

Публичное акционерное общество «Промсвязьбанк»



ПОРЯДОК
реализации функций удостоверяющего центра
Публичного акционерного общества
«Промсвязьбанк»

МОСКВА, 2020 г.

СОДЕРЖАНИЕ

1. СВЕДЕНИЯ ОБ УДОСТОВЕРЯЮЩЕМ ЦЕНТРЕ.....	3
2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ	3
3. СТАТУС ПОРЯДКА	6
4. ОБЩИЕ ПОЛОЖЕНИЯ	7
5. ПРЕДОСТАВЛЕНИЕ ИНФОРМАЦИИ	7
6. ПРАВА И ОБЯЗАННОСТИ СТОРОН	7
7. ОТВЕТСТВЕННОСТЬ СТОРОН.....	11
8. РАЗРЕШЕНИЕ СПОРОВ.....	12
9. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ И ПОЛЬЗОВАНИЯ УСЛУГАМИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА.....	12
10. СТРУКТУРА СЕРТИФИКАТОВ КЛЮЧЕЙ ПРОВЕРКИ ЭЛЕКТРОННЫХ ПОДПИСЕЙ И СРОКИ ДЕЙСТВИЯ КЛЮЧЕВЫХ ДОКУМЕНТОВ.....	20
11. ДОПОЛНИТЕЛЬНЫЕ ПОЛОЖЕНИЯ.....	24
12. ПРИЛОЖЕНИЯ.....	27

1. СВЕДЕНИЯ ОБ УДОСТОВЕРЯЮЩЕМ ЦЕНТРЕ

Публичное акционерное общество «Промсвязьбанк», именуемое в дальнейшем «Удостоверяющий центр», зарегистрировано на территории Российской Федерации в городе Москва.

Удостоверяющий центр осуществляет свою деятельность на территории Российской Федерации в соответствии с законодательством Российской Федерации и основании следующей лицензии:

Лицензия Центра по лицензированию, сертификации и защите государственной тайны ФСБ России рег. № 16290 Н от 08 ноября 2017г. 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).

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Администратор Удостоверяющего центра – ответственный сотрудник Удостоверяющего центра, наделенный Удостоверяющим центром полномочиями по осуществлению действий по регистрации и управлению Сертификатами ключей проверки электронных подписей Пользователей Удостоверяющего центра и уполномоченный Удостоверяющим центром расписываться собственноручной подписью в копиях Сертификатов ключей проверки электронных подписей на бумажном носителе, изданных Удостоверяющим центром (заверять копии Сертификатов ключей проверки электронных подписей).

Владелец сертификата ключа проверки электронной подписи – лицо, которому в соответствии с законодательством Российской Федерации и настоящим Порядком выдан Сертификат ключа проверки электронной подписи.

Договор о реализации функций УЦ – договор о реализации функций удостоверяющего центра сервиса электронной подписи, заключаемый путем присоединения к настоящим Правилам.

Клиент (заявитель) - юридическое лицо, в том числе кредитная организация, индивидуальный предприниматель или лицо, занимающееся частной практикой, заключившее с Банком Договор, в т.ч. не имеющие Счета в Банке.

Ключ электронной подписи - уникальная последовательность символов, предназначенная для создания 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 - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи.

Ключ электронной подписи Удостоверяющего центра – ключ электронной подписи, используемый Удостоверяющим центром для создания Сертификатов ключей проверки электронной подписи и списков аннулированных Сертификатов.

Копия сертификата ключа проверки электронной подписи – документ на бумажном носителе, подписанный собственноручной подписью уполномоченным на это действие сотрудником Удостоверяющего центра и заверенный печатью Удостоверяющего центра. Содержательная часть копии Сертификата ключа проверки электронной подписи соответствует содержательной части Сертификата ключа проверки электронной подписи. Структура копии Сертификата ключа проверки электронной подписи определяется настоящим Порядком.

Пользователь Удостоверяющего центра (Пользователь) – физическое лицо – уполномоченное лицо Клиента, являющееся владельцем СКП ЭП, выданного УЦ и пользующееся сервисом электронной подписи, предоставляемым Банком.

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

- реестр заявлений о присоединении к Порядку Удостоверяющего центра;
- реестр заявлений на регистрацию в Удостоверяющем центре;
- реестр зарегистрированных пользователей Удостоверяющего центра;
- реестр заявлений на изготовление Сертификатов ключей проверки электронных подписей;
- реестр заявлений на аннулирование (отзыв) Сертификатов ключей проверки электронных подписей;
- реестр заявлений на подтверждение подлинности электронной подписи в электронном документе;
- реестр Сертификатов ключей проверки электронных подписей;
- реестр изготовленных списков аннулированных Сертификатов.

