КриптоАРМ

Руководство по продажам (Sales Guide)

Аннотация: Данный документ предназначен для бизнес-партнёров компании "Цифровые технологии". Основной целью документа является предоставление информации о «КриптоАРМ», которая позволит Вам лучше, больше и эффективнее продавать «КриптоАРМ».

Версия: 1.1

Редакция от: 01.07.2014 г.

Количество страниц: 9

СОДЕРЖАНИЕ

1. Что такое КриптоАРМ? 3

2. Возможности КриптоАРМ 3

3. Возможности интеграции КриптоАРМ 5

4. Версии КриптоАРМ 6

5. Покупатели КриптоАРМ 6

6. Пользователи КриптоАРМ 8

7. Контактная информация 9

1. Что такое КриптоАРМ?

КриптоАРМ - программа для шифрования и электронной подписи файлов любого формата и размера (в т.ч. PDF, JPG, JPEG, PNG). Программа используется для подписания котировочных заявок, банковских гарантий, межевых планов, алкогольных деклараций, различных соглашений, договоров, контрактов и других документов.

Используется в тех информационных системах, в которых необходимо:

- надежно защитить данные от постороннего доступа;
- гарантировать целостность данных при отправке по незащищенным каналам связи;
- обеспечить подлинность и авторство электронных документов;
- согласовывать электронные документы с коллегами.

2. Возможности КриптоАРМ

Шифрование

- шифрование и расшифрование отдельных файлов, пакетов и архивов данных;
- размер шифруемых данных ограничен только файловой системой и доступным свободным местом;
- одновременное шифрование неограниченного количества файлов;
- удаление исходного файла после шифрования, в т.ч. гарантированное удаление;
- шифрование данных по стандарту PKCS#7, CMS;
- задание расширений выходных файлов.

Электронная подпись

- электронная подпись отдельных файлов, пакетов данных и архивов;
- варианты электронной подписи: первичная, дополнительная (подпись документа несколькими лицами) и заверяющая (подпись вышестоящим сотрудником подписанного документа);
- применение расширенных свойств ЭП (время создания подписи, комментарий пользователя);
- классический и усовершенствованный форматы электронной подписи;
- два варианта подписи (отделенная от исходных данных и совмещенная с данными);
- удаление исходного файла после подписи, в т.ч. гарантированное удаление;
- размер подписываемых данных ограничен только файловой системой и доступным свободным местом;
- одновременная обработка неограниченного количества файлов;
- печать электронной подписи на бумажный носитель.

Надежное хранение ключевой информации

- для хранения ключевой информации “КриптоАРМ” поддерживает работу с USB-токенами и смарт-картами Rutoken S, Рутокен ЭЦП, eToken PRO (Java), eToken ГОСТ, JaCarta PKI, Магистра CSP, КриптоПро Рутокен CSP, КриптоПро eToken CSP, УЭК, ESMART Token

Удостоверение точного времени подписи электронных документов

- Электронная подпись со штампом времени;
- просмотр и проверка штампа времени на подписанном документе;
- просмотр и проверка штампа времени на подписи.

Длительное (архивное) хранение электронных документов, подписанных усовершенствованной электронной подписью

- поддержка стандарта CAdES X Long (усовершенствованная ЭП);
- доказательство момента подписи документа и действительность сертификата ключа подписи на этот момент статусов при создании подписи и проверке ее корректности;
- возможность доказательства корректности ЭП и целостности файла даже после истечения срока действия сертификата подписи.

Автоматизация работы с программой

- индивидуальные настройки, которые ускоряют однотипные операции;
- криптографические операции «одним кликом»;
- возможность удаленного администрирования рабочего места в PKI инфраструктуре.

Встраивание криптографии в информационные системы

- свободное распространение “КриптоАРМ SDK”;
- подробное руководство для разработчиков с описанием характеристик, функций программы, а также примерами использования основных операций;
- поддержка международных стандартов и рекомендаций в области защиты информации (X.509v1, v3, PKCS#7, PKCS#11, CMS, CAdES);
- предпроектный и проектный консалтинг со стороны специалистов в области защиты информации и электронной подписи;
- техническая поддержка и сопровождение проектов.

