов. Работа с сертификатами, подписями CMS (Cryptography Message Syntax), шифрование осуществлены через классы – «обертки», которые упрощают прикладной код и используют удобства среды .Net и языка C# в частности. В зависимости от версии библиотеки (3.0 \ 4.0) для взаимодействия используется либо COM – объекты, либо прямые запросы Http\NamedPipe.

Графическая оболочка

Графическая оболочка реализована в виде расширения контекстного меню Windows Explorer и позволяет применять криптографические операции к выбранным файлам. Система сохраняемых профилей позволяет производить операции с заранее определёнными параметрами.

Функциональные расширения

Функциональные расширения, такие как графическое факсимиле, расширение по работе с серверами штампов времени, позволяют добавлять новые возможности КАРМА и повышать её функциональность и удобство использования.

Сервисные утилиты

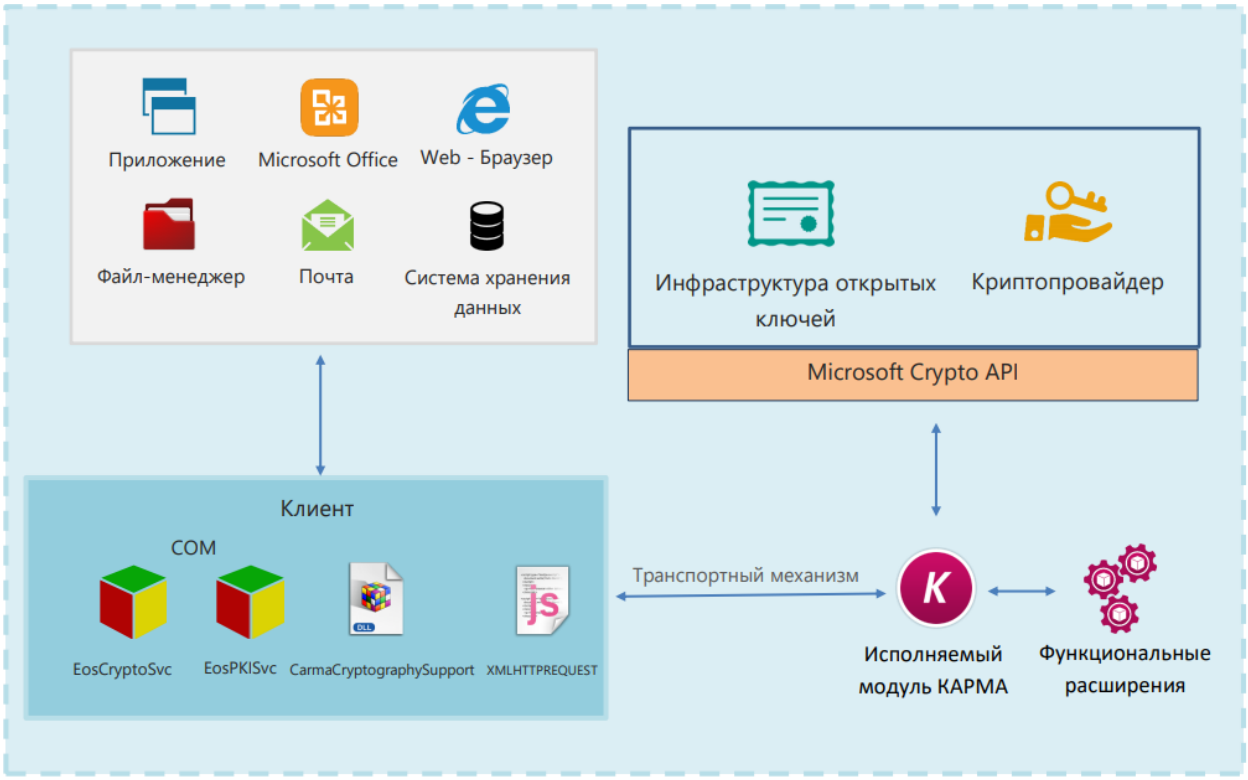
В комплект поставки КАРМА входят утилиты настройки режимов работы криптографического сервиса.

Локальный веб-сервер

После запуска сервиса КАРМА в браузере доступны следующие предопределенные страницы (порт Http по умолчанию 8080)

- http://localhost:8080/settings - страница редактирования настроек сервиса

- http://localhost:8080/test - страница тестирования функций сервиса

Доступ к API может быть осуществлен с помощью GET/POST запросов на адрес сервиса http://localhost:8080

Логическая схема работы КАРМА: