БыстроБанк

РЕГЛАМЕНТ
предоставления услуг Оператора Удостоверяющего центра
ООО "КРИПТО-ПРО"
(редакция утверждена И.о. Президента ПАО “БыстроБанк”13.06.2018)

г. Ижевск

1.Сведения об Операторе Удостоверяющего центра

Публичное акционерное общество "БыстроБанк", именуемое в дальнейшем "Оператор Удостоверяющего центра" ("Оператор"), зарегистрировано на территории Российской Федерации за основным государственным регистрационным номером 1021800001508, Книга государственной регистрации кредитных организаций: регистрационный номер 1745.

Реквизиты:
Полное наименование: Публичное акционерное общество "БыстроБанк"
Юридический адрес: 426008, Удмуртская Республика, г.Ижевск, ул.Пушкинская, 268
Фактический адрес: 426008, Удмуртская Республика, г.Ижевск, ул.Пушкинская, 268
Адрес для корреспонденции: 426008, Удмуртская Республика, г.Ижевск, ул.Пушкинская, 268
Банковские реквизиты:

- ПАО "БыстроБанк"
- БИК 049401814
- К/с 30101810200000000814 в Отделении - НБ Удмуртская республика

ИНН/КПП: 1831002591/183101001
ОГРН: 1021800001508
Контактные телефоны, факс, адрес электронной почты:

- тел./факс +7 (3412) 908-090, +7 (3412) 723-969; e-mail: contact@bystrobank.ru
- звонок по России 8-800-333-22-65

2.Сведения об Удостоверяющем центре

Общество с ограниченной ответственностью "КРИПТО-ПРО", именуемое в дальнейшем "Удостоверяющий центр", зарегистрировано на территории Российской Федерации в городе Москва. Свидетельство о регистрации N 001.602.749, выдано 16.11.1999 г. Московской регистрационной палатой, Свидетельство о внесении записи в ЕГРЮЛ за основным государственным регистрационным номером 1037700085444 от 29.01.2003 г., Свидетельство о внесении записи в ЕГРЮЛ в связи с государственной регистрацией изменений, вносимых в учредительные документы юридического лица за государственным регистрационным номером 2037719011031 от 12.03.2003 г.

Удостоверяющий центр в качестве профессионального участника рынка услуг по изготовлению и выдаче сертификатов ключей проверки электронных подписей осуществляет свою деятельность на территории Российской Федерации на основании следующей лицензии:

Лицензия Центра по лицензированию, сертификации и защите государственной тайны ФСБ России рег. N 12936 Н от 11 июня 2013 г. на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя).

Контактные телефоны, факс, адрес электронной почты ООО "КРИПТО-ПРО":
тел./факс +7 (495) 995-48-20, +7 (495) 984-07-90; e-mail: cpca@cryptopro.ru
Портал технической поддержки:
https://support.cryptopro.ru/

3.Термины и определения

Владелец сертификата ключа проверки электронной подписи (Владелец) — лицо, на имя которого Удостоверяющим центром выдан сертификат ключа проверки электронной подписи и которое владеет соответствующим ключом электронной подписи, позволяющим с помощью средств электронной подписи создавать свою электронную подпись в электронных документах (подписывать электронные документы).

Информационная система — корпоративная информационная система, устроителем которой является организатор системы, в которой используются ключи электронной подписи и сертификаты ключей проверки электронной подписи, и предоставляющей определенные услуги участникам этой системы.

Ключ электронной подписи (закрытый ключ электронной цифровой подписи, закрытый ключ подписи) — уникальная последовательность символов, известная владельцу сертификата ключа проверки электронной подписи и предназначенная для создания в электронных документах электронной подписи с использованием средств электронной подписи.

Ключ электронной подписи действует на определенный момент времени (действующий ключ электронной подписи) если:

- наступил момент времени начала действия ключа электронной подписи;
- срок действия ключа электронной подписи не истек;
- сертификат ключа проверки электронной подписи, соответствующий данному ключу электронной подписи, действует на указанный момент времени.

Ключ проверки электронной подписи (открытый ключ электронной цифровой подписи, открытый ключ подписи) — уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для подтверждения с использованием средств электронной подписи подлинности электронной подписи в электронном документе.

Копия сертификата ключа проверки электронной подписи — документ на бумажном носителе, содержащий информацию из сертификата ключа проверки электронной подписи и заверенный собственноручной подписью уполномоченного лица Оператора Удостоверяющего центра и печатью Оператора Удостоверяющего центра либо печатью и подписью уполномоченного лица Удостоверяющего центра.

Оператор Удостоверяющего центра (Оператор) — Публичное акционерное общество "БыстроБанк", наделенное Удостоверяющим центром полномочиями по осуществлению действий по регистрации и управлению сертификатами ключей проверки электронных подписей Пользователей Удостоверяющего центра — полномочных представителей Стороны, присоединившейся к Регламенту.

Пользователь Удостоверяющего центра (Пользователь УЦ, Пользователь) — физическое лицо, зарегистрированное в Удостоверяющем центре и являющееся полномочным представителем Стороны, присоединившейся к Регламенту.

Псевдоним владельца сертификата ключа подписи — вымышленное имя физического лица, которое он сознательно и легально принимает для регистрации в Удостоверяющем центре.

Рабочий день Оператора Удостоверяющего центра (далее — рабочий день) — промежуток времени с 10:00 по 18:00 (время Московское) каждого дня недели за исключением выходных и праздничных дней.

Реестр Удостоверяющего центра — набор документов Удостоверяющего центра в электронной и/или бумажной форме, включающий следующую информацию:

- реестр заявлений на регистрацию в Удостоверяющем центре;
- реестр зарегистрированных пользователей Удостоверяющего центра;
- реестр заявлений на изготовление сертификата ключа проверки электронной подписи;
- реестр заявлений на аннулирование (отзыв) сертификата ключа проверки электронной подписи;
- реестр заявлений на приостановление/возобновление действия сертификата ключа проверки электронной подписи;
- реестр заявлений на подтверждение подлинности электронной подписи в электронном документе;

- реестр заявлений на подтверждение электронной подписи уполномоченного лица Удостоверяющего центра в изданных сертификатах;
- реестр сертификатов ключей проверки электронной подписи;
- реестр изготовленных списков отозванных сертификатов.

Сертификат ключа проверки электронной подписи (сертификат ключа электронной цифровой подписи, сертификат открытого ключа, сертификат ключа подписи) — неквалифицированный сертификат ключа проверки электронной подписи, являющийся электронным документом с электронной подписью уполномоченного лица Удостоверяющего центра, структура которого определяется настоящим Регламентом и который изготавливается Удостоверяющим центром для подтверждения подлинности электронной подписи и идентификации владельца сертификата ключа проверки электронной подписи.

Сертификат ключа проверки электронной подписи действует на определенный момент времени (действующий сертификат) если:

- наступил момент времени начала действия сертификата ключа проверки электронной подписи;
- срок действия сертификата ключа проверки электронной подписи не истек;
- сертификат ключа проверки электронной подписи не аннулирован, не прекратил действие и действие его не приостановлено.

Служба актуальных статусов сертификатов — сервис Удостоверяющего центра, обеспечивающий информирование пользователей о статусе сертификатов ключей проверки электронной подписей по протоколу OCSP (Online Certificate Status Protocol).

Список отозванных сертификатов (СОС) — электронный документ с электронной подписью уполномоченного лица Удостоверяющего центра, включающий в себя список серийных номеров сертификатов, которые на определенный момент времени были отозваны или действие которых было приостановлено.

Служба штампов времени — сервис Удостоверяющего центра, обеспечивающий предоставление Пользователям Удостоверяющего центра штампов времени по протоколу TSP (Time-Stamp Protocol).

Средство электронной подписи (средство электронной цифровой подписи) — средство криптографической защиты информации (СКЗИ) "КриптоПро CSP", обеспечивающее реализацию следующих функций — создание электронной подписи в электронном документе с использованием ключа электронной подписи, подтверждение с использованием ключа проверки электронной подписи подлинности электронной подписи в электронном документе, создание ключей электронных подписей и ключей проверки электронных подписей.

Удостоверяющий центр — ООО "КРИПТО-ПРО", осуществляющее выполнение целевых функций удостоверяющего центра по изготовлению и управлению неквалифицированными сертификатами ключей проверки электронной подписи в соответствии с Федеральным законом от 06.04.2011 N 63-ФЗ "Об электронной подписи" в целях обеспечения применения участниками Информационной системы неквалифицированной усиленной электронной подписи.

Уполномоченное лицо Удостоверяющего центра — физическое лицо, являющееся сотрудником Удостоверяющего центра и наделенное Удостоверяющим центром полномочиями по заверению сертификатов ключа проверки электронной подписи и списков отозванных сертификатов.

Штамп времени электронного документа (штамп времени) — электронный документ, подписанный электронной подписью и устанавливающий существование определенного электронного документа на момент времени, указанный в штампе.

Электронная подпись (ЭП, электронная цифровая подпись, ЭЦП) — информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией. Под Электронной подписью в настоящем Регламенте понимается усиленная неквалифицированная электронная подпись, являющаяся реквизитом электронного документа, предназначенным для защиты данного электронного документа от подделки, полученная в результате криптографического преобразования информации с использованием ключа электронной подписи и позволяющая идентифицировать владельца сертификата ключа проверки электронной подписи, а также установить отсутствие искажения информации в электронном документе.

