encryption

PKI

digital signature

ЮРИДИЧЕСКАЯ ЗНАЧИМОСТЬ

КОНФИДЕНЦИАЛЬНОСТЬ

ЦЕЛОСТНОСТЬ

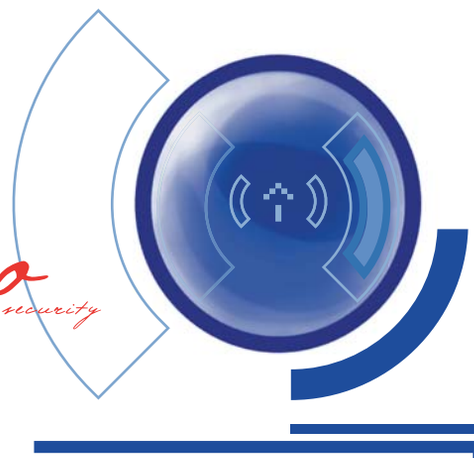
АВТОРСТВО

ЭЦП

КРИПТОПРО

CryptoPro

cryptographic information security



КЛЮЧЕВОЕ СЛОВО В ЗАЩИТЕ ИНФОРМАЦИИ

KeyWord in the world of information security

КРИПТО ПРО

О компании Крипто-Про

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.

Крипто-Про имеет все необходимые лицензии ФСБ и ФСТЭК на право осуществления деятельности по разработке, производству, распространению и техническому сопровождению шифровальных (криптографических) средств, предоставлению услуг в области шифрования информации.

С 2001 года компания активно проводит работы по гармонизации международных стандартов и рекомендаций. В 2006 году опубликован первый в истории сообщества Интернет стандарт, описывающий применение российских криптографических алгоритмов - RFC 4357, "Additional Cryptographic Algorithms for Use with GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms" (http://www.ietf.org/rfc/rfc4357.txt).

Разработаны:

- RFC 4490, "Using the GOST 28147-89, GOST R 34.11-94, GOST R 34.10-94, and GOST R 34.10-2001 Algorithms with Cryptographic Message Syntax (CMS)" - использование российских алгоритмов в документах, удовлетворяющих спецификации CMS (Cryptographic Message Syntax).
- RFC 4491, "Using the GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile" - использование российских алгоритмов в инфраструктуре открытых ключей Интернет.
- "Addition of GOST Ciphersuites to Transport Layer Security (TLS)" - дополнение к спецификации RFC 2246 "The TLS Protocol. Version 1.0" в части применения российских алгоритмов;
- "Using algorithms GOST R 34.10-2001, GOST R 34.10-94 and GOST R 34.11-94 for XML Digital Signatures" - дополнение, описывающее правила применения ЭЦП в документах формата XML.

Компания Крипто-Про выдала более 2 500 000 лицензий на использование средства криптографической защиты информации КриптоПро CSP и более 700 лицензий на использование удостоверяющего центра КриптоПро УЦ.

Продукты компании широко применяются различными государственными и коммерческими организациями в системах электронного документооборота, в система сдачи налоговой и бухгалтерской отчетности, в системах исполнения бюджета, городского заказа и т.д.

Деятельность и продукты компании отмечены национальной отраслевой Премией "За укрепление безопасности России" (ЗУБР-2007):
Выбор рынка *(диплом);*
За выдающийся вклад компании в формирование российского рынка криптографических средств защиты информации и инфраструктуры открытых ключей *(диплом лауреата);*
КриптоПро CSP, КриптоПро PKI *(золотые медали).*

Кроме интеграции КриптоПро CSP в средства российских разработчиков несколько ведущих мировых производителей встроили указанное средство в свои продукты. К этим продуктам относятся:

- RSA Keon 6.5, производства RSA Security;
- Unicert 5.1, производства Baltimore Technologies;
- Nortel VPN Router (Contivity), производства Nortel Networks;
- Check Point Connectra, производства Check Point Software Technologies;
- Borderless Security iGate, производства SafeNet Inc.;
- Oracle E-Business Suite, производства Oracle Corporation;
- Apache (Apache Software Foundation);

Microsoft GOLD CERTIFIED Partner

ISV/Software Solutions
Networking Infrastructure Solutions

Внедрение систем электронного ведения бизнеса и коммерции, документооборота и взаимодействия с органами государственной власти неразрывно связано с обеспечением информационной безопасности. Конфиденциальность, целостность, авторство, актуальность передаваемой и хранимой информации, неотказуемость от совершенного действия в электронном виде приводят к необходимости использования средств криптографической защиты информации.

