

КриптоПро PDF

Версия 1.6

Руководство по эксплуатации

АННОТАЦИЯ

Настоящий документ содержит описание процесса установки и инструкции по использованию модуля создания и проверки электронной цифровой подписи «КриптоПро PDF» в программах Adobe Reader и Adobe Acrobat.

«КриптоПро PDF» представляет собой средство создания и проверки электронной цифровой подписи для файлов в формате PDF, предназначенное для использования совместно со средством криптографической защиты информации КриптоПро CSP.

Информация о разработчике «КриптоПро PDF»:

ООО «Крипто-Про»

127 018, Москва, а/я Крипто-Про

Телефон: (495) 780 4820

Факс: (495) 780 4820

<http://www.CryptoPro.ru>

E-mail: info@CryptoPro.ru

СОДЕРЖАНИЕ

1. Требования к программному обеспечению	4
2. Установка «КриптоПро PDF»	5
3. Эксплуатация «КриптоПро PDF»	10
3.1. Настройка формирования и проверки ЭЦП в программе Adobe Acrobat	10
3.2. Ввод серийного номера лицензии «КриптоПро PDF»	11
3.3. Формирование ЭЦП	12
3.4. Виды подписей в программах Adobe.	17
3.5. Отличия Adobe Reader и Adobe Acrobat при создании ЭЦП.	17
3.6. Создание ЭЦП в Adobe Reader.....	18
3.7. Проверка ЭЦП.....	19
4. Перечень сокращений	22
5. Перечень рисунков	23
6. Перечень таблиц	24

1. Требования к программному обеспечению

«КриптоПро PDF» предназначен для функционирования в следующих ОС:

- Microsoft Windows XP всех вариантов исполнения, как англоязычных, так и локализованных, с установленным пакетом обновления Service Pack 3 и выше;
- Microsoft Windows Server 2003 всех вариантов исполнения, как англоязычных, так и локализованных, с установленным пакетом обновления Service Pack 2 и выше;
- Microsoft Windows Vista, как англоязычных, так и локализованных, с установленным пакетом обновления Service Pack 2 и выше;
- Microsoft Windows Server 2008 всех вариантов исполнения, как англоязычных, так и локализованных, с установленным пакетом обновления Service Pack 2 и выше;
- Microsoft Windows 7, как англоязычной, так и локализованной, с установленным пакетом обновления Service Pack 1 и выше;
- Microsoft Windows Server 2008 R2 всех вариантов исполнения, как англоязычных, так и локализованных, с установленным пакетом обновления Service Pack 1 и выше;
- Microsoft Windows 8 всех вариантов исполнения, как англоязычных, так и локализованных;
- Microsoft Windows Server 2012, как англоязычной, так и локализованной.

Для функционирования «КриптоПро PDF» должно быть установлено средство криптографической защиты информации КриптоПро CSP версии 3.6 или выше.

Модуль КриптоПро PDF расширяет возможности программ Adobe Acrobat и Adobe Reader в части создания и проверки ЭЦП по алгоритму ГОСТ Р 34.10-2001.

Для функционирования «КриптоПро PDF» предварительно должна быть установлена одна из следующих программ:

- Adobe Acrobat версии 8, 9, X или XI всех вариантов исполнения;
- Adobe Reader версии 8, 9, X или XI.

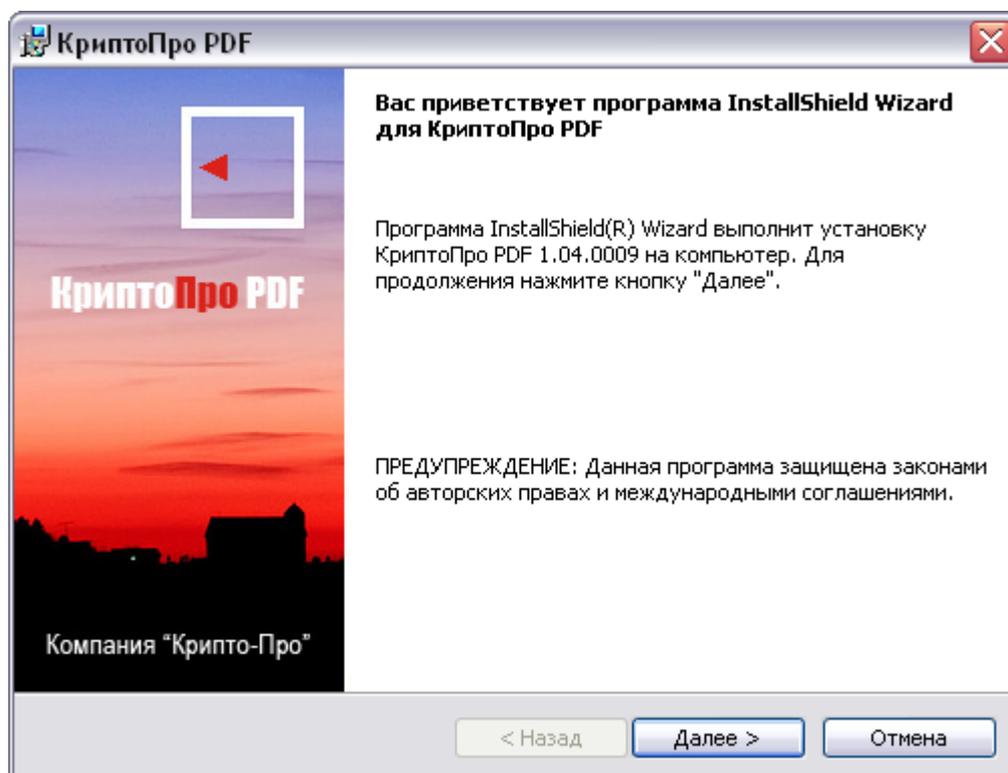


«КриптоПро PDF» поддерживает полноценную работу в защищенном режиме Adobe Reader в версии 10.0.1 и выше.

2. Установка «КриптоПро PDF»

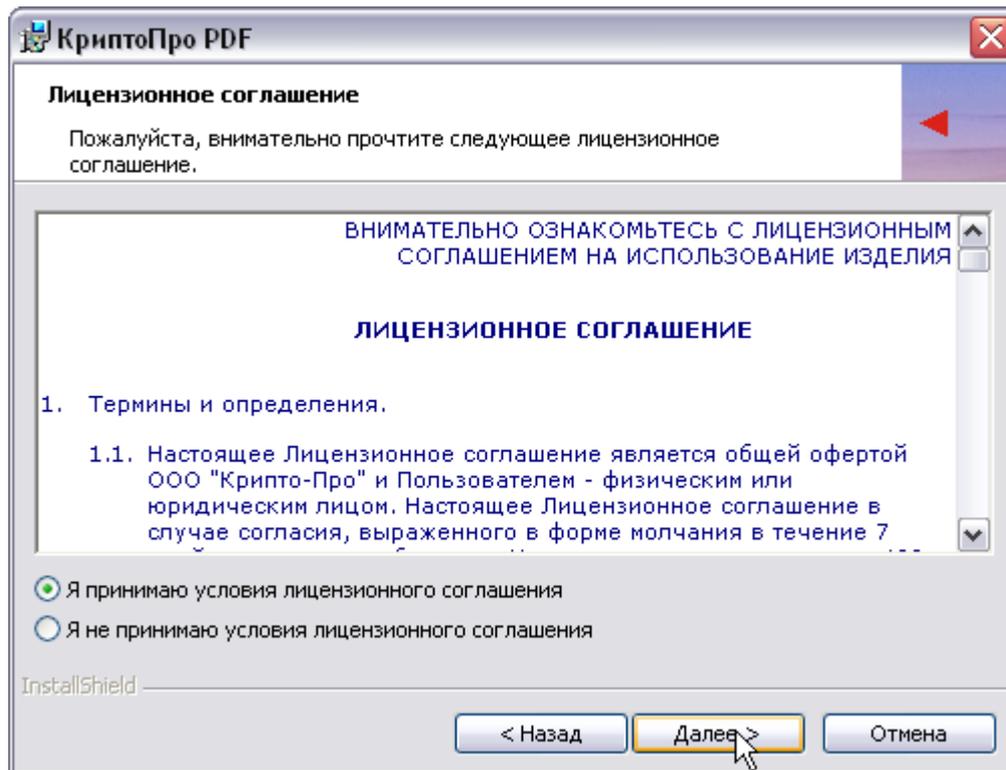
Запустите установку пакета **cppdf.msi**, расположенного на компакт-диске. После коротких подготовительных процедур на экране появится окно мастера установки (см. Рисунок 1). Нажмите кнопку **Далее**.