Электронный документ — документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных

вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

Cryptographic Message Syntax (CMS) — стандарт криптографических сообщений, описанный в RFC 3852 и RFC 3369. Удостоверяющий центр использует в своей работе криптографические сообщения, соответствующие данному стандарту с учетом 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)".

Online Certificate Status Protocol (OCSP) — протокол установления статуса сертификата ключа проверки электронной подписи, реализующий RFC 2560 "X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol — OCSP".

Public Key Cryptography Standarts (PKCS) — стандарты криптографии с ключом проверки электронной подписи, разработанные компанией RSA Security. Удостоверяющий центр осуществляет свою работу в соответствии со следующим стандартом PKCS: PKCS#10 — стандарт, определяющий формат и синтаксис запроса на сертификат ключа проверки электронной подписи.

Time-Stamp Protocol (TSP) — протокол получения штампа времени, реализующий RFC 3161 "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)".

4.Общие положения

4.1.Статус Регламента

4.1.1.Настоящий Регламент предоставления услуг Оператора Удостоверяющего центра ООО "КРИПТО-ПРО" (далее — Регламент) является договором присоединения в соответствии со статьей 428 Гражданского кодекса Российской Федерации.

4.1.2.Сторонами Регламента (далее — Стороны) являются Публичное акционерное общество "БыстроБанк", выступающее Оператором, и Сторона, присоединившаяся к Регламенту. В качестве Стороны выступает юридическое лицо, индивидуальный предприниматель или физическое лицо, занимающееся в установленном законодательством Российской Федерации порядке частной практикой — действующий клиент Публичного акционерного общества "БыстроБанк".

4.1.3.Регламент размещается на официальном сайте Оператора www.bystrobank.ru.

4.2.Присоединение к Регламенту

4.2.1.Присоединение к Регламенту осуществляется путем совершения представителем Стороны (Пользователем) конклюдентных действий. Акцепт считается совершенным с момента начала выполнения всех необходимых действий по получению сертификата ключа проверки электронной подписи в соответствии с настоящим Регламентом.

4.2.2.Факт присоединения лица к Регламенту является полным принятием условий настоящего Регламента и всех его приложений в редакции, действующей на момент подписания Соглашения.

4.2.3.После присоединения к Регламенту в установленном порядке Стороны вступают в соответствующие договорные отношения на неопределенный срок.

4.2.4.Каждая из Сторон вправе без обращения в суд расторгнуть настоящий Регламент, письменно уведомив другую сторону за 30 календарных дней до дня расторжения. При этом Стороны в течение срока предупреждения до дня прекращения действия Регламента обязаны разрешить между собой все денежные и иные имущественные вопросы, связанные с настоящим Регламентом.

4.2.5.Прекращение действия Регламента не освобождает стороны от исполнения обязательств, возникших до указанного дня прекращения действия Регламента, и не освобождает от ответственности за его неисполнение (ненадлежащее исполнение).

4.3.Применение Регламента

4.3.1.Стороны понимают термины, применяемые в настоящем Регламенте, строго в контексте общего смысла Регламента.

4.3.2.В случае противоречия и/или расхождения названия какого-либо раздела Регламента со смыслом какого-либо пункта в нем содержащегося, Стороны считают доминирующим смысл и формулировки каждого конкретного пункта.

4.3.3.В случае противоречия и/или расхождения положений какого-либо приложения к настоящему Регламенту с положениями собственно Регламента, Стороны считают доминирующим смысл и формулировки Регламента.

4.4.Изменение (дополнение) Регламента.

4.4.1.Внесение изменений (дополнений) в Регламент, включая приложения к нему, производится Оператором в одностороннем порядке.

4.4.2.Уведомление присоединившейся стороны о внесении изменений (дополнений) в Регламент осуществляется Оператором путем оповещения присоединившейся стороны по каналу связи в соответствии с Соглашением.

4.4.3.Все изменения (дополнения), вносимые Оператором в Регламент по собственной инициативе и не связанные с изменением законодательства Российской Федерации, вступают в силу и становятся обязательными для присоединившейся стороны по истечении календарных суток с даты уведомления присоединившейся стороны о внесении указанных изменений (дополнений).

4.4.4.Все изменения (дополнения), вносимые Оператором в Регламент в связи с изменением действующего законодательства Российской Федерации вступают в силу одновременно с вступлением в силу изменений (дополнений) в указанных актах.

4.4.5.Любые изменения и дополнения в Регламенте с момента вступления в силу равно распространяются на всех лиц, присоединившихся к Регламенту, в том числе присоединившихся к Регламенту ранее даты вступления изменений (дополнений) в силу. В случае несогласия с изменениями (дополнениями) присоединившаяся сторона имеет право до вступления в силу таких изменений (дополнений) на расторжение Регламента в порядке, предусмотренном п.4.2.4. настоящего Регламента.

4.4.6.Все приложения, изменения и дополнения к настоящему Регламенту являются его составной и неотъемлемой частью.

5.Права и обязанности сторон

5.1.Оператор обязан:

5.1.1.Предоставить Пользователю Удостоверяющего центра сертификат ключа проверки электронной подписи уполномоченного лица Удостоверяющего центра.

5.1.2.Обеспечить регистрацию пользователей в Удостоверяющем центре по заявлениям на регистрацию в Удостоверяющем центре, в соответствии с порядком, определенным в настоящем Регламенте.

5.1.3.Занести регистрационную информацию Пользователей Удостоверяющего центра в Реестр Удостоверяющего центра.

5.1.4.Обеспечить изготовление сертификата ключа проверки электронной подписи зарегистрированного в Удостоверяющем центре лица по запросам на изготовление сертификата ключа подписи, в соответствии с порядком, определенным в настоящем Регламенте и уведомить об этом владельца изготовленного сертификата ключа подписи.

5.1.5.Аннулировать (отозвать) сертификат ключа проверки электронной подписи Пользователя Удостоверяющего центра по заявлению на аннулирование (отзыв) сертификата ключа проверки электронной подписи, в соответствии с порядком, определенным в настоящем Регламенте.

5.1.6.Приостановить действие сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра по заявлению на приостановление действия сертификата ключа проверки электронной подписи, в соответствии с порядком, определенным в настоящем Регламенте.

5.1.7.Возобновить действие сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра по заявлению на возобновление действия сертификата ключа проверки электронной подписи (исключительно в случае поступления заявления в период срока, на который действие сертификата было приостановлено), в соответствии с порядком, определенным в настоящем Регламенте.

5.2.Сторона, присоединившаяся к Регламенту, обязана:

5.2.1.Известить Оператора об изменениях в наименовании Организации, государственного регистрационного номера, идентификационного номера налогоплательщика и по требованию Оператора предоставить подтверждающие документы в течение 5 рабочих дней с момента регистрации изменений.

5.2.2.Пользователь Удостоверяющего центра, являющийся полномочным представителем присоединившейся Стороны обязан:

5.2.2.1.Сформировать ключ электронной подписи и ключ проверки электронной подписи на своем рабочем месте только с использованием средства электронной подписи и программного обеспечения, предоставляемого Удостоверяющим центром или Оператором.

5.2.2.2.Хранить в тайне ключ электронной подписи, принимать все возможные меры для предотвращения его потери, раскрытия, искажения и несанкционированного использования.

5.2.2.3.Применять для формирования электронной подписи только действующий ключ электронной подписи.

5.2.2.4.Не применять ключ электронной подписи, если ему стало известно, что этот ключ используется или использовался ранее другими лицами.

5.2.2.5.Применять ключ электронной подписи только в соответствии с областями использования, указанными в соответствующем данному ключу сертификате ключа проверки электронной подписи (поля Key Usage, Extended Key Usage сертификата ключа подписи).

5.2.2.6.Немедленно обратиться к Оператору с заявлением на приостановление действия сертификата ключа проверки электронной подписи в случае потери, раскрытия, искажения ключа электронной подписи, а также в случае если Пользователю Удостоверяющего центра стало известно, что этот ключ электронной подписи используется или использовался ранее другими лицами.

5.2.2.7.Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, заявление на аннулирование (отзыв) которого подано на рассмотрение Оператору, в течение времени, исчисляемого с момента времени подачи заявления на аннулирование (отзыв) сертификата по момент времени официального уведомления об аннулировании (отзыве) сертификата.

5.2.2.8.Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, заявление на приостановление действия которого подано на рассмотрение Оператору, в течение времени, исчисляемого с момента времени подачи заявления на приостановление действия сертификата по момент времени официального уведомления о приостановлении действия сертификата.

5.3.Оператор имеет право:

5.3.1.Отказать в регистрации в Удостоверяющем центре уполномоченному представителю Стороны, присоединившейся к Регламенту, в случае ненадлежащего оформления необходимых регистрационных документов.

5.3.2.Отказать в изготовлении сертификата ключа проверки электронной подписи пользователя Удостоверяющего центра в случае ненадлежащего оформления запроса на изготовление сертификата ключа проверки электронной подписи.

5.3.3.Отказать в аннулировании (отзыве) сертификата ключа проверки электронной подписи пользователя Удостоверяющего центра в случае ненадлежащего оформления заявления на аннулирование (отзыв) сертификата ключа проверки электронной подписи.

5.3.4.Отказать в приостановлении/возобновлении действия сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра в случае ненадлежащего оформления заявления на приостановление/возобновление действия сертификата ключа проверки электронной подписи.

5.3.5.Отказать в аннулировании (отзыве) сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра в случае, если истек установленный срок действия ключа электронной подписи, соответствующего этому сертификату.