Сертификат ключа проверки электронной подписи (Сертификат, СКП ЭП) – электронный документ, выданный Удостоверяющим центром или доверенным лицом Удостоверяющего центра и подтверждающий принадлежность ключа проверки электронной подписи владельцу 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.

Сертификат ключа проверки электронной подписи Удостоверяющего центра – Сертификат ключа проверки электронной подписи, использующийся для проверки подлинности электронной подписи Удостоверяющего центра в созданных им Сертификатах ключей проверки электронной подписи и списках аннулированных Сертификатов.

Сертификат ключа проверки электронной подписи Службы актуальных статусов Сертификатов Удостоверяющего центра – Сертификат ключа проверки электронной подписи, использующийся для проверки подлинности электронной подписи в электронных ответах Службы актуальных статусов Сертификатов, содержащих информацию о статусе Сертификатов, выданных Удостоверяющим центром.

Сертификат ключа проверки электронной подписи Службы штампов времени Удостоверяющего центра – Сертификат ключа проверки электронной подписи, использующийся для проверки подлинности электронной подписи в штампах времени, сформированных Службой штампов времени Удостоверяющего центра.

Служба актуальных статусов Сертификатов – сервис Удостоверяющего центра (построенный на базе протокола OCSP), с использованием которого подписываются электронной подписью и предоставляются Пользователям УЦ электронные ответы, содержащие информацию о статусе Сертификатов, выданных Удостоверяющим центром.

Служба штампов времени – сервис Удостоверяющего центра (построенный на базе протокола TSP), с использованием которого подписываются электронной подписью и предоставляются Пользователям УЦ штампы времени.

Список аннулированных Сертификатов (САС) – электронный документ с электронной подписью Удостоверяющего центра, формируемый на определенный момент времени и включающий в себя список серийных номеров Сертификатов ключей проверки электронной подписи, которые на этот определенный момент времени аннулированы и действие которых прекращено.

Средство криптографической защиты информации (СКЗИ) – средство вычислительной техники, осуществляющее криптографические преобразования информации для обеспечения ее безопасности.

Средство электронной подписи – средство криптографической защиты информации (СКЗИ), 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 и ключей проверки электронных подписей.

Удостоверяющий центр (УЦ) – ПАО «Промсвязьбанк», осуществляющие функции по созданию и выдаче сертификатов Ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом «Об электронной подписи» в целях обеспечения применения участниками информационного взаимодействия неквалифицированной усиленной электронной подписи.

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

Электронный документ (ЭД) – 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, определяющий формат и синтаксис криптографических сообщений.

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».

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

3. СТАТУС ПОРЯДКА

3.1 Порядок реализации функций Удостоверяющего центра ПАО «Промсвязьбанк», именуемый в дальнейшем «Порядок», разработан в соответствии с законодательством Российской Федерации, регулирующим деятельность удостоверяющих центров.

Функции Удостоверяющего центра осуществляются ПАО «Промсвязьбанк» в рамках предоставления Клиенту услуги дистанционного банковского обслуживания в соответствии с договором дистанционного банковского обслуживания, заключаемом путем присоединения Клиента к Правилам обмена Электронными документами по Системе «PSB On-Line» (далее – Правила «PSB On-Line», Договор дистанционного банковского обслуживания).

3.2 Условия получения Клиентом услуг Удостоверяющего центра, необходимых для осуществления электронного взаимодействия с Банком, в том числе с целью получения банковской услуги, устанавливаются в соответствующем Договоре дистанционного банковского обслуживания, заключаемом между Клиентом и Банком.

Положения настоящего Порядка устанавливают порядок реализации функций Удостоверяющего центра, регулируемых договорными отношениями Сторон, и определяют условия выполнения Банком как Удостоверяющим центром требований Федерального закона «Об электронной подписи».

3.3. Заключение Договора о реализации функций УЦ осуществляется путем присоединения Клиента к настоящим Правилам в соответствии со статьей 428 Гражданского кодекса Российской Федерации. Договор о реализации функций УЦ заключается при условии одновременного заключения либо наличия ранее заключенного Договора дистанционного банковского обслуживания. Порядок присоединения к настоящим Правилам установлен п.4.1 Порядка.

3.4 Во всем, что не установлено настоящим Порядком Стороны руководствуются Правилами «PSB On-Line», в том числе, но не ограничиваясь, разделом 2 Правилами «PSB On-Line» «Заверения и подтверждения Сторон». В случае разночтений между Порядком и Правилами «PSB On-Line» приоритетное значение по вопросам, связанным с осуществлением функций по созданию и выдаче Сертификатов ключей проверки электронных подписей, а также иных функции Удостоверяющего центра имеет

настоящий Порядок; по вопросам, связанным с предоставлением услуг дистанционного банковского обслуживания приоритетное значение имеют Правила «PSB On-Line».