Рисунок 1. Мастер установки «КриптоПро PDF»



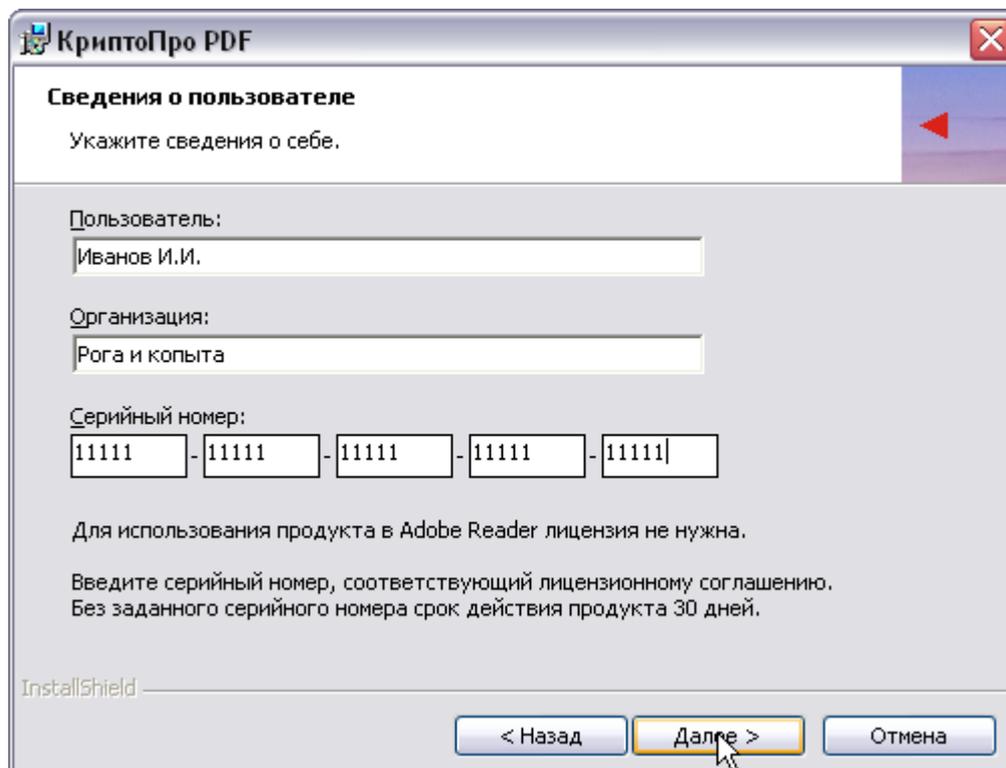
В следующем окне мастера установки ознакомьтесь с лицензионным соглашением на использование КриптоПро PDF. Если Вы согласны со всеми пунктами соглашения, выделите пункт **Я принимаю условия лицензионного соглашения**, и нажмите **Далее** (см. Рисунок 2).

Рисунок 2. Лицензионное соглашение на использование «КриптоПро PDF»



Следующим шагом необходимо ввести информацию о пользователе, производящем установку, и серийный номер лицензии на использование КриптоПро PDF (см. Рисунок 3). Поле серийного номера можно оставить пустым, тогда продукт будет работать в демонстрационном режиме в течение 30 дней.

Рисунок 3. Сведения о пользователе «КриптоПро PDF»



После нажатия кнопки **Далее** программа установки отобразит диалоговое окно (см. Рисунок 4), где необходимо выбрать вид установки. КриптоПро PDF определяет два вида установки: полная и выборочная.

Использование выборочной установки позволяет выбрать версии Adobe Acrobat и Adobe Reader, для которых будет установлен модуль «КриптоПро PDF» (см. Рисунок 5). Если при использовании выборочной установки не будет выбрана ни одна версия Adobe Acrobat или Adobe Reader, продолжить установку будет невозможно.

Рисунок 4. Вид установки «КриптоПро PDF»

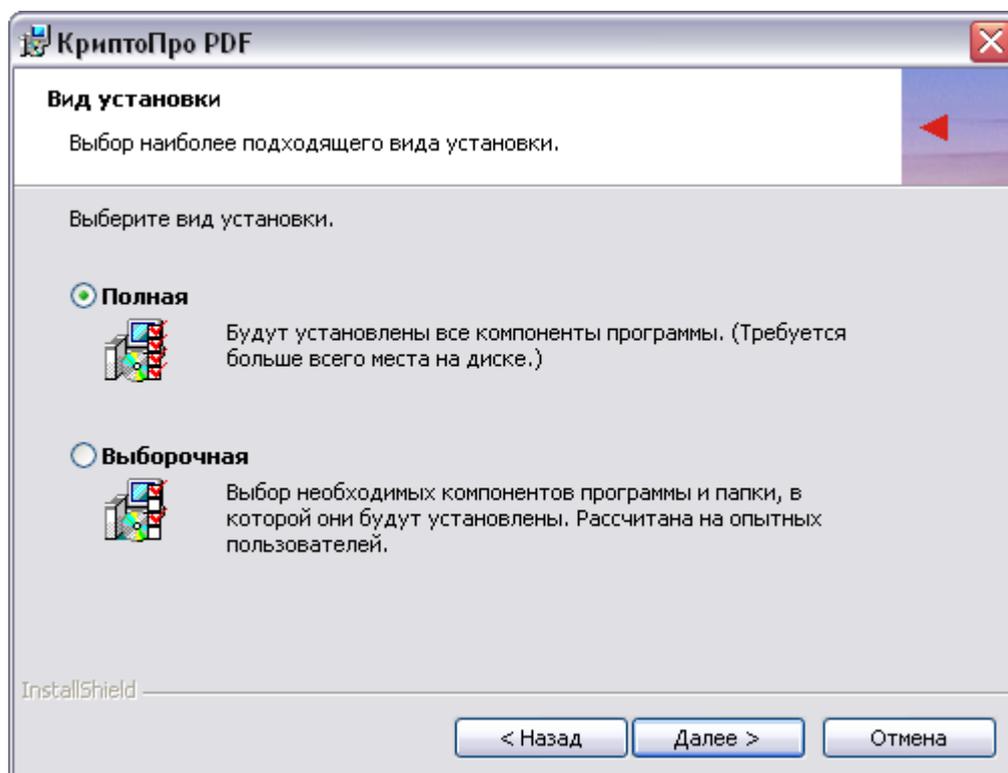
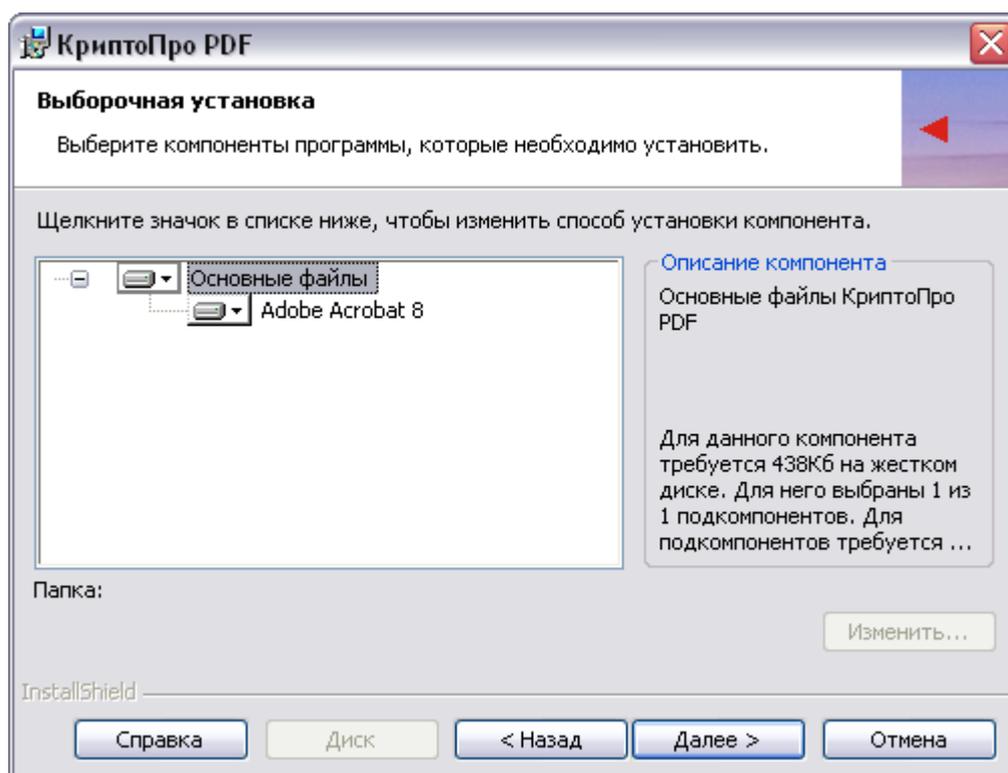
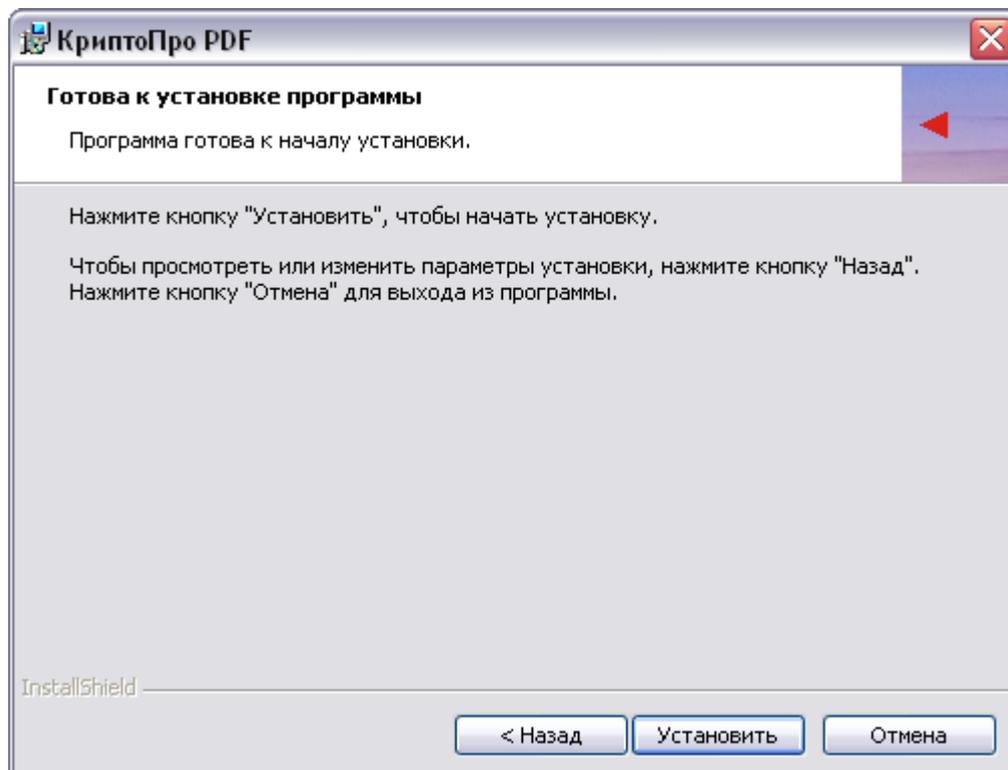