5.3.6.Отказать в приостановлении действия сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра в случае, если истек установленный срок действия ключа электронной подписи, соответствующего этому сертификату.

5.3.7.Отказать в возобновлении действия сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра в случае, если истек установленный срок действия ключа электронной подписи, соответствующего этому сертификату.

5.3.8.Отказать в изготовлении сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра в случае, если использованное Пользователем Удостоверяющего центра для формирования запроса на сертификат ключа проверки электронной подписи средство криптографической защиты информации не поддерживается Удостоверяющим центром.

5.3.9.В одностороннем порядке приостановить действие сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра с обязательным уведомлением Владельца сертификата ключа проверки электронной подписи, действие которого приостановлено, и указанием обоснованных причин.

5.4.Сторона, присоединившаяся к Регламенту, имеет право:

5.4.1.Получить сертификат ключа проверки электронной подписи уполномоченного лица Удостоверяющего центра.

5.4.2.Получить список отозванных сертификатов ключей проверки электронной подписи, изготовленный Удостоверяющим центром.

5.4.3.Применять сертификат ключа проверки электронной подписи уполномоченного лица Удостоверяющего центра для проверки электронной подписи уполномоченного лица Удостоверяющего

центра в сертификатах ключей проверки электронной подписи, изготовленных Удостоверяющим центром.

5.4.4.Применять список отозванных сертификатов ключей проверки электронной подписи, изготовленный Удостоверяющим центром, для проверки статуса сертификатов ключей проверки электронной подписи, изготовленных Удостоверяющим центром.

5.4.5.Применять сертификат ключа проверки электронной подписи Пользователя Удостоверяющего центра для проверки электронной подписи электронных документов в соответствии со сведениями, указанными в сертификате ключа проверки электронной подписи.

5.4.6.Воспользоваться предоставляемыми Удостоверяющим центром программными средствами для передачи по линиям связи в Удостоверяющий центр заявления на регистрацию в электронном виде.

5.4.7.Воспользоваться предоставляемыми Удостоверяющим центром программными средствами для передачи по линиям связи в Удостоверяющий центр заявления на изготовление сертификата ключа проверки электронной подписи в электронном виде.

5.4.8.Воспользоваться предоставляемыми Удостоверяющим Центром программными средствами, чтобы получить и установить на свое рабочее место изготовленный Удостоверяющим центром сертификат ключа проверки электронной подписи.

5.4.9.Для хранения ключа электронной подписи применять любой носитель, поддерживаемый средством электронной подписи.

5.4.10.Воспользоваться предоставляемыми Удостоверяющим центром программными средствами для передачи по линиям связи в Удостоверяющий центр заявления на аннулирование (отзыв) сертификата ключа проверки электронной подписи в электронном виде.

5.4.11.Воспользоваться предоставляемыми Удостоверяющим центром программными средствами для передачи по линиям связи в Удостоверяющий центр заявления на приостановление действия сертификата ключа проверки электронной подписи в электронном виде.

5.4.12.Воспользоваться предоставляемыми Удостоверяющим центром программными средствами для передачи по линиям связи в Удостоверяющий центр заявления на возобновление действия сертификата ключа проверки электронной подписи в электронном виде.

5.4.13.Обратиться к Оператору для аннулирования (отзыва) сертификата ключа проверки электронной подписи в течение срока действия соответствующего ключа электронной подписи.

5.4.14.Обратиться к Оператору для приостановления действия сертификата ключа проверки электронной подписи в течение срока действия соответствующего ключа электронной подписи.

5.4.15.Обратиться к Оператору для возобновления действия сертификата ключа проверки электронной подписи в течение срока действия соответствующего ключа электронной подписи и срока, на который действие сертификата было приостановлено.

6.Ответственность сторон

6.1.Стороны не несут ответственность за неисполнение либо ненадлежащее исполнение своих обязательств по настоящему Регламенту, а также возникшие в связи с этим убытки в случаях, если это является следствием встречного неисполнения либо ненадлежащего встречного исполнения другой Стороной своих обязательств.

6.2.Ответственность Сторон, не урегулированная положениями настоящего Регламента, регулируется законодательством Российской Федерации.

7.Разрешение споров

7.1.Сторонами в споре, в случае его возникновения, считаются Оператор и Сторона, присоединившаяся к Регламенту.

7.2.При рассмотрении спорных вопросов, связанных с настоящим Регламентом, Стороны будут руководствоваться законодательством Российской Федерации.

7.3.Стороны будут принимать все необходимые меры к тому, чтобы в случае возникновения спорных вопросов решить их путем переговоров.

7.4.Спорные вопросы между Сторонами, неурегулированные путем переговоров, решаются в соответствии с законодательством Российской Федерации.

8.Порядок предоставления и пользования услугами Удостоверяющего центра

8.1.Регистрация Пользователей Оператором

8.1.1.Регистрация пользователя и изготовление первого сертификата в распределенном режиме

Оператор предоставляет пользователю сертификат ключа проверки электронной подписи уполномоченного лица Удостоверяющего центра и актуальный список отозванных сертификатов в виде файлов на официальном сайте Оператора www.bystrobank.ru, а также адрес web-страницы регистрации в Удостоверяющем центре.

Пользователь производит установку и настройку своего рабочего места и с помощью автоматизированного рабочего места (АРМ) пользователя Удостоверяющего центра формирует и направляет запрос на регистрацию в электронной форме в Удостоверяющий центр, а также заявление на регистрацию пользователя Удостоверяющего центра (по форме Приложения №2 настоящего Регламента) Оператору. Указанное заявление создается автоматически после направления запроса на регистрацию в Удостоверяющий центр, подписывается пользователем и высылается Оператору в виде скан-копии на электронный адрес docscpca@bystrobank.ru.

Ответственное лицо Оператора Удостоверяющего центра подтверждает регистрацию Пользователя не позднее 3 рабочих дней с даты получения Оператором скан-копии заявления на регистрацию пользователя Удостоверяющего центра.

После регистрации в Удостоверяющем центре Пользователь с помощью АРМ пользователя Удостоверяющего центра генерирует пару ключей, формирует и направляет запрос на сертификат ключа проверки электронной подписи в электронной форме в Удостоверяющий центр и формирует заявление на изготовление сертификата ключа ЭП по форме Приложения №3 настоящего Регламента, который подписывается Пользователем, заверяется подписью полномочного представителя и печатью присоединившейся Стороны, и в виде скан-копии высылается на электронный адрес docscpca@bystrobank.ru.

Ответственное лицо Оператора производит сравнение идентификационной информации, указанной в заявлении на изготовление сертификата ключа ЭП с информацией указанной в запросе на сертификат, поданном в электронной форме в Удостоверяющий центр. В случае идентичности идентификационной информации ответственное лицо Оператора обеспечивает изготовление сертификата ключа проверки электронной подписи Пользователя.

Изготовление сертификата ключа проверки электронной подписи Пользователя должно быть осуществлено не позднее 3 рабочих дней с даты получения Оператором скан-копии заявления на изготовление сертификата ключа ЭП.

После изготовления сертификата ключа проверки электронной подписи Пользователь с помощью АРМ пользователя Удостоверяющего центра производит установку сертификата на своем рабочем месте.

До истечения 30 дней с момента изготовления сертификата Пользователь должен предоставить Оператору оригинал заявления на регистрацию пользователя Удостоверяющего центра и заявления на изготовление сертификата ключа ЭП посредством почтовой (курьерской) связи либо лично. В случае непредставления оригиналов документов в указанный срок Оператор вправе приостановить действие соответствующего(их) сертификата(ов).

8.2.Изготовление и получение ключей подписи и сертификата ключа подписи

Изготовление ключей электронной подписи и сертификата ключа проверки электронной подписи Пользователя осуществляется при плановой и внеплановой смене ключа электронной подписи Пользователя.

Формирование сертификата ключа проверки электронной подписи Пользователя осуществляется на основании запроса на изготовление сертификата ключа проверки электронной подписи и заявления на изготовление сертификата ключа ЭП согласно порядку, определенному в разделе 9.1.1 настоящего Регламента.

Ответственный сотрудник Оператора по запросу Пользователя изготавливает копию сертификата ключа проверки электронной подписи на бумажном носителе по форме, определенной Приложением №7 к настоящему Регламенту. Копия сертификата ключа проверки электронной подписи на бумажном носителе заверяется собственноручной подписью Пользователя, а также собственноручной подписью ответственного сотрудника Оператора и печатью Оператора.

По окончании процедуры изготовления ключей и сертификата ключа подписи Пользователю УЦ выдается сертификат ключа проверки электронной подписи Пользователя в электронной форме в виде файла, соответствующий закрытому ключу, а также по запросу Пользователя — копия сертификата ключа проверки электронной подписи на бумажном носителе.

8.3.Аннулирование (отзыв) сертификата ключа проверки электронной подписи Пользователя

Для осуществления аннулирования (отзыва) сертификата ключа проверки электронной подписи Пользователь подает заявление на аннулирование (отзыв) сертификата ключа проверки электронной подписи Оператору.

Заявление на аннулирование (отзыв) сертификата ключа проверки электронной подписи может подаваться в бумажной форме (при личном прибытии Пользователя в офис Оператора, либо посредством почтовой или курьерской связи) и в электронной форме с рабочего места Пользователя с использованием программного обеспечения, предоставляемого Удостоверяющим центром.

