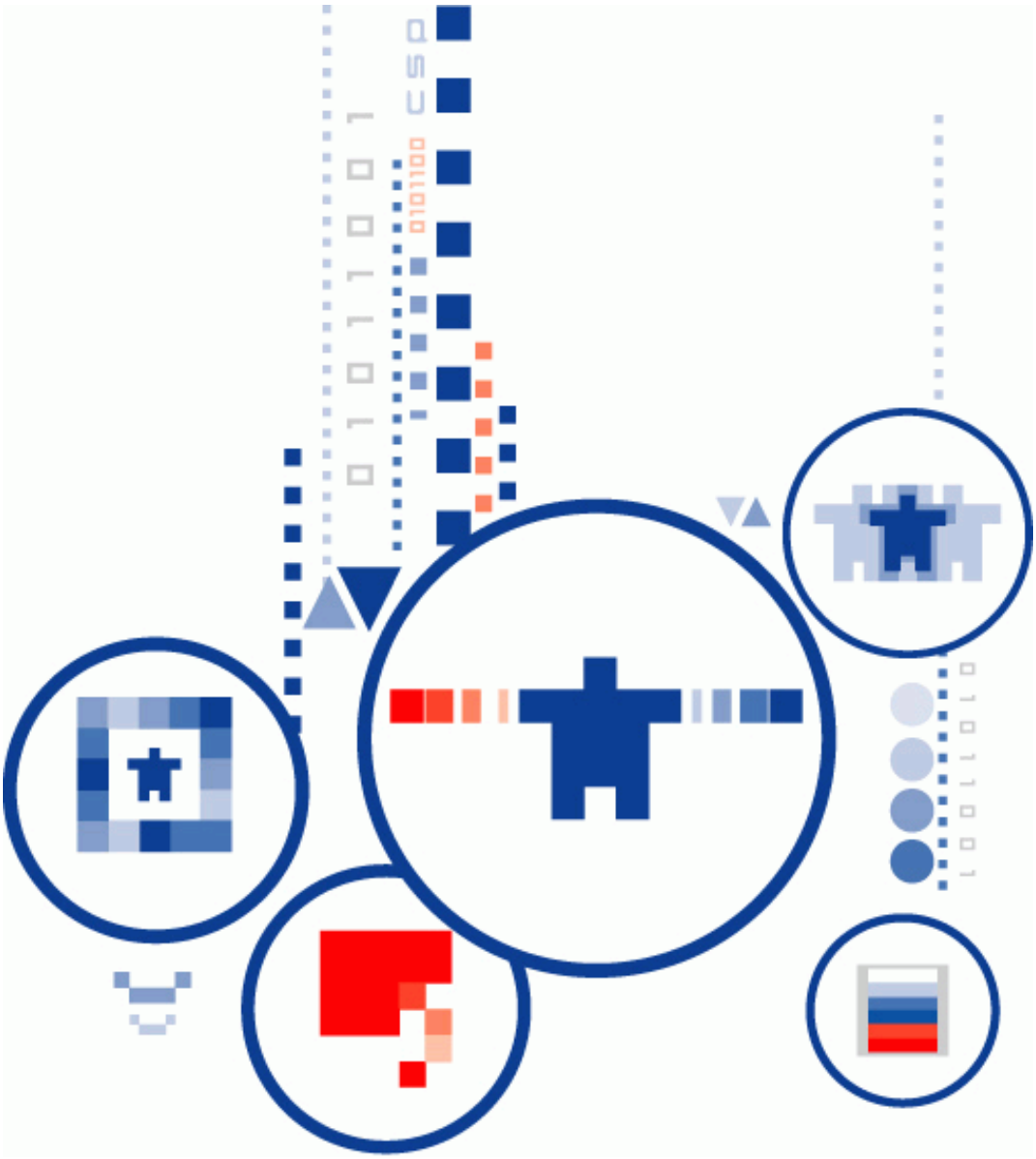

Сервер Электронной Подписи «КриптоПро DSS»

Компонент ПАКМ «КриптоПро HSM»