Рисунок 5. Выборочная установка «КриптоПро PDF»



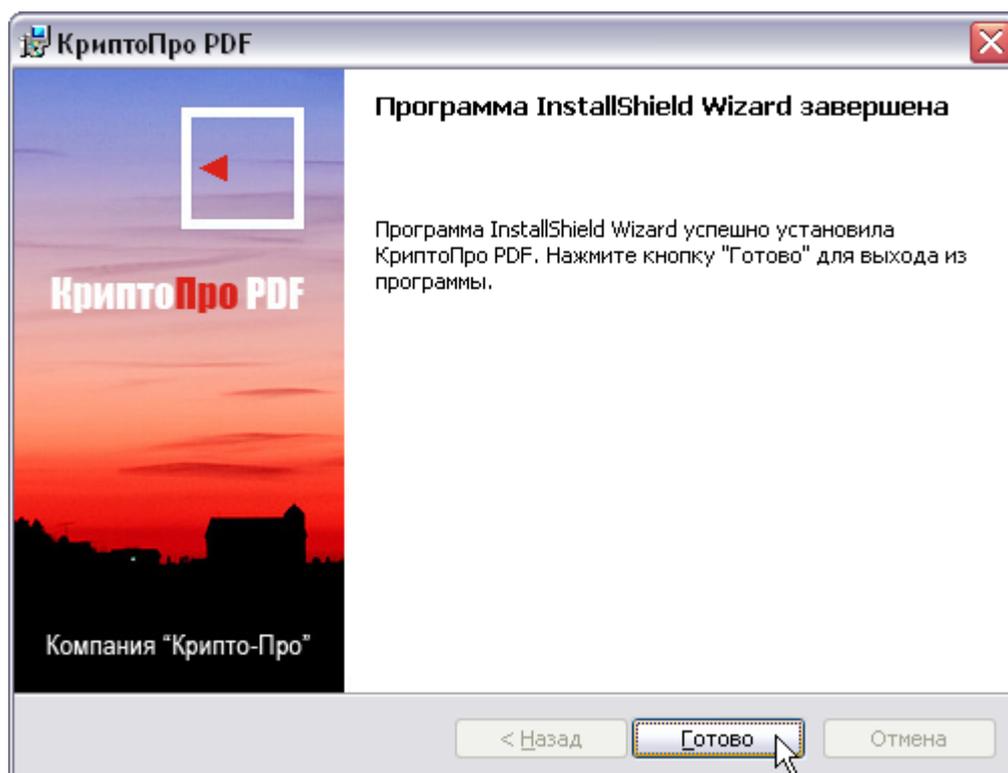
Следующее окно мастера служит для подтверждения установки (см. Рисунок 6). При необходимости можно вернуться назад и переопределить параметры установки. Для подтверждения нажмите кнопку **Установить**.

Рисунок 6. Окно подтверждения установки «КриптоПро PDF»



После выполнения всех описанных шагов мастер произведет установку КриптоПро PDF, сопровождая действия комментариями. По окончании установки мастер показывает окно с подтверждением успешной установки, где необходимо нажать кнопку **Готово** (см. Рисунок 7).