8.3.1.Аннулирование (отзыв) сертификата ключа подписи по заявлению, поданному в бумажной форме

Форма заявления на аннулирование (отзыв) сертификата ключа проверки электронной подписи приведена в Приложении №4 к настоящему Регламенту.

Заявление на аннулирование (отзыв) сертификата ключа проверки электронной подписи заверяется собственноручной подписью Владельца сертификата ключа проверки электронной подписи (Пользователя) и подается в офис Оператора.

Подача заявления и его рассмотрение осуществляется только в течение рабочего дня.

Обработка заявления на аннулирование (отзыв) сертификата ключа проверки электронной подписи и официальное уведомление Пользователя об аннулировании (отзыве) сертификата ключа проверки электронной подписи должны быть осуществлены не позднее рабочего дня, следующего за рабочим днем, в течение которого было подано заявление Оператору.

Официальным уведомлением о факте аннулирования (отзыва) сертификата ключа проверки электронной подписи является опубликование списка отозванных сертификатов, содержащего сведения об аннулированном (отозванном) сертификате. Временем аннулирования (отзыва) сертификата ключа проверки электронной подписи признается время издания списка отозванных сертификатов, содержащего сведения об аннулированном (отозванном) сертификате, указанное в поле thisUpdate изданного списка отозванных сертификатов.

Информация о размещении списка отозванных сертификатов заносится в изданные Удостоверяющим центром сертификаты ключа проверки электронной подписи в поле CRL Distribution Point.

8.3.2.Аннулирование (отзыв) сертификата ключа проверки электронной подписи по заявлению, поданному в электронной форме

Подача Пользователем заявления на аннулирование (отзыв) сертификата ключа проверки электронной подписи в электронной форме осуществляется с использованием программного обеспечения, предоставляемого Удостоверяющим центром.

Заявление на аннулирование (отзыв) сертификата ключа проверки электронной подписи Пользователя в электронной форме представляет собой электронный документ формата PKCS#7. В качестве подписываемых данных используется запрос на отзыв сертификата ключа подписи, а электронная подпись осуществляется на действующем ключе электронной подписи Пользователя.

Запрос на отзыв сертификата ключа проверки электронной подписи представляет собой строку формата "SN=CertificateSerialNumber, RC=ReasonCode, SC=SomeComment", где:

- CertificateSerialNumber — серийный номер отзываемого сертификата ключа проверки электронной подписи;
- ReasonCode - код причины отзыва из следующего перечня допустимых значений:
  - "0" Не указана
  - "1" Компрометация ключа
  - "2" Компрометация ЦС
  - "3" Изменение принадлежности
  - "4" Сертификат заменен
  - "5" Прекращение работы
- SomeComment — текстовое значение комментария владельца сертификата ключа проверки электронной подписи.

После регистрации отправленного заявления в Удостоверяющем центре ответственный сотрудник Оператора проверяет корректность электронной подписи заявления и устанавливает его автора, затем устанавливает — является ли автор заявления Владельцем сертификата ключа проверки электронной подписи (отзываемого сертификата), серийный номер которого указан в запросе на отзыв сертификата ключа проверки электронной подписи.

В случае отрицательного результата проведенных проверок, а также иных случаях, установленных настоящим Регламентом, ответственный сотрудник Оператора отклоняет заявление на аннулирование (отзыв) сертификата ключа проверки электронной подписи.

Срок рассмотрения заявления на аннулирование (отзыв) сертификата ключа проверки электронной подписи составляет один рабочий день с момента регистрации заявления в Удостоверяющем центре. В случае отказа в аннулировании (отзыве) сертификата ключа подписи Оператор официально уведомляет Пользователя об этом в срок, установленный для рассмотрения заявления.

При принятии положительного решения, ответственный сотрудник Оператора аннулирует (отзывает) сертификат ключа проверки электронной подписи.

Обработка заявления на аннулирование (отзыв) сертификата ключа проверки электронной подписи и официальное уведомление Пользователя об аннулировании (отзыве) сертификата ключа

проверки электронной подписи должны быть осуществлены не позднее рабочего дня, следующего за рабочим днем, в течение которого было зарегистрировано заявление в Удостоверяющем центре.

Официальным уведомлением о факте аннулирования (отзыва) сертификата ключа проверки электронной подписи является опубликование списка отозванных сертификатов, содержащего сведения об аннулированном (отозванном) сертификате. Временем аннулирования (отзыва) сертификата ключа проверки электронной подписи признается время издания списка отозванных сертификатов, содержащего сведения об аннулированном (отозванном) сертификате, указанное в поле thisUpdate изданного списка отозванных сертификатов.

Информация о размещении списка отозванных сертификатов заносится в изданные Удостоверяющим центром сертификаты ключа проверки электронной подписи в поле CRL Distribution Point.

8.4.Приостановление действия сертификата ключа проверки электронной подписи Пользователя

Для осуществления приостановления действия сертификата ключа проверки электронной подписи Пользователь подает заявление на приостановление действия сертификата ключа проверки электронной подписи.

Приостановление действия сертификата ключа проверки электронной подписи Пользователя осуществляется Оператором на основании заявления, поступающего в устной, бумажной или электронной форме.

Заявление в устной форме осуществляется в офис Оператора по телефону.

Заявитель должен сообщить ответственному сотруднику Оператора следующую информацию:

- Идентификационные данные владельца сертификата ключа проверки электронной подписи;
- серийный номер сертификата ключа проверки электронной подписи, действие которого требуется приостановить;
- срок, на который приостанавливается действие сертификата ключа проверки электронной подписи;
- ключевую фразу Пользователя (определяемой в процессе регистрации Пользователя).

Заявление принимается только в случае положительной аутентификации Пользователя (совпадения ключевой фразы, переданной в заявлении, с информацией из реестра пользователей Удостоверяющего центра).

Заявление в бумажной форме подается в офис Оператора по форме, определенной Приложением №5 настоящего Регламента.

Заявление в бумажной форме содержит следующую информацию:

- Идентификационные данные владельца сертификата ключа проверки электронной подписи;
- серийный номер сертификата ключа проверки электронной подписи, действие которого требуется приостановить;
- срок, на который приостанавливается действие сертификата ключа проверки электронной подписи;
- дата и время подачи заявления.

Заявление на приостановление действия сертификата ключа проверки электронной подписи подписи заверяется собственноручной подписью Владельца сертификата (Пользователя) и подается в офис Оператора (при личном прибытии заявителя, либо посредством почтовой или курьерской связи).

Заявление на приостановление действия сертификата ключа проверки электронной подписи подписи в электронной форме представляет собой электронный документ формата PKCS#7. В качестве подписываемых данных используется запрос на приостановление действия сертификата, а электронная подпись осуществляется на действующем ключе электронной подписи Пользователя.

Запрос на приостановление действия сертификата представляет собой строку формата "SN=CertificateSerialNumber, RC=ReasonCode, HD=HoldDuration, SC=SomeComment", где:

- CertificateSerialNumber — серийный номер сертификата, действие которого требуется приостановить;
- ReasonCode – "6" — приостановление действия;
- HoldDuration — срок, на который приостанавливается действие сертификата, в следующем формате: Y-M-W-D-H-M, где:
  - Y — число лет;
  - M — число месяцев;
  - W — число недель;
  - D — число дней;
  - H — число часов;
  - M — число минут;
- SomeComment — текстовое значение комментария Владельца сертификата ключа проверки электронной подписи.

Заявление на приостановление действия сертификата ключа проверки электронной подписи в электронном виде формируется и подается в Удостоверяющий центр с использованием программного обеспечения, предоставляемого Удостоверяющим центром.

После регистрации отправленного заявления в Удостоверяющем центре ответственный сотрудник Оператора проверяет корректность электронной подписи заявления и устанавливает его автора, затем устанавливает — является ли автор заявления владельцем сертификата ключа проверки электронной подписи (сертификата, действие которого требуется приостановить), серийный номер которого указан в запросе на приостановление действия сертификата ключа проверки электронной подписи.

Действие сертификата приостанавливается на исчисляемый в днях срок. Минимальный срок приостановления действия сертификата составляет 10 (Десять) дней.

Подача заявления на приостановление действия сертификата в Удостоверяющий центр и его рассмотрение осуществляется только в течение рабочего дня.

Обработка заявления на приостановление действия сертификата ключа проверки электронной подписи и оповещение Пользователя о приостановлении действия сертификата должны быть осуществлены не позднее одного рабочего дня, следующего за рабочим днем, в течение которого было подано заявление в Удостоверяющий центр.

Официальным уведомлением о приостановлении действия сертификата ключа проверки электронной подписи является опубликование списка отозванных сертификатов, содержащего сведения о сертификате, действие которого было приостановлено. Временем приостановления действия сертификата ключа подписи признается время издания списка отозванных сертификатов, содержащего сведения о сертификате, действие которого было приостановлено, указанное в поле thisUpdate изданного списка отозванных сертификатов.

Информация о размещении списка отозванных сертификатов заносится в изданные Удостоверяющим центром сертификаты ключа проверки электронной подписи в поле CRL Distribution Point.

В том случае, если в течение срока приостановления действия сертификата ключа проверки электронной подписи Пользователя Оператору не поступает заявление от Пользователя о возобновлении действия сертификата, сертификат аннулируется (отзывается) Удостоверяющим центром.

8.5.Возобновление действия сертификата ключа проверки электронной подписи Пользователя

Для осуществления возобновления действия сертификата ключа проверки электронной подписи Пользователь подает заявление на возобновление действия сертификата.