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, запроса;
- обновление списков отозванных сертификатов производится по всем удостоверяющим центрам (как корневому, так и промежуточным), входящим в путь сертификации проверяемого сертификата;
- печать на бумажный носитель информации о сертификате, запросе;
- импорт и экспорт сертификатов, запросов, списков;
- работа со справочником назначений сертификатов;
- просмотр списка ключевых контейнеров.
- поддержка хранилища цифровых сертификатов для Active Directory

Поддержка различных криптопровайдеров (CSP) и управление ими

- Стандарт Microsoft CryptoAPI 2.0: “КриптоПро CSP”, "КриптоПро УЭК CSP", “ViPNet CSP”, ”SignalCOM CSP”, “AVEST CSP”, “Tumar CSP”, базовые криптопровайдеры Microsoft;
- Стандарт PKCS#11: криптопровадеры на токенах "eToken ГОСТ", "JaCarta ГОСТ", "Рутокен ЭЦП";
- просмотр списка установленных и разрешенных к использованию криптопровайдеров и их параметров;
- просмотр и фильтрация списка криптопровайдеров.

Модульная архитектура

- модуль TSP предназначен для удостоверения точного времени создания электронных документов с помощью штампов времени;
- модуль OCSP предназначен для получения в реальном времени информации о статусе цифровых сертификатов;
- модули TSP и OCSP включены в состав комплекта «КриптоАРМ СтандартPRO»;

3. Возможности интеграции КриптоАРМ

Программа «КриптоАРМ» может применяться как основа для встраивания криптографических функций. В состав стандартной комплектации программы входит библиотека для разработчиков «КриптоАРМ SDK», в которой описаны способы интеграции программы с внешними приложениями на уровне программного кода, приведены характеристики функций и примеры их использования.

Интеграция возможна в следующих информационных системах:

- системы электронного документооборота (СЭД);
- прикладные системы для бухгалтерского, финансового и управленческого учета;
- автоматизированные информационные системы (АИС) обработки, хранения, обмена электронных документов;
- веб-сервисы и веб-порталы: отчетность в госорганы, электронные закупки, обмен документами в сети Интернет.

Внедрение криптографических функций (электронная подпись, шифрование) в информационные системы с использованием программы «КриптоАРМ» дает следующие преимущества:

- соответствие требованиям Федерального законодательства в защите информации и применению электронной подписи;
- поддержка международных стандартов и рекомендаций в области защиты информации и криптографии;
- постоянное развитие возможностей программного обеспечения;
- техническая поддержка и сопровождение;
- индивидуальный консалтинг заказчиков со стороны разработчиков ПО.

4. Версии КриптоАРМ

«КриптоАРМ Старт» версии 5 - бесплатная версия программы. Разрешает подписывать и шифровать файлы с применением базовых криптопровайдеров Microsoft. Также поддерживает возможность проверки подписи на ГОСТ алгоритмах (для КриптоПро CSP).

«КриптоАРМ Стандарт» версии 5 – наиболее популярная версия программы. Предназначена для подписи и шифрования электронных документов, поддерживает российские ГОСТ алгоритмы подписи и шифрования (КриптоПРО CSP, КриптоПро УЭК CSP, ViPNet CSP, Signal-COM CSP).

«КриптоАРМ Стандарт Плюс» версии 5 - расширенная версия программы. В отличие от стандартной версии дополнительно поддерживает работу с аппаратными криптографическими устройствами с интерфейсом PKCS#11 (eToken ГОСТ, JaCarta ГОСТ, Рутокен ЭЦП).

«КриптоАРМ Терминал» версии 5 - версия программы для работы в режиме терминального сервера, которая позволяет установить программу на одном рабочем месте и предоставить доступ пользователям внутренней локальной сети.