Рисунок 7. Завершение работы мастера установки

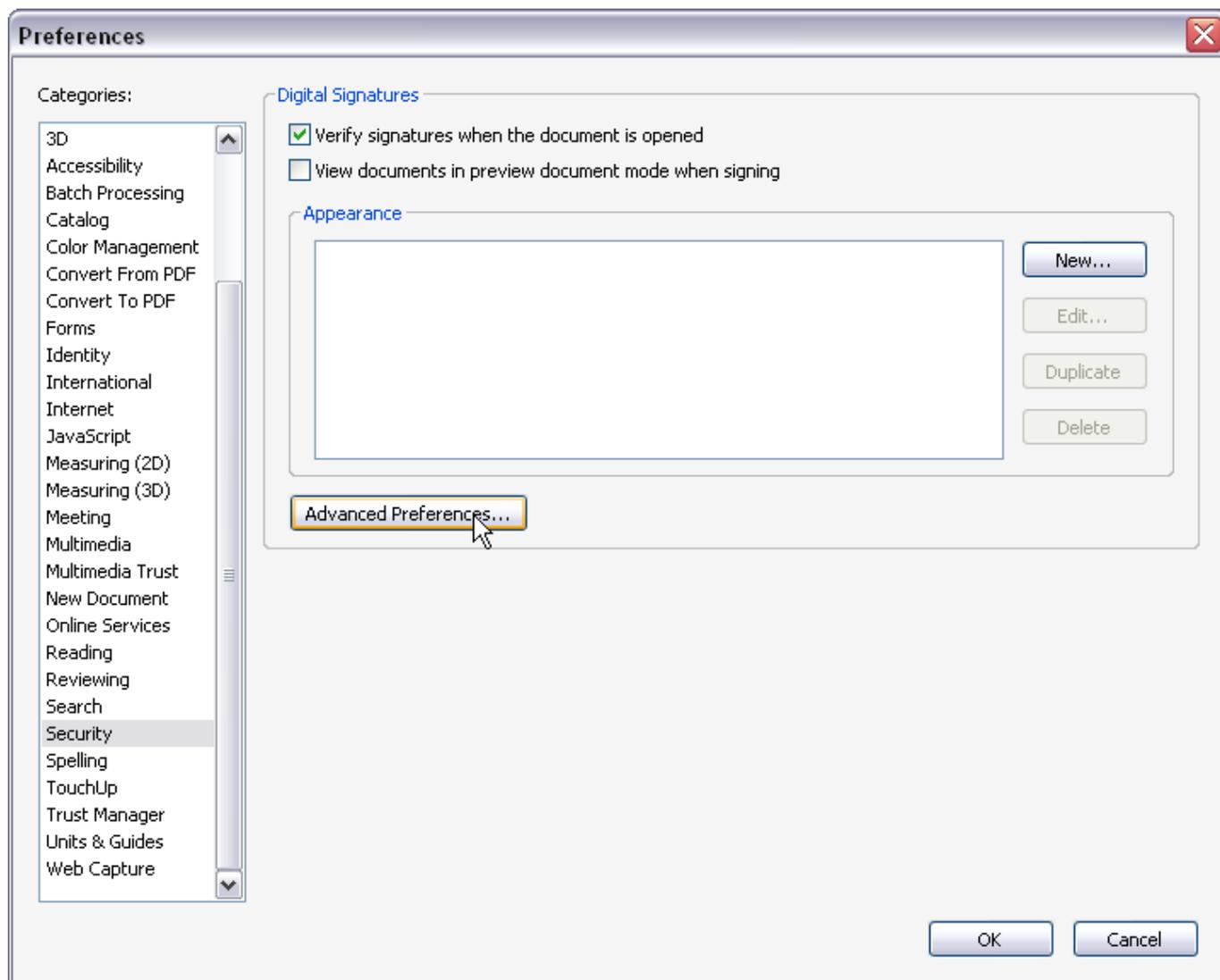


3. Эксплуатация «КриптоПро PDF»

3.1. Настройка формирования и проверки ЭЦП в программе Adobe Acrobat

Настроить формирование и проверку ЭЦП можно в окне «Digital Signatures Advanced Preferences», которое открывается через меню **Edit** ⇒ **Preferences** ⇒ **Security** ⇒ **Advanced preferences** (см. Рисунок 8).

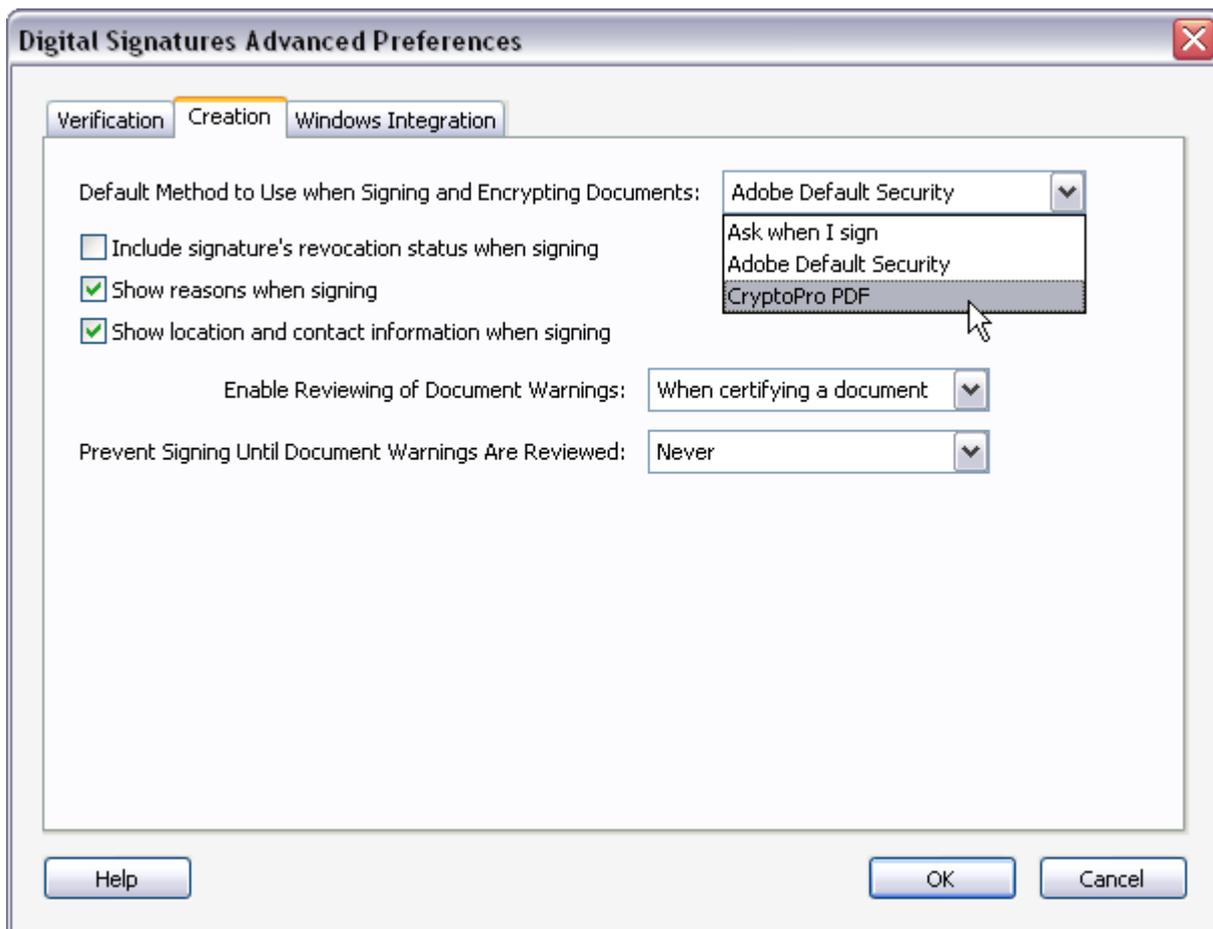
Рисунок 8. Настройка формирования и проверки ЭЦП¹



В открывшемся окне на закладке **Creation** следует назначить метод создания подписи по умолчанию (см. Рисунок 9). При выборе методом по умолчанию **CryptoPro PDF** указанный метод будет использоваться для создания всех ЭЦП, добавляемых в документ. Если же был указан параметр **Ask when I sign**, то для каждой вновь создаваемой подписи будет выведено окно с возможностью выбора метода формирования данной ЭЦП.

¹ Далее все рисунки интерфейса ЭЦП будут представлены для Adobe Acrobat версии 8. Для других версий Adobe Acrobat возможно незначительное отличие в интерфейсе.

Рисунок 9. Настройки формирования ЭЦП



3.2. Ввод серийного номера лицензии «КриптоПро PDF»

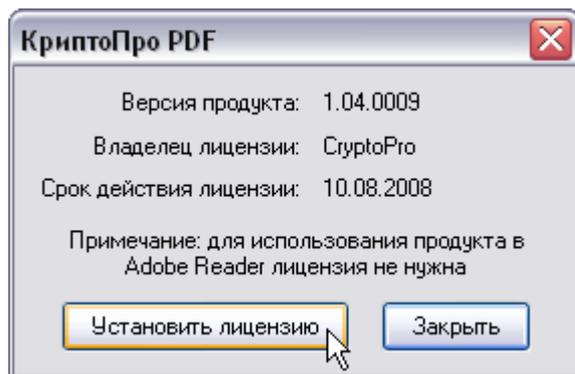
При установке КриптоПро PDF без ввода лицензии пользователю предоставляется лицензия с ограниченным сроком действия. Для использования КриптоПро PDF после окончания этого срока пользователь должен ввести серийный номер с бланка Лицензии, полученной у организации-разработчика или организации, имеющей права распространения продукта.