Возобновление действия сертификата ключа проверки электронной подписи Пользователя осуществляется ответственным сотрудником Оператора на основании заявления на возобновление действия сертификата ключа проверки электронной подписи, поступающего в бумажной или электронной форме.

Заявление в бумажной форме подается в офис Оператора по форме, определенной Приложением №6 настоящего Регламента.

Заявление в бумажной форме содержит следующую информацию:

- идентификационные данные владельца сертификата ключа проверки электронной подписи;
- серийный номер сертификата ключа проверки электронной подписи, действие которого требуется возобновить;
- дата и время подачи заявления.

Заявление на возобновление действия сертификата ключа проверки электронной подписи в бумажной форме заверяется собственноручной подписью Владельца сертификата (Пользователя) и подается в офис Оператора (при личном прибытии заявителя, либо посредством почтовой или курьерской связи).

Заявление на возобновление действия сертификата ключа проверки электронной подписи в электронной форме представляет собой электронный документ формата PKCS#7. В качестве подписываемых данных используется запрос на возобновление действия сертификата, а электронная подпись осуществляется на действующем ключе электронной подписи Пользователя.

Запрос на возобновление действия сертификата представляет собой строку формата "SN=CertificateSerialNumber, RC=ReasonCode, SC=SomeComment", где:

- CertificateSerialNumber — серийный номер сертификата ключа проверки электронной подписи, действие которого требуется возобновить;
- ReasonCode — "-1" - возобновление действия;
- SomeComment — текстовое значение комментария владельца сертификата ключа проверки электронной подписи.

Заявление на возобновление действия сертификата ключа проверки электронной подписи формируется и подается в электронном виде в Удостоверяющий центр с использованием программного обеспечения, предоставляемого Удостоверяющим центром.

После регистрации отправленного заявления в Удостоверяющем центре ответственный сотрудник Оператора проверяет корректность электронной подписи заявления и устанавливает его автора, затем устанавливает — является ли автор заявления Владельцем сертификата ключа проверки электронной подписи (сертификата, действие которого требуется возобновить), серийный номер которого указан в запросе на возобновление действия сертификата ключа проверки электронной подписи.

Подача заявления на возобновление действия сертификата в Удостоверяющий центр и его рассмотрение осуществляется только в течение рабочего дня.

Обработка заявления на возобновление действия сертификата и оповещение Пользователя о возобновлении действия сертификата должны быть осуществлены не позднее одного рабочего дня, следующего за рабочим днем, в течение которого было подано заявление в Удостоверяющий центр.

Официальным уведомлением о возобновлении действия сертификата ключа проверки электронной подписи является опубликование списка отозванных сертификатов, не содержащего сведений о сертификате, действие которого было возобновлено. Временем возобновления действия сертификата ключа проверки электронной подписи признается время издания списка отозванных сертификатов, не содержащего сведений о сертификате, действие которого было возобновлено, указанное в поле thisUpdate изданного списка отозванных сертификатов.

Информация о размещении списка отозванных сертификатов заносится в изданные Удостоверяющим центром сертификаты ключа проверки электронной подписи в поле CRL Distribution Point.

8.6.Подтверждение подлинности электронной подписи в электронном документе

Для подтверждения подлинности ЭП в электронных документах, циркулирующих в Информационной системе, Пользователь подает Заявление на подтверждение подлинности ЭП в электронном документе в офис Оператора.

Подтверждение подлинности ЭП электронного документа осуществляется на основании заявления, содержащего следующую информацию:

- Дата и время подачи заявления;
- Идентификационные данные Пользователя, ЭП которого требуется проверить в электронном документе;
- Серийный номер сертификата ключа проверки электронной подписи, на котором требуется проверить ЭП электронного документа;
- дата и время формирования ЭП в электронном документе.

Обязательным приложением к Заявлению на подтверждение подлинности ЭП в электронном документе является файл на съемном носителе, содержащий электронный документ.

Предоставляемый файл получается путем экспорта электронного документа, к которому применена электронная подпись, из Информационной системы.

Электронная подпись в предоставленном электронном документе будет считаться равнозначной собственноручной подписи при выполнении следующих условий:

- сертификат ключа проверки электронной подписи с серийным номером, указанным в заявлении на подтверждение подлинности ЭП, не утратил силу (действует) на момент формирования ЭП в электронном документе;
- электронная подпись, проверенная на сертификате ключа проверки электронной подписи с серийным номером, указанным в заявлении на подтверждение подлинности ЭП, верна;
- электронная подпись используется в соответствии со сведениями, указанными в сертификате ключа проверки электронной подписи — в поле Extended Key Usage;
- формирование электронной подписи осуществлено без нарушений условий настоящего Регламента.

Срок проведения работ по Заявлению на подтверждение подлинности ЭП в электронном документе и предоставлению заключения о произведенной проверке составляет 15 (Пятнадцать) рабочих дней с момента его предоставления Оператору.

Проведение работ по подтверждению подлинности ЭП в электронном документе осуществляет комиссия, сформированная из числа сотрудников Оператора. При проведении указанных работ Оператор (комиссия) имеет право привлекать к проведению экспертных работ специалистов Удостоверяющего центра.

Результатом проведения работ по подтверждению подлинности ЭП в электронном документе является заключение в письменной форме, подписанное всеми членами комиссии и заверенное печатью Оператора.

Заключение содержит:

- результат проверки ЭП электронного документа;

- отчет по выполненной проверке.

Отчет по выполненной проверке содержит:

- время и место проведения проверки;
- состав комиссии, осуществлявшей проверку;
- основание для проведения проверки;
- содержание и результаты проверки с указанием примененных методов;
- обоснование результатов проверки;
- данные, представленные комиссии для проведения проверки;

Отчет по выполненной проверке составляется в простой письменной форме и заверяется собственноручными подписями всех членов комиссии.

8.7.Подтверждение подлинности ЭП уполномоченного лица Удостоверяющего центра в изданных сертификатах

Для подтверждения подлинности ЭП уполномоченного лица Удостоверяющего центра в сертификате ключа проверки электронной подписи Пользователь подает заявление на подтверждение подлинности ЭП уполномоченного лица Удостоверяющего центра в сертификате ключа проверки электронной подписи Оператору.

Заявление должно содержать следующую информацию:

- Дата и время подачи заявления;
- Идентификационные данные субъекта, в сертификате ключа подписи которого необходимо подтвердить ЭП уполномоченного лица Удостоверяющего центра;
- Серийный номер сертификата ключа проверки электронной подписи, в котором необходимо подтвердить ЭП уполномоченного лица Удостоверяющего центра.

Обязательным приложением к заявлению на подтверждение подлинности ЭП уполномоченного лица Удостоверяющего центра в сертификате ключа проверки электронной подписи является съемный носитель, содержащий файл сертификата ключа проверки электронной подписи, подвергающегося процедуре проверки.

Срок проведения работ по подтверждению подлинности ЭП и предоставлению заключения о произведенной проверке составляет 15 (Пятнадцать) рабочих дней с момента его предоставления Оператору.

На основании полученного заявления Оператор установленным порядком обращается в Удостоверяющий центр, который осуществляет подтверждение подлинности ЭП уполномоченного лица Удостоверяющего центра в сертификате ключа проверки электронной подписи.

Результатом проведения работ по подтверждению подлинности ЭП уполномоченного лица Удостоверяющего центра в сертификате ключа проверки электронной подписи является заключение Удостоверяющего центра в письменной форме, подписанное уполномоченным лицом Удостоверяющего центра и заверенное печатью Удостоверяющего центра.

Заключение содержит:

- результат проверки ЭП уполномоченного лица Удостоверяющего центра;
- отчет по выполненной проверке.

Отчет по выполненной проверке содержит:

- время и место проведения проверки;
- основание для проведения проверки;
- содержание и результаты проверки с указанием примененных методов;
- обоснование результатов проверки;
- данные, представленные для проведения проверки;

Отчет по выполненной проверке составляется в простой письменной форме.

9.Структура сертификатов ключей проверки электронной подписи и сроки действия ключевых документов

9.1.Структура сертификата ключа проверки электронной подписи уполномоченного лица Удостоверяющего центра

Название	Описание	Содержание
Базовые поля сертификата		
Version	Версия	V3
Serial Number	Серийный номер	Уникальный серийный номер сертификата
Signature Algorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2001
Issuer	Издатель сертификата	CommonName = УЦ КРИПТО-ПРО – псевдоним уполномоченного лица Удостоверяющего центра Organization (Организация) = ООО КРИПТО-ПРО Locality (Город) = Москва Country (Страна) = RU Email (Электронная почта) = cpca@cryptopro.ru
Validity Period	Срок действия сертификата	Действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT Действителен по(notAfter): дд.мм.гггг чч:мм:сс GMT
Subject	Владелец сертификата	CommonName = УЦ КРИПТО-ПРО – псевдоним уполномоченного лица Удостоверяющего центра Organization (Организация) = ООО КРИПТО-ПРО Locality (Город) = Москва Country (Страна) = RU Email (Электронная почта) = cpca@cryptopro.ru
Public Key	Открытый ключ	Открытый ключ (алгоритм ГОСТ Р 34.10-2001)
Issuer Signature Algorithm	Алгоритм подписи издателя сертификата	ГОСТ Р 34.11/34.10-2001
Issuer Sign	ЭП издателя сертификата	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001
Дополнения сертификата		
Key Usage (critical)	Использование ключа	Неотрекаемость — невозможность осуществления отказа от совершенных действий; Подписывание сертификатов, Автономное подписание списка отзыва (CRL), Подписание списка отзыва (CRL)
Subject Key Idendifier	Идентификатор ключа владельца сертификата	Идентификатор ключа электронной подписи уполномоченного лица Удостоверяющего центра, соответствующего данному сертификату
BasicConstraints	Основные ограничения	SybjectType (Тип владельца сертификата) = ЦС Path Length Constraint (Ограничение на длину пути — ограничивает количество уровней иерархии при создании подчиненных Удостоверяющих центров) = Отсутствует
SzOID_CertSrv_CA_Version	Объектный идентификатор версии сертификата	Версия сертификата уполномоченного лица Удостоверяющего центра