3.5. Настоящий Порядок размещается в форме электронного документа: на Интернет-сайте Системы «PSB On-Line» <http://online.payment.ru> по адресу: URL=<http://online.payment.ru>.

Правила «PSB On-Line» размещаются на Интернет-сайте Системы «PSB On-Line» <http://online.payment.ru>

4. ОБЩИЕ ПОЛОЖЕНИЯ

4.1 Присоединение к Порядку

4.1.1 Присоединение к настоящему Порядку осуществляется путем акцепта Банком (регистрации Клиента в информационной системе, в которой используется Сертификат, выданный Удостоверяющим центром) оферты Клиента в виде поданного в Банк Заявления о присоединении к Правилам «PSB On-Line» на бумажном носителе, составленного по форме Приложения 10.1 или Приложения 10.1.1 к Правилам «PSB On-Line», или в составе заявления о предоставлении комплексного банковского обслуживания Клиентам по форме, определенной Банком (для новых Клиентов Системы «PSB On-Line»). Присоединение к настоящему Порядку Клиентов, зарегистрированных в Системе «PSB On-Line» до вступления в действие Порядка, осуществляется путем направления Клиентом в Банк Запроса на создание сертификата ключа проверки электронной подписи в Удостоверяющий центр ПАО «Промсвязьбанк» (Приложение 6 к Правилам «PSB On-Line») и его регистрации Банком в установленном порядке. Заявления, указанные в настоящем пункте, далее именуются как «Заявление о присоединении».

4.1.2 Договор о реализации функций УЦ действует в течение срока действия Договора дистанционного банковского обслуживания, за исключением условий о выполнении функций Удостоверяющего центра, не связанных с предоставлением услуг дистанционного банковского обслуживания (в частности, функций по ведению Реестра Удостоверяющего центра, по предоставлению информации о статусе СКП ЭП и их действительности на определенный момент времени, по подтверждению подлинности электронной подписи (ЭП) в электронном документе, иных функций, установленным законодательством и настоящим Порядком).

4.1.3 Факт присоединения Клиента к Порядку является полным принятием им условий настоящего Порядка и всех его приложений в редакции, действующей на момент регистрации Заявления о присоединении в Реестре Удостоверяющего центра. Лицо, присоединившееся к Порядку, принимает дальнейшие изменения (дополнения), вносимые в Порядок, в соответствии с условиями настоящего Порядка.

4.1.4 Внесение изменений в Порядок, расторжение Договора о реализации функций УЦ, заключенного путем присоединения к настоящему Порядку, осуществляются согласно условиям, определенным в Правилах «PSB On-Line» для Договора дистанционного банковского обслуживания.

5. ПРЕДОСТАВЛЕНИЕ ИНФОРМАЦИИ

5.1 Удостоверяющий центр вправе запросить, а Сторона, присоединившаяся к Порядку, обязана предоставить Удостоверяющему центру документы, установленные Порядком и Правилами «PSB On-Line», а также дополнительные документы по усмотрению Удостоверяющего центра.

6. ПРАВА И ОБЯЗАННОСТИ СТОРОН

6.1 Удостоверяющий центр обязан:

6.1.1 Предоставить Пользователю Удостоверяющего центра Сертификат ключа проверки электронной подписи Удостоверяющего центра в электронной форме.

6.1.2 Использовать ключ электронной подписи Удостоверяющего центра только для подписи издаваемых им Сертификатов ключей проверки электронных подписей и списков аннулированных Сертификатов.

6.1.3 Принять меры по защите ключа электронной подписи Удостоверяющего центра от несанкционированного доступа.

6.1.4 Организовать свою работу по UTC (всемирное координированное время) с учетом часового пояса города Москвы. Удостоверяющий центр обязан синхронизировать по времени все свои программные и технические средства обеспечения деятельности.

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

6.1.6 Обеспечить занесение регистрационной информации Пользователя Удостоверяющего центра в Реестр Удостоверяющего центра и обеспечить уникальность регистрационной информации всех зарегистрированных в Удостоверяющем центре лиц, используемой для идентификации владельцев Сертификатов ключей проверки электронных подписей.

6.1.7 Изготовить Сертификат ключа проверки электронной подписи Пользователя Удостоверяющего центра по заявлению на изготовление Сертификата ключа проверки электронной подписи, в соответствии с порядком, определенным в настоящем Порядке.

6.1.8 Обеспечить уникальность серийных номеров изготавливаемых Сертификатов ключей проверки электронных подписей.