При использовании КриптоПро PDF в Adobe Reader электронные цифровые подписи будут создаваться и проверяться без лицензии.

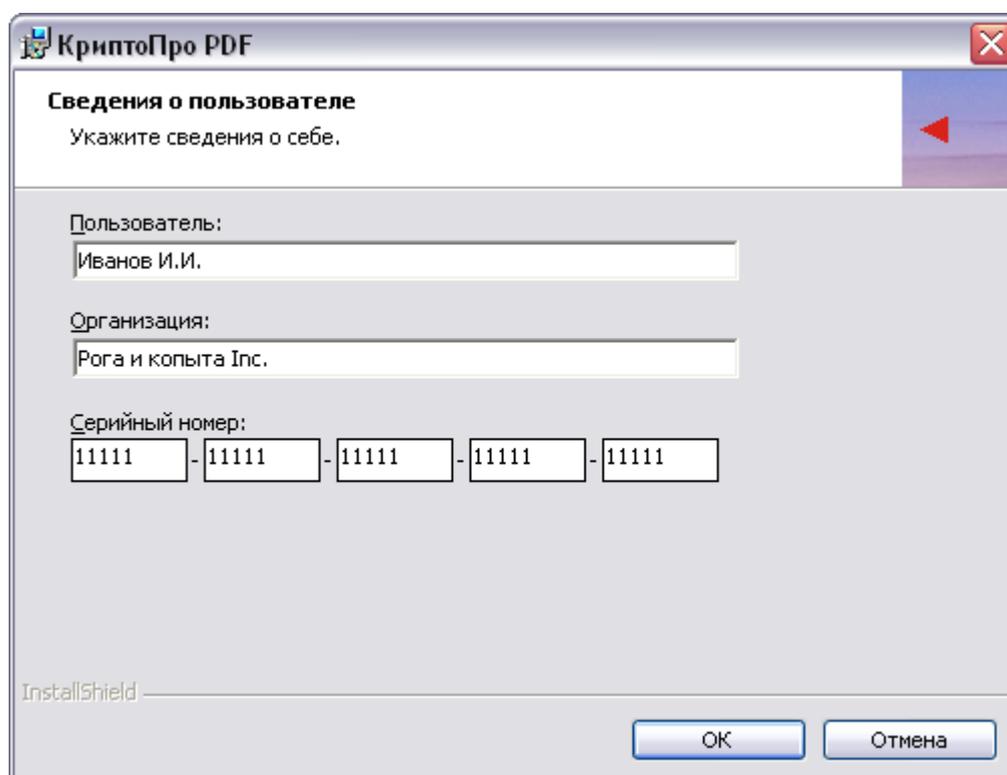
Для ввода серийного номера лицензии следует выбрать пункт меню **Help** ⇒ **About Third-Party Plug-Ins** ⇒ **CryptoProPDF**. В окне информации о КриптоПро PDF (см. Рисунок 10) нажмите кнопку **Установить лицензию**.

Рисунок 10. Панель настройки



Система отобразит окно **Сведения о пользователе**, в котором необходимо указать сведения о пользователе, организации, а также ввести **Серийный номер** с бланка лицензии в соответствующие поля ввода (см. Рисунок 11).

Рисунок 11. Ввод серийного номера лицензии КриптоПро PDF



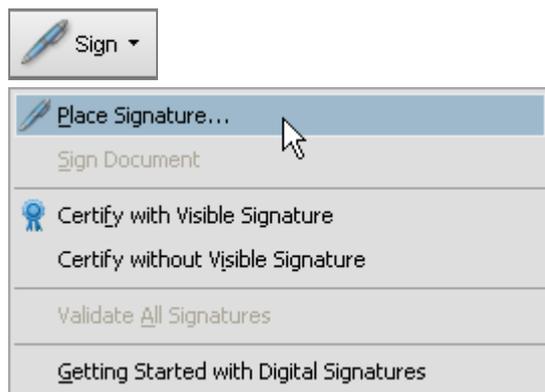
После ввода и нажатия клавиши ОК произойдет возврат к контрольной панели с указанным типом лицензии и сроком ее действия.

3.3. Формирование ЭЦП

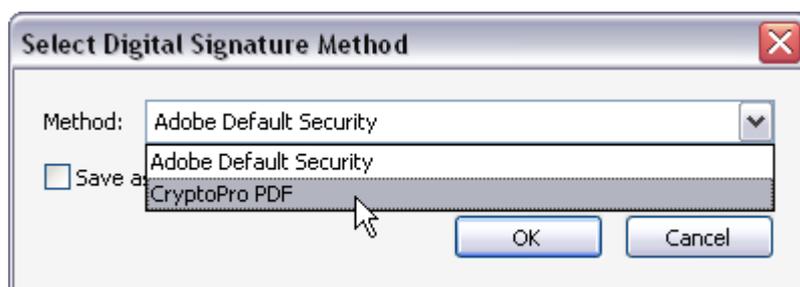
Далее представлен стандартный сценарий формирования видимой¹ ЭЦП:

Выберите пункт меню **Documents** ⇒ **Digital Signatures** ⇒ **Sign this Document...** или нажмите кнопку **Sign**, где в выпадающем меню выберите пункт **Place Signature...** (см. Рисунок 12).

¹ Видимая ЭЦП отображается в документе и может быть отображена на печати. Невидимая ЭЦП не отображается в документе и представляется как метаданные.

Рисунок 12. Добавление ЭЦП

После этого, если при выборе метода создания ЭЦП по умолчанию был указан параметр **Ask when I sign**, будет предоставлено окно для выбора метода формирования ЭЦП. В этом случае необходимо выбрать метод **CryptoPro PDF** (см. Рисунок 13). Если же в настройках (см. п. 3.1) был назначен метод создания ЭЦП по умолчанию, то окно для выбора предоставлено не будет, а указанный метод будет использоваться автоматически.

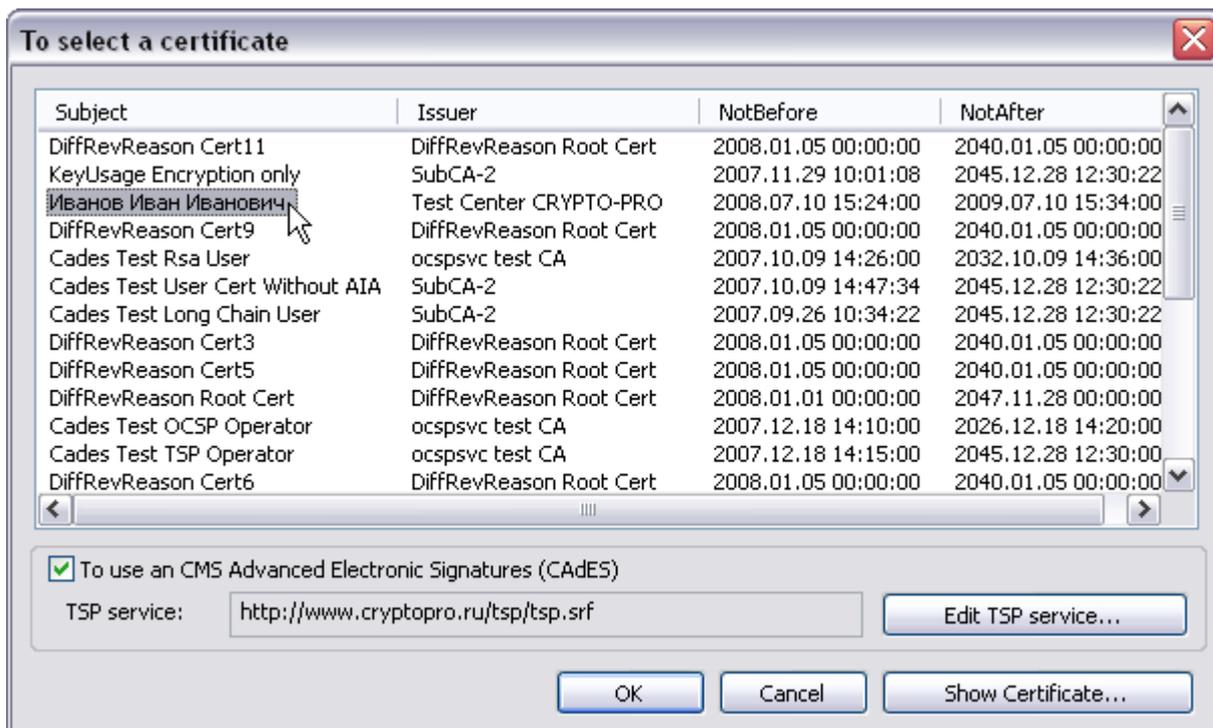
Рисунок 13. Выбор метода создания ЭЦП

Следующим шагом следует выделить в документе область для отображения ЭЦП. После чего в появившемся окне **To select a certificate (Выберите сертификат)** будет представлен список сертификатов, имеющихся в стандартном хранилище сертификатов Windows (см. Рисунок 14).