DSS Lite. Инструкция по использованию

ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ И ОБОЗНАЧЕНИЯ

CRL	—	Список отзыва сертификатов (Certificate Revocation List)
CSP	—	Криптопровайдер (Cryptographic Service Provider)
HSM	—	Аппаратный модуль системы безопасности (Hardware security module)
OCSP	—	Протокол получения статуса сертификата в реальном времени (Online Certificate Status Protocol)
OTP	—	Пароль, действительный только для одного сеанса аутентификации (One-Time Password)
SOAP	—	Простой протокол доступа к объектам (Simple Object Access Protocol)
SSL	—	Протокол защиты сокетов (Secure Sockets Layer)
TLS	—	Протокол защиты транспортного уровня (Transport Layer Security)
БД	—	База данных
ИС	—	Информационная система
СУБД	—	Система управления базой данных
ОС	—	Операционная система
ПО	—	Программное обеспечение
СКЗИ	—	Средство криптографической защиты информации
СЭП	—	Сервер электронной подписи
ЭП	—	Электронная подпись
ПАК	—	Программно-аппаратный комплекс
ПАКМ	—	Программно-аппаратный криптографический модуль
УЦ	—	Удостоверяющий Центр

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Электронная подпись	—	информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.
Сертификат открытого ключа	—	электронный или бумажный документ, содержащий открытый ключ, информацию о владельце ключа, области применения ключа, подписанный выдавшим его Удостоверяющим центром и подтверждающий принадлежность открытого ключа владельцу.
Квалифицированный сертификат открытого ключа (квалифицированный сертификат)	—	сертификат открытого ключа, выданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи.
Владелец сертификата открытого ключа	—	лицо, которому в установленном Федеральным законом (№63-ФЗ от 06.04.2011 г. «Об электронной подписи») порядке выдан сертификат открытого ключа.
Закрытый ключ	—	уникальная последовательность символов, предназначенная для шифрования.
Ключ электронной подписи	—	уникальная последовательность символов, предназначенная для создания электронной подписи
Ключ проверки электронной подписи	—	уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи.
Удостоверяющий центр	—	юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов открытых ключей, а также иные функции, предусмотренные Федеральным законом №63-ФЗ от 06.04.2011 г. «Об электронной подписи».
Средства электронной подписи	—	шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание закрытого и открытого ключей.

Оглавление

1. Аннотация

В настоящем документе описывается настройка и работа с ПО «КриптоПро DSS Lite» в режиме веб-интерфейса. КриптоПро DSS Lite позволяет подписывать документы всех распространённых форматов на различных платформах, используя различные ИС и ключевые носители.

Документ предназначен для системных администраторов и Администраторов СЭП «КриптоПро DSS» как руководство по установке и конфигурированию DSS Lite, а также для пользователей как инструкция по использованию КриптоПро DSS Lite.

2. Общие сведения о DSS Lite

2.1. Назначение DSS Lite

КриптоПро DSS Lite предоставляет следующие сценарии работы:

- в режиме программного интерфейса;
- в режиме веб-интерфейса.

КриптоПро DSS Lite в режиме веб-интерфейса является специализированным режимом работы компонента СЭП «КриптоПро DSS» Сервис Подписи. При работе в данном режиме Пользователю доступно следующее:

- создание электронной подписи документов;
- шифрование и расшифрование документов (только Enveloped CMS);
- управление сертификатами пользователей.

Ключи ЭП и закрытые ключи пользователей создаются и хранятся непосредственно на устройстве пользователя, где выполняются криптографические операции с использованием КриптоПро CSP или другого СКЗИ, имеющего действующий сертификат соответствия ФСБ России.

Регистрация и аутентификация Пользователей происходит в соответствии с возможностями КриптоПро DSS, описанными в документах «ЖТЯИ.00096–02 96 02 КриптоПро DSS. Общее описание» и «ЖТЯИ.00096–02 91 02 КриптоПро DSS. Руководство администратора».

Шифрование документов выполняется средствами КриптоПро DSS с использованием криптопровайдера, функционирующего на сервере (см. документ ЖТЯИ.00096-02 91 02 КриптоПро DSS. Руководство администратора). Расшифрование документов выполняется с использованием криптопровайдера, функционирующего на устройстве пользователя.

2.2. Принцип работы DSS Lite

Процессы DSS Lite как режима работы Сервиса Подписи аналогичны процессам КриптоПро DSS, описанным в документе «ЖТЯИ.00096–02 96 02 КриптоПро DSS. Общее описание». При этом криптографические операции выполняются локально на устройстве Пользователя, и процессы аудита событий DSS Lite и подтверждения операций отсутствуют.