6.1.9 Обеспечить уникальность значений ключей проверки электронных подписей в изготовленных Сертификатах ключей проверки электронных подписей пользователей Удостоверяющего центра.

6.1.10 Обеспечить сохранение в тайне изготовленного ключа электронной подписи Пользователя Удостоверяющего центра.

6.1.11 Аннулировать (отозвать) Сертификат ключа проверки электронной подписи Пользователя Удостоверяющего центра по соответствующему заявлению на аннулирование (отзыв) Сертификата ключа проверки электронной подписи, в соответствии с порядком, определенным в настоящем Порядке.

6.1.12 Аннулировать (отозвать) Сертификат ключа проверки электронной подписи Пользователя Удостоверяющего центра в случае компрометации ключа электронной подписи Удостоверяющего центра, с использованием которого был издан Сертификат ключа проверки электронной подписи.

6.1.13 Официально уведомить об аннулировании (отзыве) Сертификата ключа проверки электронной подписи всех лиц, зарегистрированных в Удостоверяющем центре.

6.1.14 Опубликовать актуальный список аннулированных Сертификатов на сайте Удостоверяющего центра по адресу <http://psbank.ru/cdp/dsspsbxxxx.crl>, где xxxx – год, в течение которого действует ключ подписи ПАК УЦ. Период публикации списка аннулированных Сертификатов в рабочее время Удостоверяющего центра – один раз в сутки.

6.1.14 Информировать в письменной форме Пользователей Удостоверяющего центра об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки.

6.1.15 Осуществлять иные обязанности Удостоверяющего центра, установленные законодательством Российской Федерации.

6.2. Сторона, присоединившаяся к Порядку, обязана:

6.2.1 Известить Удостоверяющий центр об изменениях в документах, приведенных в п.5.1 и по требованию Удостоверяющего центра предоставить их в порядке, установленном Правилами «PSB On-Line».

6.2.2 С целью обеспечения гарантированного ознакомления Стороны, присоединившейся к Порядку, с полным текстом изменений и дополнений Порядка до вступления их в силу не реже одного раза в один календарный день обращаться на сайт Удостоверяющего центра по адресу <http://online.payment.ru> за сведениями об изменениях и дополнениях в Порядок.

6.2.3 Оплачивать услуги Удостоверяющего центра в соответствии с тарифами и Договором дистанционного банковского обслуживания.

6.3.3 Пользователь Удостоверяющего центра обязан:

6.3.3.1 Создавать и хранить сформированный ключ электронной подписи исключительно с использованием Сервиса электронной подписи в неэкспортируемом формате, т.е. недоступном для сохранения и использования на съемных ключевых носителях и рабочем месте пользователя.

6.3.3.2 Устанавливать и хранить в тайне персональный ПИН-код для защиты доступа к ключу электронной подписи.

6.3.3.3 Устанавливать и хранить в тайне персональный пароль для защиты доступа к сервису электронной подписи (далее – СЭП).

6.3.3.4 Хранить в тайне аутентификационную информацию и обеспечить сохранность специальных средств, используемых для подтверждения доступа и выполнения операций в СЭП, принимать все возможные меры для предотвращения их раскрытия, искажения, потери и несанкционированного использования.

6.3.3.5 Соблюдать меры безопасности, установленные в соответствии с правилами пользования СЭП.

6.3.3.6 Применять для формирования электронной подписи только действующий персональный ключ электронной подписи.

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

6.3.3.8 Применять персональный 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 проверки электронной подписи)

6.3.3.9 Не применять персональный ключ электронной подписи и немедленно обратиться в Удостоверяющий центр с заявлением на приостановление действия или прекращение действия соответствующего Сертификата ключа проверки электронной подписи в случае раскрытия, искажения персонального ключа электронной подписи, компрометации аутентификационной информации и утери специальных устройств, используемых для аутентификации (мобильного телефона и(или) SIM-карты, OTP-токена), а также в случае, если Пользователю Удостоверяющего центра стало известно, что этот ключ электронной подписи используется или использовался ранее другими лицами, в том числе *если Пользователь УЦ получил сообщение от Сервиса электронной подписи о выполнении каких-либо операций от его имени в то время, когда он их не выполнял.*

6.3.3.10 Не использовать персональный ключ электронной подписи, связанный с Сертификатом ключа проверки электронной подписи, заявление на прекращение действия которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на прекращение действия Сертификата в Удостоверяющий центр по момент времени официального уведомления о прекращении действия Сертификата, либо об отказе в прекращении действия Сертификата.

6.3.3.11 Не использовать персональный ключ электронной подписи, связанный с Сертификатом ключа проверки электронной подписи, заявление на приостановление действия которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на приостановление действия Сертификата в Удостоверяющий центр по момент времени официального уведомления о приостановлении действия Сертификата, либо об отказе в приостановлении действия.