При выборе сертификата для создания ЭЦП будут доступны только сертификаты с ключами по алгоритму ГОСТ Р 34.10-2001. КриптоПро PDF не предназначен для работы с сертификатами, основанными на других криптографических алгоритмах.

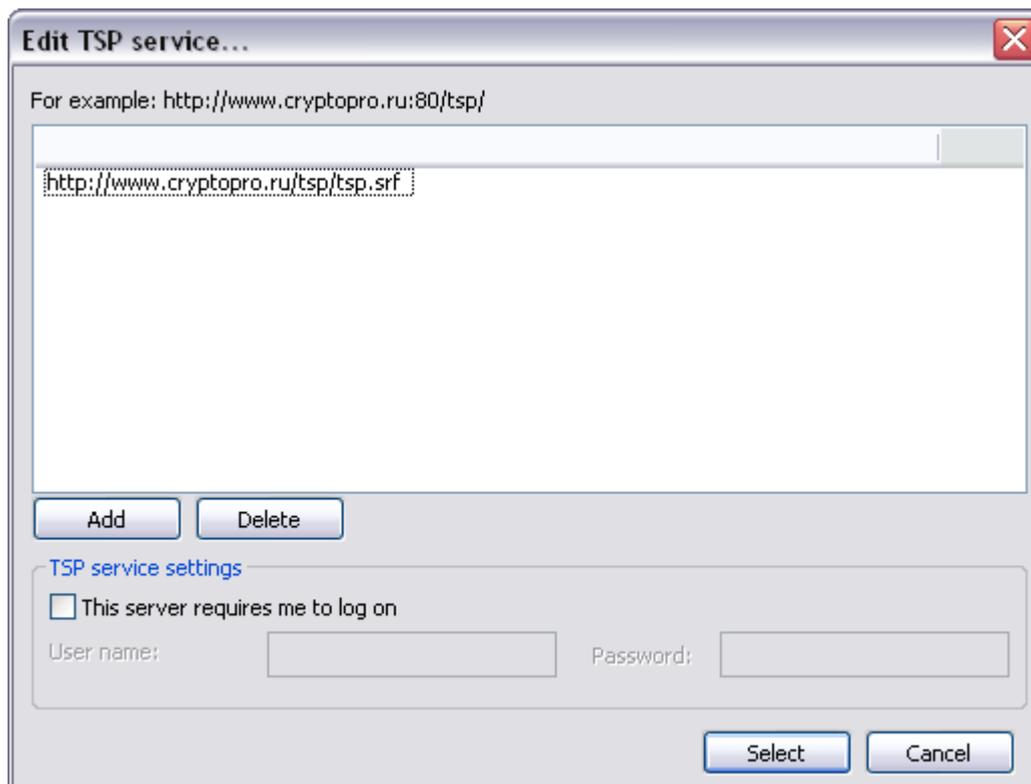
Просмотреть свойства выбранного сертификата можно нажав на кнопку **Show Certificate (Показать сертификат)**.

Рисунок 14. Выбор сертификата для формирования ЭЦП

Для использования усовершенствованной ЭЦП следует отметить пункт **To use an CMS Advanced Electronic Signatures (CAES) (Усовершенствованная ЭЦП)**. В этом случае ЭЦП будет создаваться в соответствии со стандартом CAES ("CMS Advanced Electronic Signatures", ETSI Standard, RTS/ESI-000040, TS 101 733 V1.7.4).

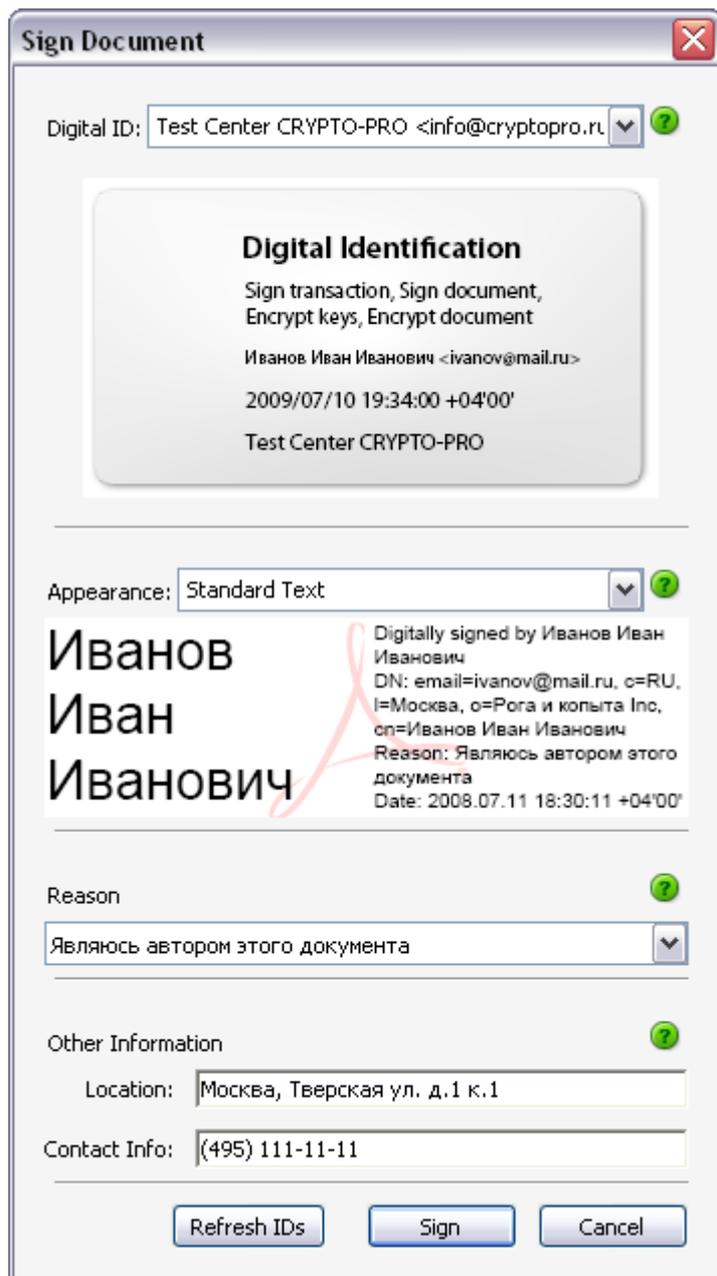
Для создания усовершенствованной подписи необходимо указать адрес службы штампов времени. Для этого следует нажать кнопку **Edit TSP Service (Изменить службу TSP)** (см. Рисунок 15). В случае если служба TSP требует аутентификации, соответствующие параметры также можно задать в окне настройки параметров соединения со службой штампов времени.

Рисунок 15. Выбор и редактирование служб штампов времени



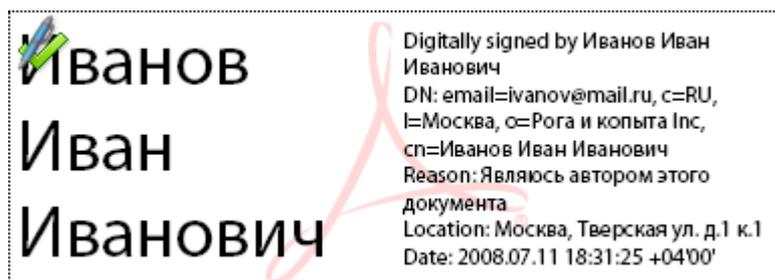
Далее в окне **Sign Document** будет предоставлена возможность заполнить дополнительные поля, отображаемые в свойствах ЭЦП (см. Рисунок 16). Для формирования ЭЦП следует нажать кнопку **Sign**.