9.2.Структура сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра

Название	Описание	Содержание
Базовые поля сертификата		
Version	Версия	V3
Serial Number	Серийный номер	Уникальный серийный номер сертификата
Signature Algorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2001
Issuer	Издатель сертификата	CommonName = УЦ КРИПТО-ПРО – псевдоним уполномоченного лица Удостоверяющего центра Organization (Организация) = ООО КРИПТО-ПРО Locality (Город) = Москва Country (Страна) = RU Email (Электронная почта) = cpca@cryptopro.ru
Validity Period	Срок действия сертификата	Действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT Действителен по(notAfter): дд.мм.гггг чч:мм:сс GMT
Subject	Владелец сертификата	CommonName = Фамилия, Имя, Отчество или псевдоним OrganizationUnit = Подразделение Organization = Организация Title = Должность Locality = Город State = Субъект Федерации

		Country = Страна = RU Email = Электронная почта Компоненты имени CN, Organization, Locality, Country обязательны для заполнения, необходимость заполнения остальных значений определяется Владельцем сертификата и Оператором Удостоверяющего центра. В поле Subject сертификата могут быть добавлены дополнительные компоненты имени согласно RFC 3280
Public Key	Открытый ключ	Открытый ключ (алгоритм подписи)
Issuer Signature Algorithm	Алгоритм подписи издателя сертификата	ГОСТ Р 34.11/34.10-2001
Issuer Sign	ЭП издателя сертификата	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001
Расширения сертификата		
Key Usage (critical)	Использование ключа	Неотрекаемость - невозможность осуществления отказа от совершенных действий; Цифровая подпись, Шифрование ключей, Шифрование данных
Extended Key Usage	Улучшеный ключ	Набор областей использования ключей и сертификатов из перечня областей использования, зарегистрированных в Удостоверяющем центре
Application Policy	Политика применения	Набор областей использования ключей и сертификатов из перечня областей использования, зарегистрированных в Удостоверяющем центре
Subject Key Idendifier	Идентификатор ключа владельца сертификата	Идентификатор ключа электронной подписи Владельца сертификата
Authority Key Identifier	Идентификатор ключа издателя сертификата	Идентификатор ключа электронной подписи уполномоченного лица Удостоверяющего центра, на котором подписан данный сертификат
CRL Distribution Point	Точка распространения списка отозванных сертификатов	Набор адресов точек распространения списков отозванных сертификатов следующего вида: URL=http://ResourceServer/Path/hex.crl, где ResourceServer — имя сервера, Path — путь к файлу списка отозванных сертификатов, hex — шестнадцатеричное значение идентификатора ключа электронной подписи уполномоченного лица Удостоверяющего центра, с использованием которого издан сертификат и список отозванных сертификатов
Authority Information Access	Адрес Службы актуальных статусов сертификатов	URL адреса web-приложения Службы актуальных статусов сертификатов. Заносится в сертификаты, статус которых может быть установлен по протоколу OCSP
		В сертификат ключа проверки электронной подписи могут быть добавлены дополнительные поля и расширения согласно RFC 3280

9.3.Структура списка отозванных сертификатов (CRL) Удостоверяющего центра

Название	Описание	Содержание
Базовые поля списка отозванных сертификатов		
Version	Версия	V2
Issuer	Издатель СОС	CommonName = УЦ КРИПТО-ПРО – псевдоним уполномоченного лица Удостоверяющего центра Organization (Организация) = ООО КРИПТО-ПРО Locality (Город) = Москва Country (Страна) = RU Email (Электронная почта) = cpca@cryptopro.ru
thisUpdate	Время издания СОС	дд.мм.гггг чч:мм:сс GMT
nextUpdate	Время, по которое действителен СОС	дд.мм.гггг чч:мм:сс GMT
revokedCertificates	Список отозванных сертификатов	Последовательность элементов следующего вида 1. Серийный номер сертификата (CertificateSerialNumber) 2. Время обработки заявления на аннулирование (отзыв) сертификата (Time) 3. Код причины отзыва сертификата (Reson Code) "0" Не указана "1" Компрометация ключа "2" Компрометация ЦС "3" Изменение принадлежности "4" Сертификат заменен "5" Прекращение работы "6" Приостановка действия
signatureAlgorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2001
Issuer Sign	Подпись издателя СОС	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001
Расширения списка отозванных сертификатов		
Authority Key Identifier	Идентификатор ключа издателя	Идентификатор ключа электронной подписи уполномоченного лица Удостоверяющего центра, на котором подписан СОС
SzOID_CertSrv_CA_Version	Объектный идентификатор сертификата издателя	Версия сертификата уполномоченного лица Удостоверяющего центра

9.4.Расширения Key Usage, Extended Key Usage, Application Policy сертификата ключа проверки электронной подписи содержат сведения об отношениях, при которых электронный документ будет иметь юридическое значение. Наличие в сертификате ключа проверки электронной подписи области использования "Пользователь Центра Регистрации (1.2.643.2.2.34.6)" устанавливает, что Владелец указанного сертификата имеет право подписывать электронной подписью электронные документы, определенные настоящим Регламентом для Пользователя Удостоверяющего центра.

9.5.Сроки действия ключевых документов

9.5.1.Срок действия ключа электронной подписи уполномоченного лица Удостоверяющего центра составляет максимально допустимый срок действия, установленный для применяемого средства обеспечения деятельности Удостоверяющего центра, и для средства электронной подписи, с использованием которого данный ключ электронной подписи был сформирован.

Начало периода действия ключа электронной подписи уполномоченного лица Удостоверяющего центра исчисляется с даты и времени генерации ключа электронной подписи уполномоченного лица Удостоверяющего центра.

Срок действия сертификата ключа проверки электронной подписи уполномоченного лица Удостоверяющего центра не превышает 30 (тридцать) лет. Время начала периода действия сертификата ключа проверки электронной подписи уполномоченного лица Удостоверяющего центра и его окончания заносится в поля "notBefore" и "not After" поля "Validity Period" соответственно.

9.5.2.Срок действия ключа электронной подписи Пользователя составляет 1 (один) год.

Начало периода действия ключа электронной подписи Пользователя исчисляется с даты и времени начала действия соответствующего сертификата ключа проверки электронной подписи.

Срок действия сертификата ключа проверки электронной подписи Пользователя составляет 5 (пять) лет. Время начала периода действия сертификата ключа подписи Пользователя и его окончания заносится в поля "notBefore" и "not After" поля "Validity Period" соответственно.

10.Дополнительные положения

10.1.Плановая смена ключей уполномоченного лица Удостоверяющего центра

Плановая смена ключей (ключа электронной подписи и соответствующего ему ключа проверки электронной подписи) уполномоченного лица Удостоверяющего центра выполняется в период действия ключа электронной подписи уполномоченного лица Удостоверяющего центра.

Процедура плановой смены ключей уполномоченного лица Удостоверяющего центра осуществляется в следующем порядке:

- Уполномоченное лицо Удостоверяющего центра генерирует новый ключ электронной подписи и соответствующий ему ключ проверки электронной подписи;
- Уполномоченное лицо Удостоверяющего центра изготавливает новый сертификат ключа проверки электронной подписи уполномоченного лица Удостоверяющего центра

Старый ключ электронной подписи уполномоченного лица Удостоверяющего центра используется в течение своего срока действия для формирования списков отозванных сертификатов, изданных Удостоверяющим центром в период действия старого ключа электронной подписи уполномоченного лица Удостоверяющего центра.

По истечении одного года с момента проведения плановой смены ключей уполномоченного лица Удостоверяющий центр изготавливает список отозванных сертификатов, соответствующий старому ключу электронной подписи, со сроком действия соответствующим сроку действия старого сертификата уполномоченного лица Удостоверяющего центра (значение поля nextUpdate списка отозванных сертификатов совпадает со значением поля notAfter поля Validity сертификата ключа проверки электронной подписи уполномоченного лица Удостоверяющего центра). Изданный список отозванных сертификатов публикуется Удостоверяющим центром, изготовление нового списка отозванных сертификатов, соответствующего старому ключу электронной подписи уполномоченного лица Удостоверяющего центра, более не осуществляется.

10.2.Компрометация ключевых документов уполномоченного лица Удостоверяющего центра, внеплановая смена ключей уполномоченного лица Удостоверяющего центра

В случае компрометации ключа электронной подписи уполномоченного лица Удостоверяющего центра сертификат уполномоченного лица Удостоверяющего центра аннулируется (отзывается), Пользователи уведомляются об указанном факте путем рассылки соответствующего уведомления по электронной почте и публикации информации о компрометации на сайте Удостоверяющего центра. Все сертификаты, изданные с использованием скомпрометированного ключа уполномоченного лица Удостоверяющего центра, считаются аннулированными.