Основой для обеспечения информационной безопасности с использованием средств криптографической защиты является Инфраструктура Открытых Ключей (Public Key Infrastructure - PKI), главная роль в которой отводится удостоверяющим центрам.

Программный комплекс КриптоПро УЦ разработан с учетом положений Федерального закона № 1 от 10.01.2002 г. "Об электронной цифровой подписи" и получил первый в России сертификат соответствия СФ/128-0662 от 20 ноября 2003 г., выданный центром безопасности связи ФСБ, который удостоверяет, что КриптоПро УЦ соответствует требованиям к информационной безопасности удостоверяющих центров класса КС2 и может использоваться в составе технических средств удостоверяющих центров корпоративных информационных систем, предназначенных для обработки информации, не содержащих сведений, составляющих государственную тайну, с применением средств электронной цифровой подписи.

КриптоПро УЦ - комплекс программных средств, предназначенных для внедрения и использования Инфраструктуры Открытых Ключей в целях обеспечения информационной безопасности и юридической значимости электронного документооборота с применением электронной цифровой подписи в соответствии с положениями Федерального закона "Об электронной цифровой подписи". В состав КриптоПро УЦ входят программные средства и нормативные документы, позволяющие производить разбор конфликтных ситуаций, которые могут возникнуть в процессе применения ЭЦП.

Использование в качестве средства криптографической защиты информации сертифицированного продукта КриптоПро CSP, аппаратного датчика случайных чисел, взаимодействие всех компонент комплекса по защищенному протоколу TLS со строгой криптографической аутентификацией, ролевое разграничение функций, протоколирование действий - обеспечивают высокий уровень безопасности, что подтверждено результатами сертификационных испытаний.

Возможно использование внешнего аппаратного криптографического модуля.

Использование в полной мере функциональности операционной системы Microsoft Windows 2000 Server, MS SQL 2000 Ser ver (MSDE), службы сертификации позволяет обеспечить высокий уровень надежности и производительности при эксплуатации комплекса, реализовать процедуры архивирования и восстановления компонентов и баз КриптоПро УЦ в случае сбоев.

Для обеспечения достоверности сведений, содержащихся в сертификатах ключей подписей, КриптоПро УЦ позволяет использовать несколько режимов регистрации и изготовления сертификатов открытых ключей.

- Режим централизованной регистрации пользователей обеспечивает наиболее строгую политику идентификации пользователей, являющихся владельцами сертификатов открытых ключей.
- Режим распределенной (удаленной) регистрации пользователей обеспечивает обслуживание пользователей, территориально удаленных от удостоверяющего центра. Регистрация пользователей происходит на основании запросов на регистрацию, управление которыми осуществляется администратором Центра Регистрации с использованием программного обеспечения своего АРМа.
- Режим централизованного управления ключами и сертификатами пользователей обеспечивает формирование ключей и сертификатов пользователей на основании их заявления.
- Режим распределенного управления пользователями личными ключами и сертификатами. В данном режиме, пользователи посредством программного обеспечения АРМа, имеют возможность на своем рабочем месте выполнить генерацию ключей, сформировать запрос на сертификат и передать запрос в Центр Регистрации. Дальнейшее управление запросами и выпуском сертификатов осуществляется администратором удостоверяющего центра.

В зависимости от требований политики предприятия программное обеспечение комплекса позволяет использовать комбинированные режимы, совмещая централизованные и распределенные модели регистрации.

Криптография

- Юридическая значимость
- Безопасность
- Надежность
- Гибкость
- Масштабируемость
- Интеграция

- Автоматическая публикация сертификатов во внешние сетевые справочники (LDAP, Active Directory);
- Автоматическое распространение списков отозванных сертификатов в иерархии удостоверяющих центров;
- Автоматическое оповещение пользователей удостоверяющего центра по электронной почте по всем событиям жизненного цикла сертификатов открытых ключей, владельцами которых они являются;
- Возможность использования различных криптографических алгоритмов, реализованных в соответствии с интерфейсом Microsoft Cryptographic Service Providers;
- Возможность определения различных областей применения сертификатов и различных сроков их действия в соответствии с рекомендациями X.509 и RFC 3280.