Рисунок 16. Окно создания подписи



Последним шагом следует указать файл в окне **Save as**, в который будет сохранена подписанная копия документа. Пример созданной в документе ЭЦП приведен на рисунке (см. Рисунок 17).

Рисунок 17. Пример ЭЦП в документе



3.4. Виды подписей в программах Adobe.

Компания Adobe в своих продуктах разделяет подписи на ЭЦП (в документации Adobe такие подписи называются цифровыми) и подписи от руки.

Подпись от руки представляет собой сделанную вручную пометку на странице, аналогичную рисунку произвольной формы, созданному при помощи инструмента "Карандаш". Подпись от руки не имеет никакого отношения к ЭЦП и не отображается на панели "Подписи".

Большинство цифровых подписей называются **подписями для утверждения**. Подписи, удостоверяющие документ PDF, называются **сертифицирующими**. Лишь первый подписывающий документ PDF (обычно это его автор) может добавить сертифицирующую подпись. Сертифицирующая подпись подтверждает подлинность содержимого документа. Она также позволяет подписавшему указывать типы изменений, разрешенных для документа без нарушения статуса сертифицированного документа. Эти изменения отображаются в панели "Подписи".

Таблица 1. Виды подписей в программах Adobe.

Вид подписи	Отображение в документе	Описание
 Обычная подпись (подпись для утверждения)	Подпись отображается в виде поля подписи в документе, и на панели "Подписи".	Может использоваться для многократного подписания документа PDF несколькими людьми.
 Сертифицирующая подпись	Документ может быть сертифицирован как с видимой, так и без видимой подписи. В первом случае подпись будет отображаться в виде поля подписи в документе и на панели "Подписи". Во втором случае подпись будет отображаться только на панели "Подписи".	Удостоверяет документ PDF. Сертифицирующую подпись можно применять только в том случае, если документ PDF не содержит других подписей. Позволяет указывать типы изменений, разрешенных для документа (добавление комментариев, заполнение форм или добавление обычных подписей) или запретить любые дальнейшие изменения.
Подпись от руки	Рисунок в документе.	Не имеет никакого отношения к ЭЦП.

3.5. Отличия Adobe Reader и Adobe Acrobat при создании ЭЦП.

Отличия в возможностях работы с электронной цифровой подписью в программах Adobe Reader и Adobe Acrobat обусловлены особенностями функционирования этих программ (такова политика их производителя - компании Adobe) и никак не связаны с работой модуля КриптоПро PDF.

Программа Adobe Acrobat позволяет:

- сертифицировать произвольный документ PDF (видимой подписью или без видимой подписи), в том числе на алгоритме ГОСТ Р 34.10-2001 с помощью КриптоПро PDF;
- подписывать произвольный документ PDF (в том числе на алгоритме ГОСТ Р 34.10-2001 с помощью КриптоПро PDF);
- проверять ЭЦП (в том числе на алгоритме ГОСТ Р 34.10-2001 с помощью КриптоПро PDF) в произвольном документе PDF.

Программа Adobe Reader позволяет:

- проверять ЭЦП (в том числе на алгоритме ГОСТ Р 34.10-2001 с помощью КриптоПро PDF) в произвольном документе PDF;
- подписывать документы PDF с расширенным доступом (в том числе на алгоритме ГОСТ Р 34.10-2001 с помощью КриптоПро PDF).

К документам PDF с расширенным доступом относятся PDF-формы, предназначенные для заполнения пользователями в Adobe Reader или PDF-файлы, с которыми проведена операция расширения доступа. Операция расширения доступа или создания PDF-формы может быть осуществлена над произвольным документом PDF, при этом сам документ PDF может быть создан любым доступным способом.

На настоящий момент такая операция доступна в программах Adobe Acrobat 8 Professional, Adobe Acrobat 9 Pro и Adobe Acrobat 9 Pro Extended, Adobe Acrobat X, Adobe Acrobat XI.

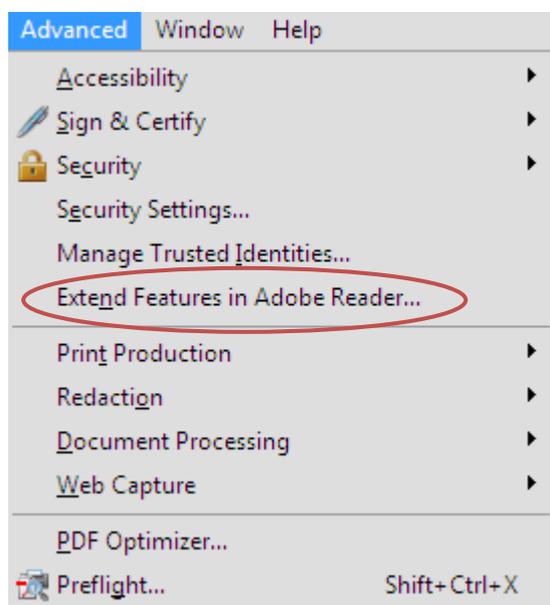
Обратите внимание, что в программе Adobe Acrobat 9 Standard операция расширения доступа присутствует в усеченном виде и ее проведение не даст пользователям Adobe Reader возможности создания или добавления подписи.

3.6. Создание ЭЦП в Adobe Reader

Для того чтобы пользователь получил возможность создания ЭЦП документа в Adobe Reader, необходимо сделать с данным документом ряд предварительных действий в Adobe Acrobat:

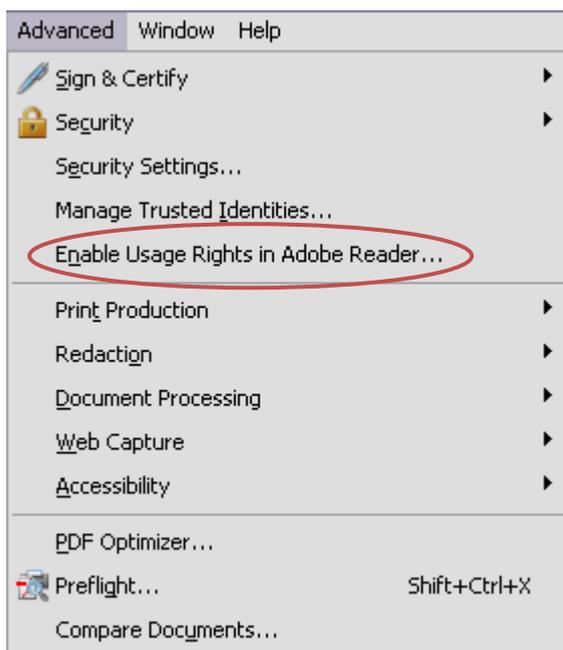
- Открыть документ в программе Adobe Acrobat;
- Для Adobe Acrobat Professional версии 9 - выбрать пункт меню **Advanced** ⇒ **Extend Features in Adobe Reader** (см. Рисунок 18) и в появившемся окне нажать кнопку **Save Now**.

Рисунок 18. Разрешение дополнительных возможностей пользователя в Adobe Acrobat Professional версии 9



- Для Adobe Acrobat Professional версии 8 - выбрать пункт меню **Advanced** ⇒ **Enable Usage Rights in Adobe Reader** (см. Рисунок 19) и в появившемся окне нажать кнопку **Save Now**.

Рисунок 19. Разрешение дополнительных возможностей пользователя в Adobe Acrobat Professional версии 8



- Сохранить документ.

После выполнения описанных действий в данном документе появится возможность создания ЭЦП в программе Adobe Reader. Процесс формирования ЭЦП описан в п.п. 3.3 настоящего Руководства.

3.7. Проверка ЭЦП

По умолчанию при открытии документа проверяются все имеющиеся в нем ЭЦП.