6.3.3.12 Не использовать персональный ключ электронной подписи, связанный с Сертификатом ключа проверки электронной подписи, действие которого приостановлено или прекращено.

6.2.3.13 Не использовать персональный ключ электронной подписи до предоставления в Удостоверяющий центр подписанной копии соответствующего Сертификата ключа проверки электронной подписи.

6.4 Удостоверяющий центр имеет право:

6.4.1 Отказать пользователю в регистрации в Удостоверяющем центре в случае ненадлежащего оформления Заявления о присоединении, иных необходимых регистрационных документов, не предоставлении, не полном предоставлении документов и сведений, необходимых для идентификации Клиента, Пользователя услугами Удостоверяющего центра, а также нарушением порядка проведения такой идентификации.

6.4.2 Отказать в изготовлении Сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра в случае ненадлежащего оформления Заявления на изготовление Сертификата ключа проверки электронной подписи.

6.4.3 Отказать в аннулировании (отзыве) Сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра в случае ненадлежащего оформления соответствующего заявления на аннулирование (отзыв) Сертификата ключа проверки электронной подписи.

6.4.4 Отказать в аннулировании (отзыве) Сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра в случае, если истек установленный срок действия ключа электронной подписи, соответствующего Сертификату.

6.5 Пользователь Удостоверяющего центра имеет право:

6.5.1 Применять Сертификат ключа проверки электронной подписи Удостоверяющего центра для проверки электронной подписи Удостоверяющего центра в Сертификатах ключей проверки электронных подписей, изготовленных Удостоверяющим центром.

6.5.2 Применять список аннулированных Сертификатов ключей проверки электронных подписей, изготовленный Удостоверяющим центром, для установления статуса Сертификатов ключей проверки электронных подписей, изготовленных Удостоверяющим центром.

6.5.3 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.

Хранить сформированный Ключ электронной подписи исключительно с использованием Сервиса электронной подписи в неэкспортируемом формате, т.е. недоступном для сохранения и использования на съемных ключевых носителях и рабочем месте пользователя

6.5.4 Обратиться в Удостоверяющий центр с заявлением на изготовление Сертификата ключа проверки электронной подписи.

6.5.5 Обратиться в Удостоверяющий центр с заявлением на аннулирование (отзыв) Сертификата ключа проверки электронной подписи, владельцем которого он является, в течение срока действия соответствующего ключа.

6.5.6 Обратиться в Удостоверяющий центр за получением информации о статусе Сертификатов ключей проверки электронных подписей и их действительности на определенный момент времени.

6.5.7 Обратиться в Удостоверяющий центр за подтверждением подлинности ЭП в электронном документе, сформированной с использованием Сертификата ключа проверки электронной подписи, изданного Удостоверяющим центром.

7. ОТВЕТСТВЕННОСТЬ СТОРОН

7.1. За невыполнение или ненадлежащее выполнение обязательств по Договору о реализации функций УЦ, Стороны несут имущественную ответственность в пределах суммы доказанного реального ущерба, причиненного Стороне невыполнением или ненадлежащим выполнением обязательств другой Стороной. Ни одна из Сторон не отвечает за неполученные доходы (упущенную выгоду), которые бы получила другая Сторона.

7.2. Стороны не несут ответственность за неисполнение либо ненадлежащее исполнение своих обязательств по Договору о реализации функций УЦ, а также возникшие в связи с этим убытки в случаях, если это является следствием встречного неисполнения либо ненадлежащего встречного исполнения другой Стороной Договора о реализации функций УЦ своих обязательств.

7.3. Удостоверяющий центр не несет ответственность за неисполнение, либо ненадлежащее исполнение своих обязательств по Договору о реализации функций УЦ, а также возникшие в связи с этим убытки в случае, если Удостоверяющий центр

обоснованно полагался на сведения, указанные в заявлениях Пользователя Удостоверяющего центра.

7.4. Ответственность Сторон, не урегулированная положениями Договора о реализации функций УЦ, регулируется Правилами Системы «PSB On-Line», законодательством Российской Федерации.

8. РАЗРЕШЕНИЕ СПОРОВ

8.1 Сторонами в споре, в случае его возникновения, считаются Удостоверяющий центр и Сторона, присоединившаяся к Порядку.

8.2 При рассмотрении спорных вопросов, связанных с настоящим Порядком, Стороны будут руководствоваться законодательством Российской Федерации.

8.3 Стороны будут принимать все необходимые меры к тому, чтобы в случае возникновения спорных вопросов решить их, прежде всего, в претензионном порядке.