В DSS Lite возможна настройка отображения документов перед подписью на Веб-интерфейсе Пользователя. При этом настройки отображения документов аналогичны

описанному в документе «ЖТЯИ.00096–02 91 02 КриптоПро DSS. Руководство администратора».

2.3. Поддерживаемые форматы подписи

КриптоПро DSS Lite поддерживает все форматы электронной подписи, описанные в документе «ЖТЯИ.00096–02 96 02 КриптоПро DSS. Общее описание».

3. Системные требования

3.1. Требования к аппаратному обеспечению

Требования к аппаратному обеспечению аналогичны требованиям, описанным в документе «ЖТЯИ.00096–02 91 02 КриптоПро DSS. Руководство администратора».

3.2. Требования к программному обеспечению

Обеспечение работоспособности DSS Lite подразумевает предъявление требований к ПО, установленному как на сервере с DSS Lite, так и на устройстве пользователя, с которого осуществляется работа в DSS Lite.

Программное обеспечение на устройстве пользователя

На устройстве пользователя, с которого он подписывает документы при помощи DSS Lite, должны быть установлены:

- КриптоПро CSP или другое СКЗИ, имеющее действующий сертификат соответствия ФСБ России;
- Современный веб-браузер;
- КриптоПро ЭЦП Browser plug-in;
- ОС из списка операционных систем, поддерживаемых как выбранным пользователем сертифицированным ФСБ России СКЗИ (например, КриптоПро CSP), так и браузером.

Программное обеспечение сервера DSS Lite

К программному обеспечению сервера, на котором размещается DSS Lite (а именно компонент КриптоПро DSS Сервис Подписи), предъявляются следующие требования:

- ОС Windows Server 2008 R2/2012/2012R2 (x64)/2016/2019;
- КриптоПро CSP версии 4.0 и выше (серверная лицензия входит в комплект поставки КриптоПро DSS);
- (Опционально) КриптоПро .NET.
- (Опционально) КриптоПро TSP Client (Компонент из состава ПАК «Службы УЦ 2.0», используется при наличии действующего сертификата, выданного ФСБ России, требуется для создания подписи форматов CAdES -T и CAdES-X Long Type 1);
- (Опционально) КриптоПро OCSP Client (Компонент из состава ПАК «Службы УЦ 2.0», используется при наличии действующего сертификата, выданного ФСБ России, требуется для создания подписи формата CAdES-X Long Type 1);

Для создания электронной подписи XML-документов (XMLDSig) и документов MS Office необходимо установить продукт «КриптоПро .NET» и ввести действующую серверную лицензию.

3.3. Требования к компонентам ОС, установленной на веб-сервере

Для функционирования всех компонентов СЭП «КриптоПро DSS» необходима установка Microsoft Internet Information Services (IIS). Необходимые роли и компоненты, а также их установка и настройка полностью аналогичны описанному в документе «ЖТЯИ.00096–02 91 02 КриптоПро DSS. Руководство администратора».

4. Развертывание DSS Lite

4.1. Порядок развертывания

Развертывание DSS Lite осуществляется в следующем порядке:

1. Установка веб-сервера Microsoft IIS с необходимыми компонентами (см. раздел 3.3).
2. Установка дополнительного ПО (производится автоматически, если необходимо, после запуска дистрибутива DSS Lite).
3. Установка КриптоПро CSP.
4. Установка КриптоПро .NET (если требуется подписывать XML-документы и документы MS Office).
5. Установка минимально необходимых для DSS Lite компонентов КриптоПро DSS (см. раздел 4.2).
6. Настройка минимально необходимых для DSS Lite компонентов КриптоПро DSS (см. раздел 5).

4.2. Установка DSS Lite

Установка компонентов КриптоПро для обеспечения работы DSS Lite производится в порядке, установленном в документе «ЖТЯИ.00096-02 91 02 КриптоПро DSS. Руководство администратора». При этом в окне выбора конфигурации установки компонентов необходимо установить следующие компоненты:

- Сервис Подписи;
- Веб-интерфейс Пользователя
- Центр Идентификации.

Если были установлены другие компоненты КриптоПро DSS, необходимо оставить включенными соответствующие чекбоксы, иначе будет произведено удаление этих компонентов.