Входящие в состав КриптоПро УЦ компоненты - Центр сертификации, Центр регистрации, АРМ администратора, WEB интерфейс, пользовательские средства взаимодействия с УЦ, программный интерфейс взаимодействия с УЦ, позволяют построить многоуровневую, территориально распределенную архитектуру управления сертификатами открытых ключей.
Горизонтальное масштабирование позволяет наращивать функциональность удостоверяющего центра в соответствии с отдельными направлениями электронного документооборота и областей ведения бизнеса.
Документация включает типовой Регламент удостоверяющего центра, учитывающий положения действующего законодательства РФ в части применения ЭЦП.
Использование XML шаблонов дает гибкий инструмент организации по созданию бланка для печати сертификатов открытых ключей и запросов на сертификаты.
Авторизованные курсы по внедрению и эксплуатации Инфраструктуры Открытых Ключей с использованием КриптоПро УЦ проводятся в учебных центрах НИП ИНФОРМЗАЩИТА и Академии АйТи.

УДОСТОВЕРЯЮЩИЙ ЦЕНТР

КРИПТОПРО CryptoPro

КриптоПро OCSP

КриптоПро OCSP - программный комплекс, предназначенный для выполнения функции онлайновой проверки статуса сертификата в соответствии со спецификацией RFC 2560 - "Internet X.509 Public Key Infrastructure. Online Certificate Status Protocol - OCSP".

- Функционирование под управлением операционных систем Windows 2000 Server и Windows 2003 Server.
- Реализация расширения протокола RFC 2560 - предоставление информации о статусе сертификата на определенное время, за счет ведения истории выпущенных списков отозванных сертификатов.
- Использование Microsoft IIS с различными способами аутентификации, криптографическая аутентификация по протоколу TLS (SSL).
- Использование СУБД MSDE или Microsoft SQL Server.
- Несколько экземпляров службы на одном сервере.
- Использование дополнений сертификатов Authority Information Access (AIA) для доступа к службе.
- Разграничение доступа к службе по списку контроля доступа, ролевая модель разграничения доступа.
- Использование российских сертифицированных средств криптографической защиты информации (КриптоПро CSP) или любого другого криптопровайдера в операционной системе Windows.
- Одновременное использование нескольких криптопровайдеров на разных экземплярах службы.
- Возможность работы как с сохранением всех выпущенных OCSP-ответов в журнале, так и без сохранения.

КриптоПро TSP

КриптоПро TSP - программный комплекс, предназначенный для создания штампов времени в соответствии со спецификацией протокола RFC 3161 - "Internet X.509 Public Key Infrastructure. Time-Stamp Protocol (TSP)"

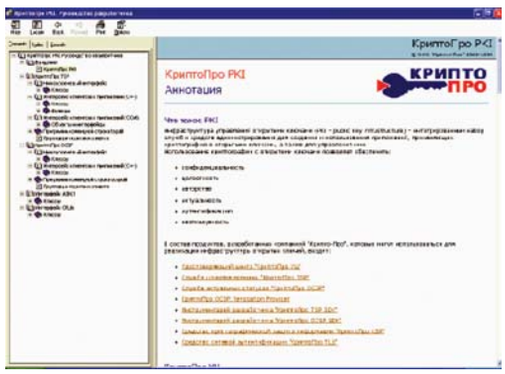
- Функционирование под управлением операционных систем Windows 2000 Windows Server и Windows 2003 Server.
- Поддержка технологии Authenticode в операционной системе Microsoft Windows.
- Использование Microsoft IIS с различными способами аутентификации, криптографическая аутентификация по протоколу TLS (SSL).
- Несколько экземпляров службы на одном сервере.
- Разграничение доступа к службе по списку контроля доступа, ролевая модель разграничения доступа.
- Использование российских сертифицированных средств криптографической защиты информации (КриптоПро CSP) или любого другого криптопровайдера в операционной системе Windows.
- Одновременное использование нескольких криптопровайдеров на разных экземплярах службы.
- Защита от непреднамеренного и злоумышленного перевода времени.
- Режим упорядочивания штампов (все штампы имеют разное, монотонно возрастающее время).

Программные комплексы КриптоПро TSP и КриптоПро OCSP получили положительное заключение ФСБ России на соответствие требованиям по информационной безопасности по уровню КС2.