После аннулирования сертификата уполномоченного лица Удостоверяющего центра выполняется процедура внеплановой смены ключей уполномоченного лица Удостоверяющего центра. Процедура внеплановой смены ключей уполномоченного лица Удостоверяющего центра выполняется в порядке, определенном процедурой плановой смены ключей уполномоченного лица Удостоверяющего центра.

Все действовавшие на момент компрометации ключа электронной подписи уполномоченного лица Удостоверяющего центра сертификаты ключей проверки электронной подписи, а также сертификаты, действие которых было приостановлено, подлежат внеплановой смене.

10.3.Компрометация ключевых документов Пользователя

Пользователь самостоятельно принимает решение о факте или угрозе компрометации своего ключа электронной подписи

В случае компрометации или угрозы компрометации ключа электронной подписи Пользователь связывается с Оператором по телефону и сообщает ему следующие сведения:

- Свои идентификационные данные;
- Серийный номер сертификата ключа проверки электронной подписи, соответствующего скомпрометированному ключу.

В случае успешной аутентификации Оператор приостанавливает действие сертификата на 30 календарных дней.

Если в течение срока приостановления действия сертификата ключа проверки электронной подписи Пользователь не направит в Удостоверяющий центр заявление на возобновление действия сертификата, то Удостоверяющий центр автоматически аннулирует (отзовет) данный сертификат.

Пользователь Удостоверяющего центра осуществляет внеплановую смену ключей в соответствии с пунктом 8.2 настоящего Регламента.

10.4.Конфиденциальность информации

10.4.1.Типы конфиденциальной информации

10.4.1.1.Ключ электронной подписи, соответствующий сертификату ключа проверки электронной подписи, является конфиденциальной информацией лица, зарегистрированного в Удостоверяющем центре. Оператор не осуществляет хранение ключей электронной подписи Пользователей.

10.4.1.2.Персональная и корпоративная информация о лицах, зарегистрированных в Удостоверяющем центре и содержащаяся в Реестре Удостоверяющего центра, не подлежащая непосредственной рассылке в качестве части сертификата ключа проверки электронной подписи, считается конфиденциальной.

10.4.2.Типы информации, не являющейся конфиденциальной

10.4.2.1.Информация, не являющаяся конфиденциальной информацией, считается открытой информацией.

10.4.2.2.Открытая информация может публиковаться по решению Оператора и Удостоверяющего центра. Место, способ и время публикации открытой информации определяется Оператором и Удостоверяющим центром.

10.4.2.3.Информация, включаемая в сертификаты ключей проверки электронной подписи и списки отозванных сертификатов, издаваемые Удостоверяющим центром, не считается конфиденциальной.

10.4.2.4.Персональные данные, включаемые в сертификаты ключей проверки электронной подписи, издаваемые Удостоверяющим центром, относятся к общедоступным персональным данным.

10.4.2.5.Информация, содержащаяся в настоящем Регламенте, не считается конфиденциальной.

10.4.3.Исключительные полномочия Оператора и Удостоверяющего центра

10.4.3.1.Оператор и Удостоверяющий центр имеет право раскрывать конфиденциальную информацию третьим лицам только в случаях, установленных законодательством Российской Федерации.

10.5.Форс-мажор

10.5.1.Стороны освобождаются от ответственности за полное или частичное неисполнение своих обязательств по настоящему Регламенту, если это неисполнение явилось следствием форс-мажорных обстоятельств, возникших после присоединения к настоящему Регламенту.

10.5.2.Форс-мажорными обстоятельствами признаются чрезвычайные (т. е. находящиеся вне разумного контроля Сторон) и непредотвратимые при данных условиях обстоятельства включая военные действия, массовые беспорядки, стихийные бедствия, забастовки, технические сбои функционирования программного обеспечения, пожары, взрывы и иные техногенные катастрофы, действия (бездействие) государственных и муниципальных органов, повлекшие невозможность исполнения Стороной/Сторонами своих обязательств по настоящему Регламенту.

10.5.3.В случае возникновения форс-мажорных обстоятельств, срок исполнения Сторонами своих обязательств по настоящему Регламенту отодвигается соразмерно времени, в течение которого действуют такие обстоятельства.

10.5.4.Сторона, для которой создалась невозможность исполнения своих обязательств по настоящему Регламенту, должна немедленно известить в письменной форме другую Сторону о наступлении, предполагаемом сроке действия и прекращении форс-мажорных обстоятельств, а также представить доказательства существования названных обстоятельств.

10.5.5.Не извещение или несвоевременное извещение о наступлении обстоятельств непреодолимой силы влечет за собой утрату права ссылаться на эти обстоятельства.

10.5.6.В случае, если невозможность полного или частичного исполнения Сторонами какого-либо обязательства по настоящему Регламенту обусловлена действием форс-мажорных обстоятельств и существует свыше одного месяца, то каждая из Сторон вправе отказаться в одностороннем порядке от дальнейшего исполнения этого обязательства и в этом случае ни одна из Сторон не вправе требовать возмещения возникших у нее убытков другой Стороной.

11.Список приложений

11.1.Приложение №1. Список объектных идентификаторов (OID), зарегистрированных в Удостоверяющем центре ООО "КРИПТО-ПРО", определяющих отношения, при осуществлении которых электронный документ с электронной подписью будет иметь юридическое значение

11.2.Приложение №2. Заявление на регистрацию пользователя Удостоверяющего центра

11.3.Приложение №3. Бланк запроса на изготовление сертификата ключа подписи Пользователя Удостоверяющего центра ООО "КРИПТО-ПРО"

11.4.Приложение №4. Заявление на аннулирование (отзыв) сертификата ключа подписи Пользователя Удостоверяющего центра ООО "КРИПТО-ПРО"

11.5.Приложение №5. Заявление на приостановление действия сертификата ключа подписи Пользователя Удостоверяющего центра ООО "КРИПТО-ПРО"

11.6.Приложение №6. Заявление на возобновление действия сертификата ключа подписи Пользователя Удостоверяющего центра ООО "КРИПТО-ПРО"

11.7.Приложение №7. Копия сертификата ключа подписи Пользователя Удостоверяющего центра ООО "КРИПТО-ПРО" (Пример) 8

Приложение №1 к Регламенту предоставления услуг
Оператора Удостоверяющего центра
ООО "КРИПТО-ПРО"

Список объектных идентификаторов (OID), зарегистрированных в Удостоверяющем центре ООО "КРИПТО-ПРО", определяющих отношения, при осуществлении которых электронный документ с электронной подписью будет иметь юридическое значение

	OID	Область применения
1.	1.2.643.2.2.34.5	Оператор Центра Регистрации — формирование электронной подписи электронных документов, определенных Регламентом для Оператора
2.	1.2.643.2.2.34.6	Пользователь Центра Регистрации — 1. Формирование электронной подписи электронных документов, определенных Регламентом для Пользователя 2. Формирование электронной подписи электронных документов, циркулирующих в *Информационной системе*

Приложение №2 к Регламенту предоставления услуг
Оператора Удостоверяющего центра
ООО "КРИПТО-ПРО"

ФОРМА

Заявление на регистрацию пользователя Удостоверяющего центра

Я, *Фамилия Имя Отчество*, прошу зарегистрировать меня в Реестре Удостоверяющего Центра и наделить полномочиями Пользователя, установленными Регламентом Удостоверяющего Центра в соответствии с указанными в настоящем заявлении идентификационными данными:

Наименование	Значение
Общее имя (2.5.4.3)	*Фамилия Имя Отчество*
Страна (2.5.4.6)	
Город (2.5.4.7)	
Организация (2.5.4.10)	
Должность (2.5.4.12)	
Электронная почта (1.2.840.113549.1.9.1)	

Согласен (согласна) с обработкой своих персональных данных Удостоверяющим Центром и признаю, что персональные данные, заносимые в сертификаты ключей подписи, владельцем которых я являюсь, относятся к общедоступным персональным данным.

Фамилия Имя Отчество

_____
(подпись)

"___" _____ 20 ___ г.

Приложение №3 к Регламенту предоставления услуг
Оператора Удостоверяющего центра
ООО "КРИПТО-ПРО"

Заявление на изготовление сертификата ключа ЭП (ОБРАЗЕЦ)

Прошу изготовить сертификат ключа проверки электронной подписи в соответствии с указанными данными:

Сведения о запросе на сертификат:
Версия: 1
Субъект запроса на сертификат: 2.5.4.7=Москва, 2.5.4.6=RU, 2.5.4.3=Фамилия Имя Отчество, 2.5.4.10=Организация, 1.2.840.113549.1.9.1=mail@example.org
Ключ проверки электронной подписи:
Алгоритм ключа: ГОСТ Р 34.10-2001 (1.2.643.2.2.19)
Параметры: 30 12 06 07 2A 85 03 02 02 24 00 06 07 2A 85 03 02 02 1E 01
Значение: 0440 0027 9E33 75AE 0E8A AA54 D381 EE24 5F09 971D E1B3 5975 9ED0 9E59 43DF D2E9 3F9A 6811 6147 2201 A597 0BA6 E5D1 C83E 6E7F 1A8C 2579 A80C C627 D957 B432 D43D 49EF

Расширения сертификата X.509

Расширение: Использование ключа (критичное)

Идентификатор: 2.5.29.15
Значение: Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных (f0)

Расширение: Сведения о шаблоне сертификата

Идентификатор: 1.3.6.1.4.1.311.21.7
Значение: Шаблон=1.2.643.2.2.46.0.8, Основная версия=1,

Расширение: Идентификатор ключа субъекта

Идентификатор: 2.5.29.14
Значение: 66 ed 16 58 ae 7b 54 96 fb 0c 1a fb c5 42 e4 1f 33 e5 8a 14

Подпись владельца ключа электронной подписи: _____/_____

"___" _____ 20__ г.