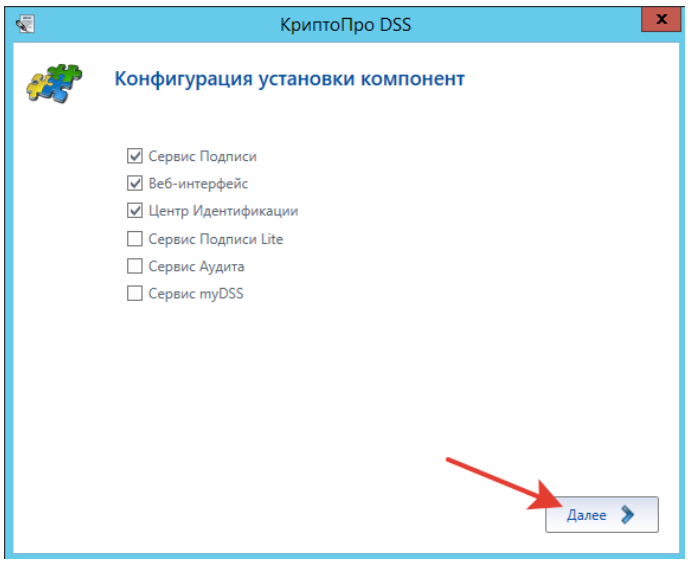

Рис. 1 — Пример конфигурации компонентов для установки DSS Lite

При подтверждении параметров установки убедитесь, что компоненты КриптоПро DSS имеют статус «Не изменять».

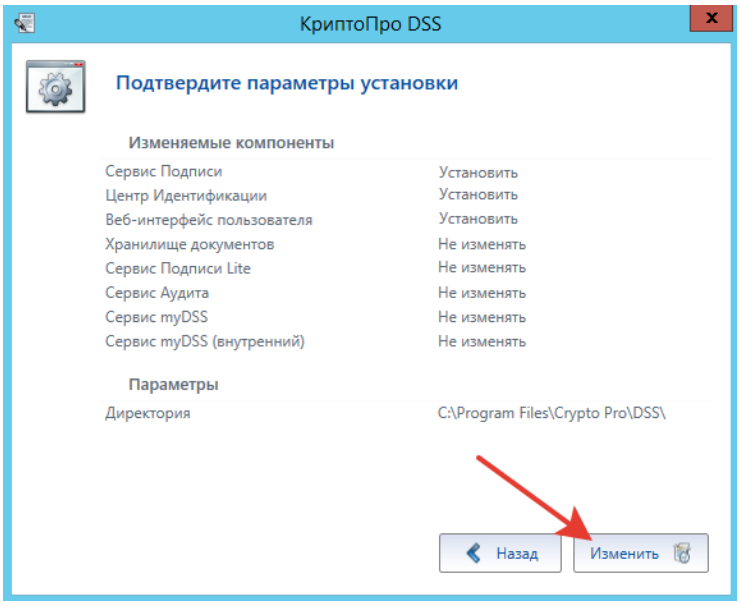

Рис. 2 — Подтверждение параметров установки DSS Lite

Для получения более подробной информации, а также информации по обновлению и удалению компонентов КриптоПро DSS и DSS Lite см. документ «ЖТЯИ.00096-02 91 02 КриптоПро DSS. Руководство администратора».

5. Настройка DSS Lite

5.1. Последовательность шагов по настройке DSS Lite

Настройка DSS Lite как режима работы Сервиса Подписи КриптоПро DSS должна производиться следующим образом.

1. Создание и настройка экземпляра Центра Идентификации КриптоПро DSS (см. документ «ЖТЯИ.00096-02 91 02 КриптоПро DSS. Руководство администратора»).
2. Создание и настройка экземпляра Сервиса Подписи КриптоПро DSS **для работы в режиме DSS Lite**. (см раздел 5.2).
3. Создание и настройка экземпляра Веб-интерфейса Пользователя КриптоПро DSS. (см. документ «ЖТЯИ.00096-02 91 02 КриптоПро DSS. Руководство администратора»).
4. Зарегистрировать необходимых Операторов DSS.