КриптоПро TSP
КриптоПро OCSP

инструментарий разработчика

Для создания приложений, реализующих службы штампов времени в соответствии со спецификацией RFC 3161 "Internet X.509 Public Key Infrastructure, Time-Stamp Protocol (TSP)" и онлайновой проверки статуса сертификата в соответствии со спецификацией RFC 2560 "Internet X.509 Public Key Infrastructure. Online Certificate Status Protocol - OCSP".



Реализация алгоритма хэширования данных в соответствии с ГОСТ Р 34.11-94 и ЭЦП в соответствии с ГОСТ Р34.10-94 и ГОСТ Р34.10-2001 с использованием КриптоПро CSP, а также поддержка любых других алгоритмов, доступных через интерфейс CryptoAPI 2.0.
Для платформ Win98/ME/2K/XP/2003.

КриптоПро CSP

КриптоПро CSP - средство криптографической защиты информации, реализующее российские криптографические алгоритмы разработанное в соответствии с интерфейсом Microsoft - Cryptographic Service Provider (CSP).

юридическая значимость

Федеральный закон "Об электронной цифровой подписи" определяет условия применения средств электронной цифровой подписи для создания систем юридически значимого электронного документооборота. Использование КриптоПро CSP в качестве средства ЭЦП в соответствии с положениями закона позволяет обеспечить равнозначность ЭЦП собственноручной подписи.

интеграция с Windows

Интеграция КриптоПро CSP с операционной системой Windows позволяет использовать стандартные продукты и встраивать в разрабатываемые системы с применением различных интерфейсов Microsoft.

Реализация ЭЦП XML документов XMLdsig для Windows (MSXML5, MSXML6) - возможность использования российские криптоалгоритмы в Microsoft Office InfoPath 2003 - составляющей системы Microsoft Office.

реализация криптографических сообщений CMS/PKCS#7 для Unix

С целью облегчения интеграции криптографических функций в приложения на Unix платформах и использования единого кода реализован программный интерфейс аналогичный спецификации Microsoft CryptoAPI 2.0. Данный интерфейс позволяет использовать высокоуровневые функции для создания криптографических сообщений (шифрование, ЭЦП), построения и верификации цепочек сертификатов, генерации ключей, обработки данных сообщений и сертификатов.

протокол TLS

Для всех платформ реализован протокол TLS (SSL) - модуль сетевой аутентификации КриптоПро TLS.

поддержка технологий Java, Oracle, Apache

Продукты партнеров компании Крипто-Про, обеспечивающие использование КриптоПро CSP в приложениях Oracle E-Business Suite 11i, Oracle Application Server 10g, Java, Apache.

поддержка протокола Kerberos-RK

Реализована аутентификация пользователей в домене Windows с использованием смарт-карт (USB токенов) и сертификатов открытых ключей.

Стандартное использование КриптоПро CSP в электронной почте, а также в продуктах MS Word, Excel.

пплатформы

Windows (x86, ia64), Solaris 9 (x86, Sparc), FreeBSD 5, Red Hat Linux

состав

Для всех платформ в состав КриптоПро CSP входит модуль уровня ядра операционной системы (криптодрайвер), что позволяет использовать основные криптографические функции (шифрование/расшифрование, проверка подписи, хэширование) на уровне ядра операционной системы.

надежность, маштабируемость

Критические компоненты КриптоПро CSP протестированы на совместимость с ОС Windows по методикам WHQL test lab и подписаны Microsoft.

По результатам тестов Intel Identifier Program, проведенных при участии специалистов компании Intel, версии КриптоПро CSP для платформ P4HT и Xeon получили статус Runs great on Pentium 4 HT и Runs great on Xeon.

Улучшена масштабируемость на многопроцессорных системах и HyperThreading системах.

производительность

Значительно повышена производительность криптографических операций
шифрование 66 мбайт/сек.
хеширование 43 мбайт/сек.
вычисление ЭЦП (эллиптические кривые): 1.3 мсек.
проверка ЭЦП (эллиптические кривые): 2.3 мсек.
Значения приведены для P4 HT 3 ГГц.

соответствие требованиям

КриптоПро CSP имеет сертификаты соответствия ФСБ.