8.4 Сторона, получившая от другой Стороны претензию, обязана в течение 30 (Тридцати) календарных дней удовлетворить заявленные в претензии требования или направить другой Стороне мотивированный отказ с указанием оснований отказа. К ответу должны быть приложены все необходимые документы.

8.5 Спорные вопросы между Сторонами, неурегулированные в претензионном порядке, решаются в Арбитражном суде города Москвы.

9. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ И ПОЛЬЗОВАНИЯ УСЛУГАМИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

9.1 Изготовление первого Сертификата ключа проверки электронной подписи

Удостоверяющий центр осуществляет изготовление Сертификатов ключей проверки электронных подписей физическим и уполномоченным представителям юридических лиц только в том случае, если указанное лицо присоединилось к Порядку в соответствии с пунктом 4.1 настоящего Порядка.

Изготовление Сертификата ключа проверки электронной подписи осуществляется на основании заявления. Форма заявления установлена правилами системы, в которой используется Сертификат ключа проверки электронной подписи, выданный Удостоверяющим центром (Приложение 10.16 п.2.1 «Регистрация Пользователя УЦ и создание Сертификата ключа проверки электронной подписи» Правил «PSB On-Line»). Пользователь, являющийся уполномоченным представителем Стороны, присоединившейся к Порядку (если Сторона Порядка - юридическое лицо), должен предоставить доверенность, выданную на его имя по форме, установленной Правилами Системы, в которой используется Сертификат ключа проверки электронной подписи, выданный Удостоверяющим центром. (ПРИЛОЖЕНИЯ 10.15. Правил «PSB On-Line»).

Удостоверяющий центр при выполнении возложенных на него функций обязан:

- 1) Осуществлять идентификацию лиц, обратившихся за получением Сертификата ключа проверки ЭП (заявителей, Пользователей).

- 2) Отказать в осуществлении действий по заявлениям Пользователей в случае ненадлежащего оформления необходимых регистрационных заявительных документов.
 - 3) Обеспечить достоверность информации, заносимой в Сертификаты ключей проверки электронной подписи Пользователей Удостоверяющего центра.
 - 4) Инициировать отправку в Удостоверяющий центр заявок в электронной форме на создание и прекращение действия Сертификатов ключей проверки электронной подписи Пользователей на основании заявлений Пользователей.
 - 5) Обеспечить вручение Сертификатов ключей проверки электронной подписи Пользователей Удостоверяющего центра.
 - 6) Обеспечить выдачу Пользователям QR-кода в соответствии с Правилами «PSB On-Line», в которой используется QR-код (Приложение 10.16 Правил «PSB On-Line»), содержащего ключ аутентификации, для использования в мобильном приложении myDSS, в случае если Пользователю назначен метод аутентификации по мобильному приложению.
 - 7) Ознакамливать под роспись Пользователей с информацией, содержащейся в Сертификате ключа проверки электронной подписи Пользователя.
 - 8) Информировать Пользователей об условиях и о порядке использования электронных подписей и СЭП, о рисках, связанных с использованием электронных подписей, а также о мерах, необходимых для обеспечения безопасности ключей электронных подписей.
 - 9) Выдавать владельцу Сертификата руководство по обеспечению безопасности использования электронной подписи и средств электронной подписи в соответствии с Правилом «PSB On-Line».
 - 10) Выполнять требования по обеспечению защиты и сохранности в тайне конфиденциальной информации.
 - 11) Соблюдать требования законодательства Российской Федерации в области обработки и защиты персональных данных.
 - 12) Обеспечивать систематизацию, сохранность и должное хранение находящихся в работе документов.
- Дополнительно при выполнении функций посредством веб-интерфейса СЭП:
- 13) Регистрировать Пользователей в СЭП посредством веб-интерфейса СЭП.
 - 14) Назначать Пользователям методы аутентификации.
 - 15) Формировать и отправлять в Удостоверяющий центр заявки в электронной форме на создание и прекращение действия Сертификатов ключей проверки электронной подписи.
 - 16) Обеспечивать конфиденциальность Ключей электронных подписей, которые используются для взаимодействия с СЭП при работе через веб-интерфейс СЭП, их защиту от несанкционированного доступа, а также их своевременную смену.

9.2 Изготовление и получение ключа электронной подписи и Сертификата ключа проверки электронной подписи при плановой и внеплановой смене ключей Пользователя Удостоверяющего центра.

Плановая смена ключа электронной подписи и Сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра проводится не ранее одного календарного месяца до окончания срока его действия.

Внеплановая смена ключа электронной подписи и Сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра осуществляется в том случае, если Пользователь УЦ не осуществил плановую смену в установленные Порядком сроки, либо произошла компрометация ключа электронной подписи Пользователя Удостоверяющего центра.