5.2. Создание и настройка экземпляра Сервиса Подписи КриптоПро DSS для работы в режиме DSS Lite

Данный раздел определяет последовательность действий при разворачивании и настройке экземпляра Сервиса Подписи КриптоПро DSS в режиме DSS Lite

5.2.1. Предварительные условия

- Установленный SQL-Server;
- Установленная роль Сервер приложений (IIS) (см. раздел 3.3);
- Настроенная привязка https на Сервере приложений (IIS);
- Установленный КриптоПро CSP (входит в комплект поставки);
- Установленный КриптоПро .NET (устанавливается автоматически при установке КриптоПро DSS);
- Выпущенный и установленный сервисный сертификат Сервиса Подписи (см. документ «ЖТЯИ.00096-02 91 02 КриптоПро DSS. Руководство Администратора»).

5.2.2. Базовая последовательность шагов по настройке

Выполнение шагов, описанных в данном разделе, обеспечивает минимально необходимую настройку экземпляра Сервиса Подписи для работы в режиме DSS Lite.

Полное описание всех упоминаемых в данном документе командлетов администрирования находится в документе «ЖТЯИ.00096–02 91 02 КриптоПро DSS. Руководство администратора».

1. Создание экземпляра службы Сервиса Подписи (командлет New-DssSignServerInstance).

На данном шаге будет создано веб-приложение на Сервере приложений IIS, развёрнуты базы данных, зарегистрированы журналы Windows.

2. Настройка сервисного сертификата Сервиса Подписи.

На данном шаге экземпляру Сервиса Подписи назначается сервисный сертификат, который используется для аутентификации при межсервисном взаимодействии (см. документ «ЖТЯИ.00096–02 91 02 КриптоПро DSS. Руководство администратора»).

Учетной записи, под которой работает пул приложения Сервиса Подписи, необходимо выдать права на доступ к закрытому ключу сервисного сертификата (см. документ «ЖТЯИ.00096–02 91 02 КриптоПро DSS. Руководство администратора»).

3. Переключение экземпляра Сервиса Подписи в режим работы DSS Lite.

На данном шаге происходит включение DSS Lite. При этом Веб-интерфейс Пользователя автоматически подстроится под работу с DSS Lite, даже если будет создан после выполнения данного действия.

```
Set-DssProperties -DisplayName <Имя экземпляра Сервиса Подписи> -ServiceType
Client
```

4. Регистрация криптопровайдеров.

Регистрация локальных криптопровайдеров Пользователя производится при помощи командлета Add-DssCryptoProvider. При этом необходимо указать параметр **-TypeId Lite**.

5. Регистрация обработчика, реализующего функцию по созданию запроса на сертификат.

Данный шаг выполняется при помощи командлета Add-DssEnrollment.

6. Настройка отношений доверия с Центром Идентификации

На данном шаге устанавливается отношение доверия между Центром Идентификации и Сервисом Подписи, которое необходимо для аутентификации Пользователей и Операторов на Сервисе Подписи.

Настройка выполняется в два шага:

- Регистрация на Сервисе Подписи Центра Идентификации в качестве доверенного издателя маркеров безопасности.

Данное действие выполняется при помощи командлета Add-DssClaimsProviderTrust.

- Регистрация Сервиса Подписи в качестве доверенной стороны на Центре Идентификации.

Данное действие выполняется при помощи командлета Add-DssRelyingPartyTrust. Примеры регистрации доверенных сторон приведены также в документе «ЖТЯИ.00096–02 91 02 КриптоПро DSS. Руководство администратора».

К моменту выполнения указанных шагов по настройке DSS Lite должен быть развёрнут и настроен экземпляр Центра Идентификации.

После внесения изменений в конфигурацию экземпляра необходимо перезапустить пул веб-приложения при помощи соответствующей команды:

```
Restart-DssSignServerInstance -DisplayName <Имя экземпляра
Сервиса Подписи>
```

5.2.3. Дополнительные действия по настройке

1. Настройка параметров подписи

При помощи командлета Set-DssProperties Администратор может ограничить набор форматов подписи, которые может создавать Сервис Подписи. По умолчанию доступны все форматы подписи, описанные в документе «ЖТЯИ.00096–02 96 02 КриптоПро DSS. Общее описание».

2. Для подписи формата CAdES-T и CAdES-X Long Type 1 необходимо задать адреса служб штампов времени (см. документацию на Службы УЦ 2.0).

Список настроенных служб штампов времени будет отображаться в Веб-интерфейсе Пользователя.

Администратор может настроить обязательную проверку актуального статуса сертификата перед подписью.

3. Журналирование экземпляра.

Администратор может включить журналирование экземпляра Сервиса Подписи, работающего в режиме DSS Lite (см. документ «ЖТЯИ.00096–02 91 02 КриптоПро DSS. Руководство администратора»).