КриптоПро JSP

КриптоПро JCP - средство криптографической защиты информации, разработаное в соответствии с интерфейсами JCA (Java Cryptography Architecture).
Интеграция КриптоПро JCP с архитектурой Java позволяет использовать стандартные продукты, такие как ЭЦП XMLdsig и другие на широком спектре операционных систем и аппаратных платформ. В базовой модели поддерживаются различные отделяемые ключевые носители.
На основе КриптоПро JCP разработана реализация протокола cpSSL.

Атликс HSM

Безопасное хранение и использование закрытого ключа служб доверенной третьей стороны (уполномоченного лица УЦ, OCSP, TSP и др.) обеспечивается за счет использования аппаратного криптомодуля, выполняющего все криптографические операции, в том числе по генерации закрытого ключа.
Атликс HSM разработан в соответствии с требованиями к средствам криптографической защиты информации ФСБ России по уровню КВ2.
Защита закрытого ключа обеспечивается с использованием "раздельных секретов" - для активизации закрытого ключа одновременно необходимы три из пяти ключей, хранящихся на процессорных картах РИК (российская интеллектуальная карта). Кроме этого, канал взаимодействия с аппаратным криптомодулем защищен и взаимодействие с ним возможно только после двусторонней криптографической аутентификации.
Атликс HSM может использоваться как аппаратный криптографический модуль, обеспечивающий хранение и использование закрытых ключей пользователей в локальной сети.

Усовершенствованная подпись

Компания Крипто-Про предлагает новый формат ЭЦП - усовершенствованную подпись.

Опыт Крипто-Про – ведущей российской компании в области технологии ЭЦП – свидетельствует, что при использовании "классической" ЭЦП в юридически значимом электронном документообороте, в случае возникновения спора достаточно трудно, а подчас и невозможно, доказать подлинность ЭЦП и момент подписи (создания) ЭЦП. Эти трудности могут привести к тому, что арбитр не примет электронный документ в качестве письменного доказательства.

Данные трудности порождаются рядом проблем, присущих "классической" ЭЦП, а именно:

- отсутствием доказательства момента подписи;
- неопределенностью статуса сертификата открытого ключа подписи на момент подписи (действителен, аннулирован, приостановлен).

Предлагаемая Крипто-Про усовершенствованная подпись позволяет решить эти проблемы и обеспечить участников документооборота всей необходимой доказательной базой (причем собранной в самой ЭЦП в качестве реквизитов электронного документа), связанной с установлением момента подписи и статуса сертификата открытого ключа подписи на момент подписи.

Формат усовершенствованной подписи основан на европейском стандарте ETSI 101 733 и решает описанные выше проблемы и множество других, обеспечивая:

- доказательство момента подписи документа и действительности сертификата ключа подписи на этот момент;
- отсутствие необходимости сетевых обращений при проверке подписи;
- архивное хранение электронных документов;
- простоту встраивания и отсутствие необходимости контроля встраивания.

Доказательство момента подписи документа и действительности сертификата ключа подписи на этот момент

Согласно статье 4 ФЗ "Об электронной цифровой подписи", ЭЦП признаётся равнозначной собственноручной подписи в документе на бумажном носителе при условии, что сертификат ключа подписи, относящийся к этой ЭЦП, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания.

Формат усовершенствованной подписи предусматривает обязательное включение в реквизиты подписанного документа доказательства момента подписания документа и доказательства действительности сертификата в момент подписания.

Для доказательства момента подписи используются штампы времени, в соответствии с международной рекомендацией RFC 3161 "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)".

Проверка подлинности ЭЦП без сетевых обращений

Доказательства действительности сертификата в момент подписи обеспечиваются вложением в реквизиты документа цепочки сертификатов до доверенного УЦ и OCSP-ответов. На эти доказательства также получается штамп времени, подтверждающий их целостность в момент проверки.

Вложение в реквизиты документа всех доказательств, необходимых для проверки подлинности ЭЦП, обеспечивает возможность оффлайн-проверки подлинности ЭЦП. Доступ к репозиторию сертификатов, службам OCSP и службам штампов времени необходим только в момент создания подписи.

Простота встраивания и отсутствие необходимости контроля встраивания

Усовершенствованная подпись просто встраивается в любое приложение. Для этого не требуется углублённое знание интерфейса CryptoAPI, а также не требуется работа со всеми структурами, составляющими подпись, такими как штампы времени и OCSP-ответы.