Подпись руководителя организации: _____/_____

"___" _____ 20__ г.

М. П.

Приложение №4 к Регламенту предоставления услуг
Оператора Удостоверяющего центра
ООО "КРИПТО-ПРО"

Заявление на аннулирование (отзыв) сертификата ключа подписи Пользователя Удостоверяющего центра ООО "КРИПТО-ПРО"

_____
(полное наименование организации, включая организационно-правовую форму)

в лице _____,
(должность)

_____,
(фамилия, имя, отчество)

действующего на основании _____

в связи с _____
(причина отзыва сертификата*)

Просит аннулировать (отозвать) сертификат ключа подписи своего уполномоченного представителя – Пользователя Удостоверяющего центра ООО "КРИПТО-ПРО", содержащего следующие идентификационные данные:

SerialNumber (SN)	Серийный номер сертификата ключа подписи	
CommonName (CN)	Общее имя – Фамилия, Имя, Отчество	
E-Mail (E)	Адрес электронной почты	
Organization (O)	Наименование организации	
Locality (L)	Город	
State (S)	Область	
Contry (C)	Страна	
Extended Key Usage	Проверка подлинности клиента Защищенная электронная почта Пользователь Центра Регистрации	(1.3.6.1.5.5.7.3.2) (1.3.6.1.5.5.7.3.4) (1.2.643.2.2.34.6)

Подпись владельца сертификата ключа подписи – Пользователя Удостверяющего центра ООО "КРИПТО-ПРО"

_____ /_____/

"____" _____ 20____ г.

Должность и Ф.И.О. руководителя организации
Подпись руководителя организации, дата подписания заявления
Печать организации

Приложение №5 к Регламенту предоставления услуг
Оператора Удостоверяющего центра
ООО "КРИПТО-ПРО"

Заявление на приостановление действия сертификата ключа подписи Пользователя Удостоверяющего центра ООО "КРИПТО-ПРО"

_____
(полное наименование организации, включая организационно-правовую форму)

в лице _____,
(должность)

_____,
(фамилия, имя, отчество)

действующего на основании _____

Просит приостановить действие сертификата ключа подписи своего уполномоченного представителя – Пользователя Удостоверяющего центра ООО "КРИПТО-ПРО", содержащего следующие идентификационные данные:

SerialNumber (SN)	Серийный номер сертификата ключа подписи	
CommonName (CN)	Общее имя – Фамилия, Имя, Отчество	
E-Mail (E)	Адрес электронной почты	
Organization (O)	Наименование организации	
Locality (L)	Город	
State (S)	Область	
Contry (C)	Страна	
Extended Key Usage	Проверка подлинности клиента Защищенная электронная почта Пользователь Центра Регистрации	(1.3.6.1.5.5.7.3.2) (1.3.6.1.5.5.7.3.4) (1.2.643.2.2.34.6)

Срок приостановления действия сертификата _____ дней.
(количество дней прописью)

Подпись владельца сертификата ключа подписи – Пользователя Удостверяющего центра ООО "КРИПТО-ПРО"

_____ /_____/

"____" _____ 20____ г.

Должность и Ф.И.О. руководителя организации
Подпись руководителя организации, дата подписания заявления
Печать организации

Приложение №6 к Регламенту предоставления услуг
Оператора Удостоверяющего центра
ООО "КРИПТО-ПРО"

Заявление на возобновление действия сертификата ключа подписи Пользователя
Удостоверяющего центра ООО "КРИПТО-ПРО"

_____
(полное наименование организации, включая организационно-правовую форму)

в лице _____,
(должность)

_____,
(фамилия, имя, отчество)

действующего на основании _____

Просит возобновить действие сертификата ключа подписи своего уполномоченного представителя – Пользователя Удостоверяющего центра ООО "КРИПТО-ПРО", содержащего следующие идентификационные данные:

SerialNumber (SN)	Серийный номер сертификата ключа подписи	
CommonName (CN)	Общее имя – Фамилия, Имя, Отчество	
E-Mail (E)	Адрес электронной почты	
Organization (O)	Наименование организации	
Locality (L)	Город	
State (S)	Область	
Contry (C)	Страна	
Extended Key Usage	Проверка подлинности клиента Защищенная электронная почта Пользователь Центра Регистрации	(1.3.6.1.5.5.7.3.2) (1.3.6.1.5.5.7.3.4) (1.2.643.2.2.34.6)

Подпись владельца сертификата ключа подписи – Пользователя Удостверяющего центра ООО "КРИПТО-ПРО"

_____ /_____/

"____" _____ 20____ г.

Должность и Ф.И.О. руководителя организации
Подпись руководителя организации, дата подписания заявления
Печать организации

Удостоверяющий Центр ООО "КРИПТО-ПРО"
Сертификат ключа проверки электронной подписи (ОБРАЗЕЦ)
Сведения о сертификате:

Кому выдан:
Фамилия Имя Отчество
Кем выдан:
УЦ КРИПТО-ПРО
Версия: 3
Серийный номер: 46AA8133000E0001DAAF
Издатель сертификата: CN=УЦ КРИПТО-ПРО, O=ООО КРИПТО-ПРО, L=Москва, C=RU, E=cpca@cryptopro.ru
Владелец сертификата: CN=Фамилия Имя Отчество, O=Организация, L=Москва, C=RU, E=mail@example.org
Срок действия:
Действителен с: 07.04.2017 8:58:00
Действителен по: 07.04.2022 9:08:00
Ключ проверки электронной подписи:
Алгоритм: ГОСТ Р 34.10-2001 (1.2.643.2.2.19)
Параметры: 30 12 06 07 2A 85 03 02 02 24 00 06 07 2A 85 03 02 02 1E 01
Значение: 0440 7447 194D 149A 9CC4 769B 7437 B12A 7CBB 250B 4FE1 45A8 A66A 54D6 A85E 42E1 60D3 28B2 36EB A86F E7B8 83BA A68F 7ED1 A0C3 4121 D568 307B 6EAB D6D3 E884 ED55 280D
Расширения сертификата X.509
Расширение: Использование ключа (критичное)
Идентификатор: 2.5.29.15
Значение: Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных (f0)
Расширение: Улучшенный ключ
Идентификатор: 2.5.29.37
Значение: Защищенная электронная почта (1.3.6.1.5.5.7.3.4), Пользователь Центра Регистрации, HTTP, TLS клиент (1.2.643.2.2.34.6), Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)
Расширение: Идентификатор ключа субъекта
Идентификатор: 2.5.29.14
Значение: 62 02 e1 9e bf bb e0 9c 66 9b 62 6e 62 e2 52 af 36 3e 05 0d
Расширение: Идентификатор ключа центра сертификатов
Идентификатор: 2.5.29.35
Значение: Идентификатор ключа=2f 8d 57 cc 87 83 49 b0 81 9a 7a fd 46 ac 1f 27 04 a9 25 58
Расширение: Точки распространения списков отзыва (CRL)
Идентификатор: 2.5.29.31
Значение: [1]Точка распределения списка отзыва (CRL): Имя точки распространения:Полное имя:URL=http://cdp.cryptopro.ru/ra/cdp/2f8d57cc878349b0819a7afd46ac1f2704a92558.crl, [2]Точка распределения списка отзыва (CRL): Имя точки распространения:Полное имя:URL=http://cpca.cryptopro.ru/ra/cdp/2f8d57cc878349b0819a7afd46ac1f2704a92558.crl, [3]Точка распределения списка отзыва (CRL): Имя точки распространения:Полное имя:URL=http://cpca2.cryptopro.ru/ra/cdp/2f8d57cc878349b0819a7afd46ac1f2704a92558.crl
Расширение: Доступ к информации о центрах сертификации
Идентификатор: 1.3.6.1.5.5.7.1.1
Значение: [1]Доступ к сведениям центра сертификации: метод доступа=Протокол определения состояния сертификата через сеть (1.3.6.1.5.5.7.48.1), дополнительное имя=URL=http://ocsp.cryptopro.ru/ocsp/ocsp.srf, [2]Доступ к сведениям центра сертификации: метод доступа=Протокол определения состояния сертификата через сеть (1.3.6.1.5.5.7.48.1), дополнительное имя=URL=http://ocsp2.cryptopro.ru/ocsp/ocsp.srf, [3]Доступ к сведениям центра сертификации: метод доступа=Поставщик центра сертификации (1.3.6.1.5.5.7.48.2), дополнительное имя=URL=http://cpca.cryptopro.ru/cacer.p7b
Расширение: Период использования ключа электронной подписи
Идентификатор: 2.5.29.16
Значение: Действителен с 7 апреля 2017 г. 8:58:00 по 7 апреля 2018 г. 8:58:00

Подпись Удостоверяющего центра:
Алгоритм подписи: ГОСТ Р 34.11/34.10-2001 (1.2.643.2.2.3)
Параметры:
Значение: 73FA 5F6C 3BBA 1176 147E 8D2C 7343 4A8D F4B0 A988 E662 641A 8D00 2843 0247 76A5 6B6D E24C 07FD E2F8 E4AF ACAF C53B 8177 C96A E8C8 BAE6 0C19 54CB 2D6C D6FF C09A

Подпись владельца сертификата: _____/_____

"___" _____ 20__ г.