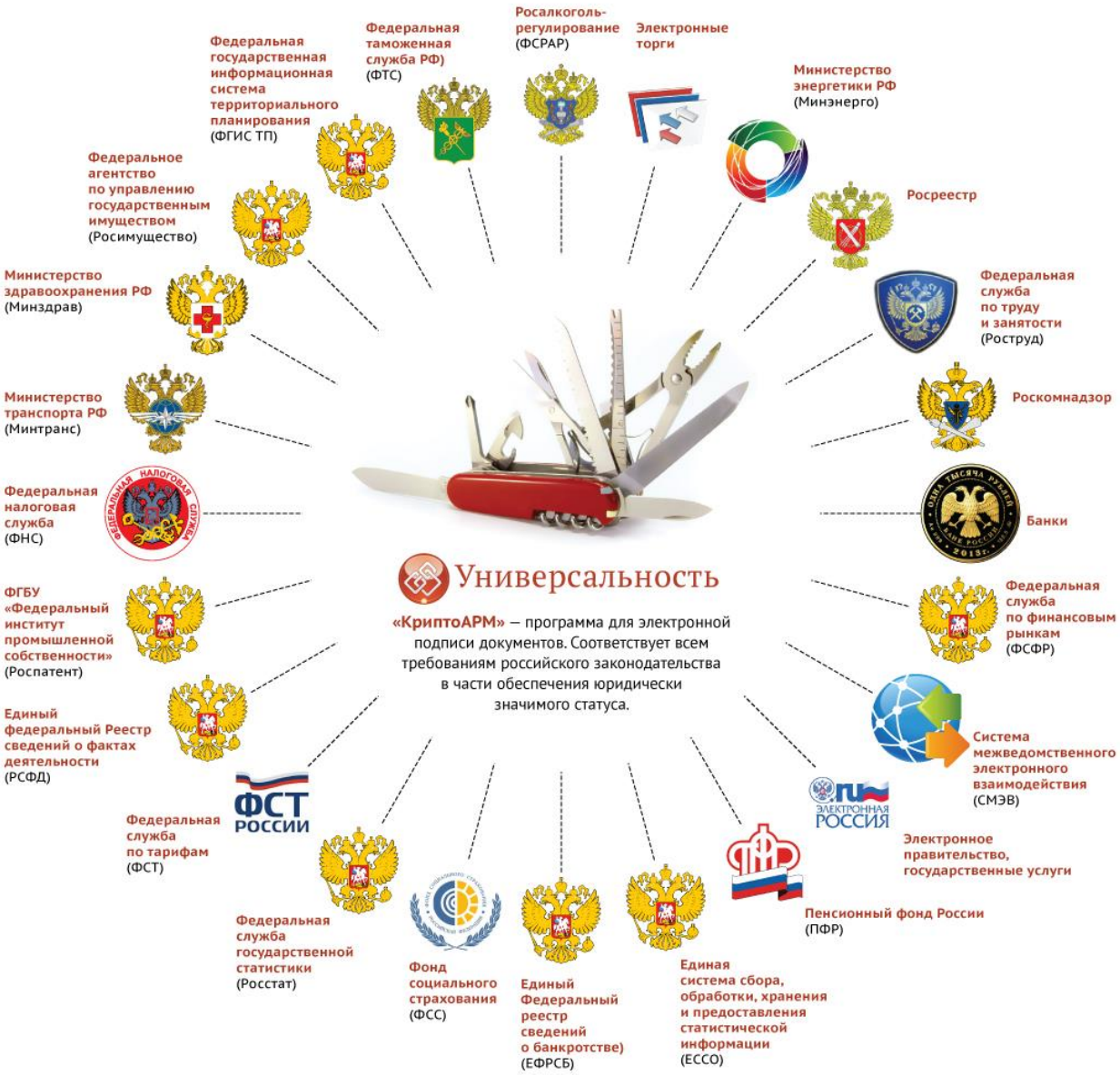
«КриптоАРМ Сервер» версии 5 - версия программы для работы на серверных системах без ограничения количества пользователей, которые будут использовать программу для шифрования или электронной подписи.

СКЗИ «КриптоАРМ Стандарт» версии 4 – сертифицированная версия программы, имеет сертификат соответствия требованиям ФСБ России к СКЗИ класса КС 1 и может использоваться для криптографической защиты информации, не содержащей сведений, составляющих государственную тайну. Необходимо наличие эталонного дистрибутива.

СКЗИ «КриптоАРМ Стандарт PRO» версии 4 – сертифицированная версия программы, предназначена для работы с усовершенствованной квалифицированной подписью. Позволяет организовать длительное хранение электронных документов с сохранением их юридической силы. В состав входят модули «КриптоПро TSP Client» и «КриптоПро OCSP Client». Необходимо наличие эталонного дистрибутива.