5.3. Пример PowerShell-сценария для настройки DSS Lite как режима работы Сервиса Подписи

```
# Создание нового экземпляра компонента Сервис Подписи
New-DssSignServerInstance -SiteName "Default Web Site"  ApplicationName
SignServer SQLServerName ".\SQLEXPRESS" -DisplayName SignServer

# Ввод отпечатка сервисного сертификата
Set-DssProperties -ServiceCertificateThumbprint <Отпечаток сертификата
компонента>

Переключение экземпляра Сервиса Подписи в режим работы DSS Lite.
Set-DssProperties -DisplayName <Имя экземпляра Сервиса Подписи> -ServiceType
Client

#Добавление локального криптопровайдера
Add-DSSCryptoProvider -TypeId Lite -ProviderName " Crypto-Pro GOST R 34.10-
2012 Cryptographic Service Provider" -ProviderType 80

#Регистрация обработчика, отвечающего за генерацию запроса на сертификат
Add-DssEnrollment -Type EnrollOutOfBand -EnrollName <Имя обработчика> -
RdnConfig <Путь к файлу политики имен> TemplatesConfig <Путь к файлу шаблонов
сертификатов>

# Настройка отношений доверия с Центром Идентификации
Add-DssClaimsProviderTrust -IssuerName realsts -Thumbprint <Отпечаток
сертификата Центра Идентификации>

# Пример регистрации Сервиса Подписи в качестве доверенной стороны на Центре
Идентификации:
Add-DssRelyingPartyTrust -Name "SignServer" -MetadataUri
http://<signserver_host>/SignServer/FederationMetadata/2007-
06/FederationMetadata.xml
```

```
# Регистрация службы штампов времени
Add-DssTspService -Name testTSP -Title "TSP-служба КРИПТО-ПРО" -Url "
http://tsp.cryptopro.ru/tsp20/tsp.srf"

#Пример включения журналирования:
# Настройка журналирования событий
Set-DssSignServerTracing -ServiceModelListenerLogFile
C:\dsstrace\SignServer.svclog -ServiceModelListenerSourceLevel All

# Настройка журналирования сообщений
Set-DssSignServerTracing -ServiceModelMessageLoggingListenerLogFile
C:\dsstrace\SignServerMessage.svclog -
ServiceModelMessageLoggingListenerSourceLevel All

# Включение журналирования
Enable-DssSignServerTracing
```

СВЕДЕНИЯ О РАЗРАБОТЧИКЕ

Компания КриптоПро создана в 2000 году и в настоящее время занимает лидирующее положение по распространению средств криптографической защиты информации и электронной цифровой подписи.

Основное направление деятельности компании - разработка средств криптографической защиты информации и развитие Инфраструктуры Открытых Ключей (Public Key Infrastructure) на основе использования международных рекомендаций и российских криптографических алгоритмов.

Компания разработала полный спектр программных и аппаратных продуктов для обеспечения целостности, авторства и конфиденциальности информации с применением ЭП и шифрования для использования в различных средах (Windows, Unix, Java). Новое направление продуктов компании – программно-аппаратные средства криптографической защиты информации и использованием смарт-карт и USB ключей, позволяющих существенно повысить безопасность систем, использующих ЭП.

Компания КриптоПро является разработчиком и поставщиком средств применения ЭП в автоматизированных информационных системах. Кроме этого, компания оказывает консультационные услуги по обеспечению деятельности удостоверяющих центров и применению ЭП в автоматизированных информационных системах предприятий различных форм собственности.

Удостоверяющий центр компании КриптоПро предоставляет организациям (юридическим лицам) услуги по изготовлению и управлению открытыми и закрытыми ключами пользователей информационных систем, включая процедуру подачи и обработки запросов на сертификаты, верификацию запросов на сертификаты, формирования сертификатов, их получения, использования и отзыва. Также Удостоверяющим центром предоставляются иные сервисные функции, связанные с использованием электронных подписей, шифрованием, обеспечением электронного юридически-значимого документооборота.

Контакты:

ООО «КРИПТО-ПРО»

127018, Москва, ул. Сущёвский вал, 18

Телефон: (495) 995 4820

Факс: (495) 995 4820

URL: http://www.CryptoPro.ru

E-mail: info@CryptoPro.ru