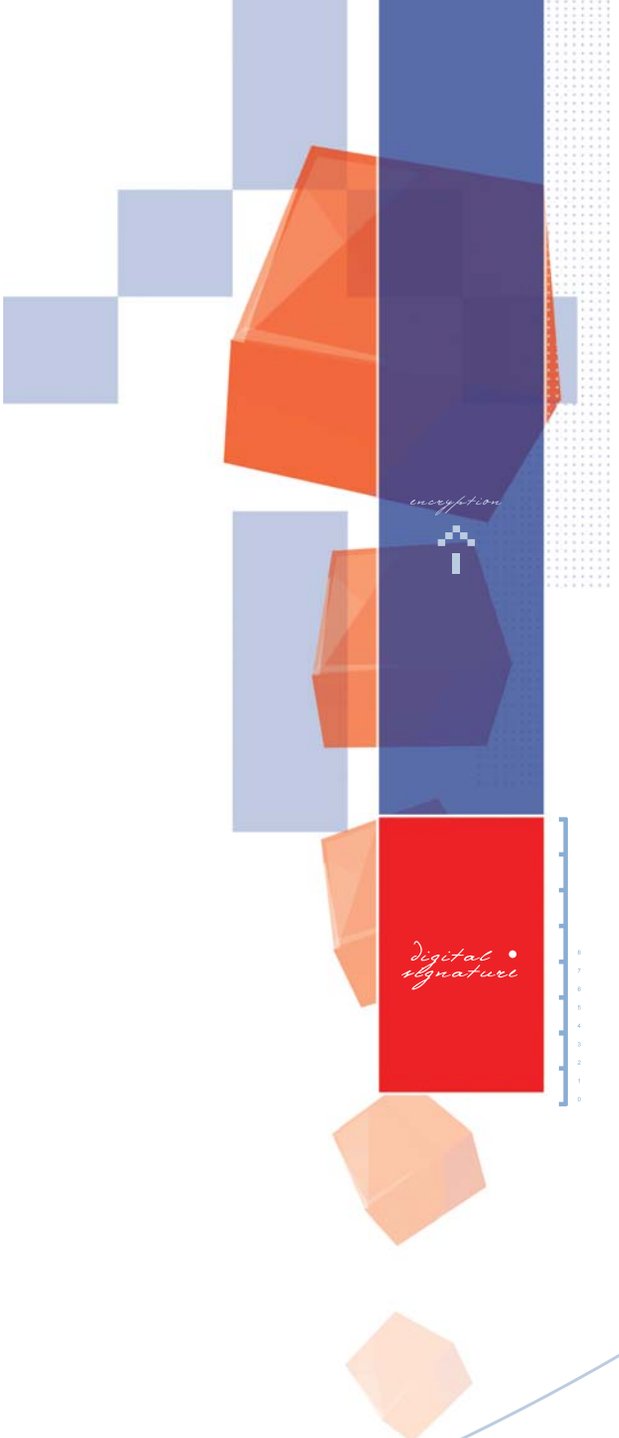
Вся работа с подписью заключается в вызове двух функций, одна из которых создаёт подпись, другая проверяет её.

Усовершенствованная подпись использует КриптоПро CSP. Простота встраивания делает тривиальным контроль встраивания, который осуществляется следующим образом: если в коде приложения вызываются функции создания усовершенствованной подписи, и её проверки, то встраивание выполнено правильно.

Архивное хранение

Использование усовершенствованной подписи является необходимым условием архивного хранения электронных документов, удостоверенных ЭЦП.

В формате усовершенствованной подписи вся необходимая информация для проверки подлинности ЭЦП находится в реквизитах документа. Для сохранения юридической значимости электронных документов при архивном хранении остаётся только обеспечить их целостность организационнотехническими мерами. В этом случае подлинность ЭЦП может быть подтверждена через сколь угодно долгое время, в том числе и после истечения срока действия сертификата ключа подписи.



Россия, 127018
Москва, Сущевский вал д.16 стр.5
тел/факс: +7 (495) 7804820
http://www.cryptopro.ru
info@cryptopro.ru

КЛЮЧЕВОЕ СЛОВО В ЗАЩИТЕ ИНФОРМАЦИИ
KeyWord in the world of information security

КРИПТО ПРО