Изготовление Сертификата ключа проверки электронной подписи при плановой и внеплановой смене осуществляется в соответствии с Правилами «PSB On-Line» (Приложения 10.16 п. 2.1 «Регистрация Пользователя УЦ и создание Сертификата ключа проверки электронной подписи» Правил «PSB On-Line»).

9.3 Аннулирование (отзыв) Сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра

Удостоверяющий центр аннулирует Сертификат ключа проверки электронной подписи Пользователя Удостоверяющего центра в следующих случаях:

- в случае прекращения действия настоящего Порядка и (или) Правил «PSB On-Line» в отношении Стороны, присоединившейся к Порядку;
 - в случае отзыва доверенности Пользователя Удостоверяющего центра;
 - по заявлению Пользователя Удостоверяющего центра;
 - по истечении срока его действия;
 - при компрометации ключа электронной подписи Удостоверяющего центра.

В случае прекращения действия настоящего Порядка, Правил «PSB On-Line», отзыва доверенности Пользователя, отзыва Сертификата Пользователя по его заявлению Удостоверяющий центр должен официально уведомить Пользователя и всех лиц, зарегистрированных в Удостоверяющем центре, об аннулировании (отзыве) Сертификата не позднее одного рабочего дня с момента наступления описанного события.

Официальным уведомлением о факте отзыва Сертификата ключа проверки электронной подписи является опубликование первого (наиболее раннего) списка аннулированных Сертификатов, содержащего сведения об отозванном Сертификате, и изданного не ранее времени наступления произошедшего случая. Временем отзыва Сертификата ключа проверки электронной подписи признается время издания указанного списка аннулированных Сертификатов, хранящееся в поле thisUpdate списка аннулированных Сертификатов.

Информация о размещении списка аннулированных Сертификатов заносится в изданные Удостоверяющим центром Сертификаты ключей проверки электронных подписей в расширение CRL Distribution Point Сертификата ключа проверки электронной подписи.

В случае аннулирования Сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра по истечении срока его действия временем аннулирования Сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра признается время, хранящееся в поле notAfter поля Validity Сертификата ключа проверки электронной подписи. В данном случае информация об аннулированном Сертификате ключа проверки электронной подписи Пользователя Удостоверяющего центра в список аннулированных Сертификатов не заносится.

В случае компрометации ключа электронной подписи Удостоверяющего центра временем аннулирования Сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра признается время компрометации ключа электронной подписи Удостоверяющего центра, фиксирующееся в Реестре

Удостоверяющего центра. В случае компрометации ключа электронной подписи Удостоверяющего центра информация о Сертификате ключа проверки электронной подписи Пользователя Удостоверяющего центра в список аннулированных Сертификатов не заносится.

9.3.1 Аннулирование (отзыв) Сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра по заявлению его владельца

Подача заявления на аннулирование (отзыв) Сертификата ключа проверки электронной подписи осуществляется в соответствии Правилами «PSB On-Line» (Приложение 10.16 к Правилам «PSB On-Line»).

После получения заявления на аннулирование (отзыв) Сертификата ключа проверки электронной подписи Оператор осуществляет следующие действия:

1. Осуществляет проверку корректности заявления;
2. Отказывает в осуществлении действий по заявлению Пользователя, в случае ненадлежащего оформления необходимых регистрационных заявительных документов;
3. Иницирует отправку в УЦ заявки в электронной форме на прекращение действия Сертификатов ключей проверки электронной подписи Пользователей на основании заявлений Пользователей.

Обработка заявления на отзыв Сертификата должна быть осуществлена не позднее рабочего дня, следующего за рабочим днем, в течение которого указанное заявление было принято.

В случае отказа в отзыве Сертификата ключа проверки электронной подписи Удостоверяющий центр уведомляет об этом Пользователя Удостоверяющего центра.

Фактом аннулирования Сертификата является публикация САС, содержащего серийный номер отозванного Сертификата, согласно расписанию работы УЦ (см. п.0).

9.3.2 Аннулирование (отзыв) Сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра по заявлению на отзыв доверенности.

Сторона, присоединившаяся к Порядку, являющаяся юридическим лицом, вправе аннулировать (отозвать) Сертификаты ключей проверки электронных подписей своих полномочных представителей, зарегистрированных в Удостоверяющем центре, путем подачи заявления на отзыв доверенности.

Форма заявления на отзыв доверенности приведена в Приложении № 1 к настоящему Порядку.