5. Покупатели КриптоАРМ

Согласно анализу продаж «КриптоАРМ» за 2013 год, проведенному компанией «Цифровые технологии», благодаря своей универсальности, программа пользуется спросом, как в государственном, так и в коммерческом, а также частном сегменте. Ниже приведено описание целевой аудиторий программы «КриптоАРМ»



«КриптоАРМ» используется для подписания различных документов:

*** Для предоставления межевых планов в орган кадастрового учёта;**
*** Для предоставления деклараций в Росалкогольрегулирование (ФСРАР);**
*** Для участия в запросах котировок;**
*** Для получения банковских гарантий;**
*** Для заключения соглашений, договоров, контрактов;**
*** Для подачи запроса на выгрузку из Единого реестра запрещенных сайтов;**
*** Для предоставления энергетических паспортов в Минэнерго.**

В отдельных регионах «КриптоАРМ» используется:

*** ТФОМС Брянской области.** Медицинские организации Брянской области используют решение «eToken КриптоАРМ» для подписания квалифицированной подписью отчетных финансовых документов для территориального фонда обязательного медицинского страхования.

*** Абитуриентами для подачи документов в СыктГУ.** В 2014 году Сыктывкарский государственный университет в качестве эксперимента при помощи программы «КриптоАРМ» реализовал возможность подавать абитуриентам документы для поступления в ВУЗ в электронном виде, используя электронную подпись.
*** Службой занятости Йошкар-Олы.** Работодатели Йошкар-Олы имеют возможность предоставлять информацию в центр занятости населения с применением электронной подписи: сведения о потребности в работниках, наличии свободных рабочих мест, о выполнении квоты по трудоустройству инвалидов и др.
*** УФМС по Астраханской области.** Гостиницы, отели, санатории и пансионаты обязаны предоставлять информацию об отдыхающих на их территории иностранных граждан в Федеральную миграционную службу. При передаче данных в электронном виде необходимо подписание и шифрование, которое организуется при помощи программы «КриптоАРМ».
*** Органами ЗАГС Волгоградской области.** Передача органами записи актов гражданского состояния сведений о государственной регистрации рождения и смерти может осуществляться как на бумажном носителе, так и в форме электронного документа, подписанного уполномоченным должностным лицом органа записи актов гражданского состояния усиленной квалифицированной электронной подписью.
*** Нотариальными палатами.** При работе с персональными данными в электронном виде нотариусы обязаны использовать квалифицированную электронную подпись. Таким образом, нотариусы имеют возможность осуществлять передачу сведений в единую информационную систему нотариата России в электронном виде.
* **Бюро кредитных историй.** Микрофинансовые организации и кредитные кооперативы при выдаче займов и кредитов физическим лицам подают соответствующую информацию в БКИ в шифрованном виде.

6. Пользователи КриптоАРМ

В настоящее время на территории Российской Федерации реализовано свыше 300 000 лицензий «КриптоАРМ» различных версий. Программа используется в различных государственных и корпоративных информационных системах. Защиту электронных данных программе «КриптоАРМ» доверили:
* Государственная Дума Российской Федерации
* Счетная палата Российской Федерации
* Министерство внутренних дел Российской Федерации
* Министерство обороны Российской Федерации
* Министерство энергетики Российской Федерации
* Федеральная налоговая служба Российской Федерации
* Федеральная таможенная служба Российской Федерации
* Федеральная служба по регулированию алкогольного рынка
* Федеральная служба государственной регистрации, кадастра и картографии
* Федеральная служба по финансовым рынкам
* Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций
* Федеральный фонд обязательного медицинского страхования
* ОАО «АК БАРС» БАНК

* ОАО «АЛЬФА-БАНК»
* ЗАО «Банк Русский Стандарт»
* ОАО «Газпромбанк»
* ООО «Хоум Кредит энд Финанс Банк»
* ЗАО «Связной Банк»
* ОАО АКБ «Связь Банк»
* ОАО "ОТП Банк"
* ОАО «Финансовая корпорация «УРАЛСИБ»
* ОАО «Национальное бюро кредитных историй»
* ОАО «УЭК»

7. Контактная информация

ООО «Цифровые технологии»
Адрес: 424033, Россия, Республика Марий Эл, г. Йошкар-Ола, ул. Петрова, д.1
Телефон: 8 (8362) 33-70-50, 8(800)555-65-81
Электронная почта: info@trusted.ru
Сайт: www.trusted.ru