Чтобы просмотреть результат проверки отдельной ЭЦП, следует нажать левую кнопку мыши на данной электронной цифровой подписи в документе. В результате выбранная подпись будет подвергнута проверке и появится окно **Signature Validation Status (Результат проверки подписи)** (см. Рисунок 20).

Рисунок 20. Результат проверки подписи



Подпись может иметь один из следующих статусов (см. Таблица 2):

- **ДЕЙСТВИТЕЛЬНА**, если с момента подписания, подписанные данные не были изменены.
- **НЕДЕЙСТВИТЕЛЬНА**, если с момента подписания, подписанные данные были изменены или повреждены.

- **НЕОПРЕДЕЛЕНА**, если по каким-либо причинам не удалось проверить подпись, либо подписанные данные не были изменены, но сертификат подписавшего определен как недоверенный.

Сертификат считается доверенным, если одновременно выполняются следующие условия:

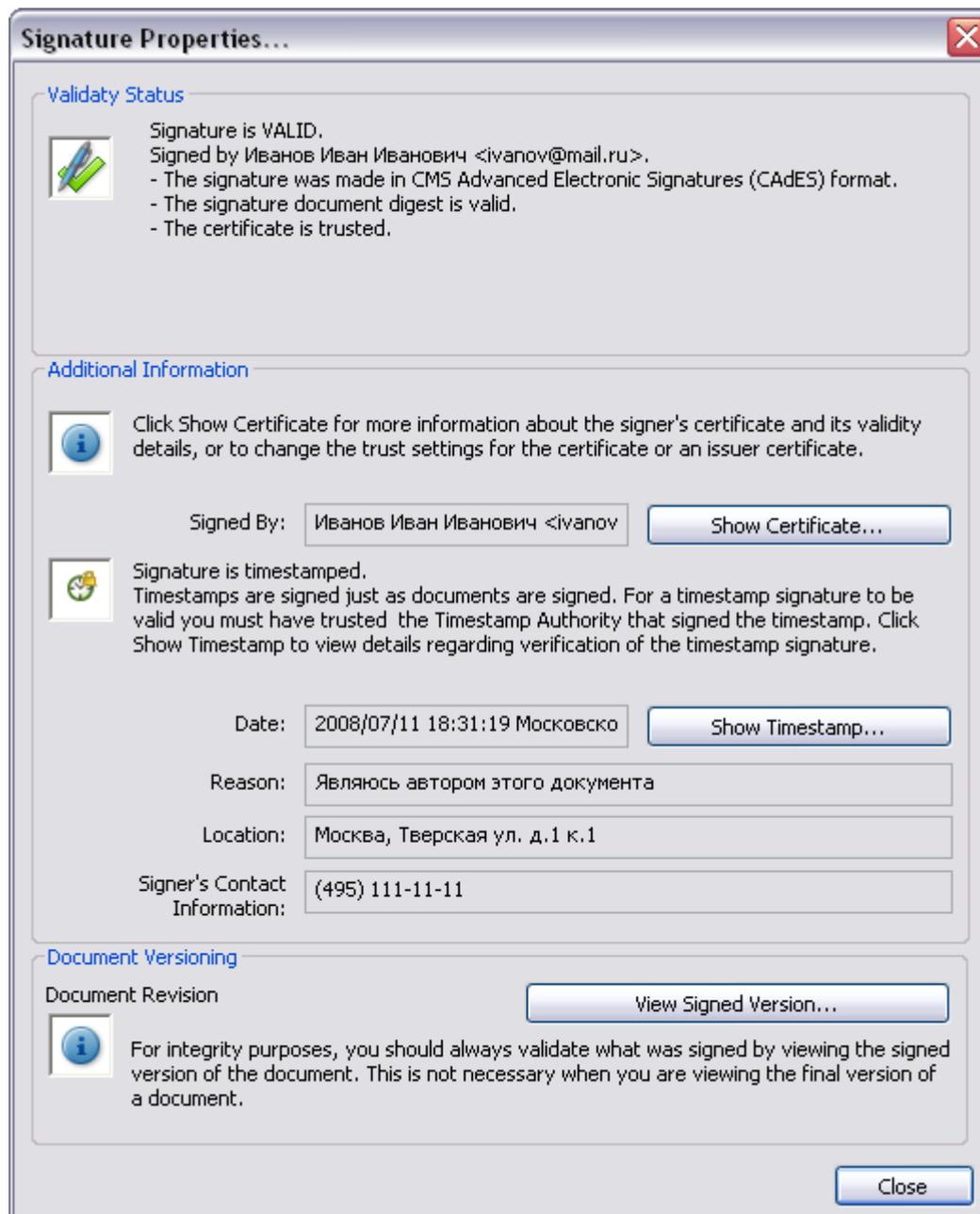
1. Сертификат имеет корректную ЭЦП центра сертификации, выдавшего сертификат.
2. Сертификат актуален на текущую дату по сроку действия.
3. Сертификат центра сертификации, выдавшего сертификат, установлен в хранилище (ROOT) доверенных корневых сертификатов Windows.
4. Сертификат отсутствует в актуальном на текущую дату списке отозванных сертификатов.

Таблица 2. Перечень статусов электронной цифровой подписи

Иконка	Статус	Описание
	ДЕЙСТВИТЕЛЬНА	Подписанные данные не были изменены с момента подписания.
	ДЕЙСТВИТЕЛЬНА	Подписанные данные не были изменены с момента подписания. Однако в сам документ были внесены изменения.
	НЕДЕЙСТВИТЕЛЬНА	Подписанные данные документа были изменены или повреждены после подписания.
	НЕОПРЕДЕЛЕНА	Подписанные данные не были изменены с момента подписания. Однако сертификат подписавшего определен как недействителен.
	НЕОПРЕДЕЛЕНА	Подписанные данные не были изменены с момента подписания, но в сам документ были внесены изменения. И сертификат подписавшего определен как недействителен.
	НЕОПРЕДЕЛЕНА	На стадии проверки подписи возникли ошибки.

Окно с параметрами подписи можно вызвать нажатием кнопки **Signature Properties (Параметры подписи)** в окне **Результат проверки подписи**. Либо выделить пункт **Show Signature Properties** в контекстном меню, вызываемом по нажатию правой кнопки на область ЭЦП в документе.

Рисунок 21. Параметры подписи



4. Перечень сокращений

ДПМ	Дополнительный программный модуль (plug-in)
ПК	Программный комплекс
СКЗИ	Средство криптографической защиты информации
ЭЦП	Электронно-цифровая подпись
PDF	Portable Document Format, платформонезависимый формат электронных документов
TSP	Time-Stamp Protocol

5. Перечень рисунков

Рисунок 1. Мастер установки «КриптоПро PDF»	5
Рисунок 2. Лицензионное соглашение на использование «КриптоПро PDF»	6
Рисунок 3. Сведения о пользователе «КриптоПро PDF»	6
Рисунок 4. Вид установки «КриптоПро PDF»	7
Рисунок 5. Выборочная установка «КриптоПро PDF»	7
Рисунок 6. Окно подтверждения установки «КриптоПро PDF»	8
Рисунок 7. Завершение работы мастера установки	9
Рисунок 8. Настройка формирования и проверки ЭЦП	10
Рисунок 9. Настройки формирования ЭЦП	11
Рисунок 10. Панель настройки	12
Рисунок 11. Ввод серийного номера лицензии КриптоПро PDF	12
Рисунок 12. Добавление ЭЦП	13
Рисунок 13. Выбор метода создания ЭЦП	13
Рисунок 14. Выбор сертификата для формирования ЭЦП	14
Рисунок 15. Выбор и редактирование служб штампов времени	15
Рисунок 16. Окно создания подписи	16
Рисунок 17. Пример ЭЦП в документе	16
Рисунок 18. Разрешение дополнительных возможностей пользователя в Adobe Acrobat Professional версии 9	18
Рисунок 19. Разрешение дополнительных возможностей пользователя в Adobe Acrobat Professional версии 8	19
Рисунок 20. Результат проверки подписи	19
Рисунок 21. Параметры подписи	21

6. Перечень таблиц

Таблица 1. Виды подписей в программах Adobe.	17
Таблица 2. Перечень статусов электронной цифровой подписи	20