После получения заявления на отзыв доверенности Пользователя УЦ Оператор осуществляет следующие действия:

1. Осуществляет проверку корректности заявления;
2. Отказывает в осуществлении действий по заявлению Пользователя, в случае ненадлежащего оформления необходимых регистрационных заявительных документов;
3. Иницирует отправку в Удостоверяющий центр заявки в электронной форме на прекращение действия Сертификатов ключей проверки электронной подписи Пользователей на основании заявлений Пользователей.

Обработка заявления на отзыв Сертификата должна быть осуществлена не позднее рабочего дня, следующего за рабочим днем, в течение которого указанное заявление было принято.

В случае отказа в отзыве Сертификата ключа проверки электронной подписи Удостоверяющий центр уведомляет об этом Пользователя Удостоверяющего центра.

Фактом аннулирования Сертификата является публикация САС, содержащего серийный номер отозванного Сертификата, согласно расписанию работы УЦ (см. п.0).

9.4 Получение информации о статусе Сертификата ключа проверки электронной подписи, изданного Удостоверяющим центром

Получение информации о статусе Сертификата ключа проверки электронной подписи, изданного Удостоверяющим центром, осуществляется на основании заявления Пользователя Удостоверяющего центра. Данное заявление оформляется по форме Приложения № 2 настоящего Порядка и предоставляется в Удостоверяющий центр посредством почтовой либо курьерской связи или лично в офис обслуживания.

Заявление должно содержать следующую информацию:

- время и дата подачи заявления;
- время и дата (либо период времени), на момент наступления которых требуется установить статус Сертификата ключа проверки электронной подписи;
- идентификационные данные пользователя Удостоверяющего центра, статус Сертификата ключа проверки электронной подписи которого требуется установить;
- серийный номер Сертификата ключа проверки электронной подписи, статус которого требуется установить.

По результатам проведения работ по заявлению оформляется справка, содержащая информацию о статусе Сертификата ключа проверки электронной подписи, которая предоставляется Пользователю Удостоверяющего центра.

Предоставление Пользователю Удостоверяющего центра справки о статусе Сертификата ключа проверки электронной подписи должно быть осуществлено не позднее 10 (Десяти) рабочих дней с момента получения Удостоверяющим центром соответствующего заявления.

9.5 Подтверждение подлинности электронной подписи в электронном документе

По желанию Стороны, присоединившейся к Порядку, Удостоверяющий центр осуществляет проведение экспертных работ по подтверждению подлинности электронной подписи в электронном документе.

В том случае, если формат электронного документа с ЭП соответствует стандарту криптографических сообщений Cryptographic Message Syntax (CMS), то Удостоверяющий центр обеспечивает подтверждение подлинности ЭП в электронном документе. Решение о соответствии электронного документа с ЭП стандарту CMS принимает Удостоверяющий центр.

В данном случае для подтверждения подлинности ЭП в электронных документах Пользователь Удостоверяющего центра подает заявление в Удостоверяющий центр по форме, приведенной в Приложении № 4.

Заявление должно содержать следующую информацию:

- дата и время подачи заявления;
- идентификационные данные пользователя, подлинность ЭП которого необходимо подтвердить в электронном документе;
- время и дата формирования ЭП электронного документа;

- время и дата, на момент наступления которых требуется установить подлинность ЭП.

Обязательным приложением к заявлению на подтверждение подлинности ЭП в электронном документе является магнитный носитель, содержащий:

- Сертификат ключа проверки электронной подписи, с использованием которого необходимо осуществить подтверждение подлинности ЭП в электронном документе – в виде файла стандарта CMS;
- электронный документ – в виде одного файла (стандарта CMS), содержащего данные и значение ЭП этих данных, либо двух файлов: один из которых содержит данные, а другой значение ЭП этих данных (файл стандарта CMS).

Проведение работ по подтверждению подлинности ЭП в электронном документе осуществляет комиссия, сформированная из числа сотрудников Удостоверяющего центра.

Результатом проведения работ по подтверждению подлинности ЭП в электронном документе является заключение Удостоверяющего центра.

Заключение содержит:

- состав комиссии, осуществлявшей проверку;
- основание для проведения проверки;
- результат проверки ЭП электронного документа;
- данные, представленные комиссии для проведения проверки;
- отчет по выполненной проверке.

Отчет по выполненной проверке содержит:

- время и место проведения проверки;
- содержание и результаты проверки;
- обоснование результатов проверки.

Заключение Удостоверяющего центра по выполненной проверке составляется в произвольной форме в двух экземплярах, подписывается всеми членами комиссии и заверяется печатью Удостоверяющего центра. Один экземпляр заключения по выполненной проверке предоставляется заявителю.

Срок проведения работ по подтверждению подлинности ЭП в одном электронном документе и предоставлению пользователю заключения по выполненной проверке составляет десять рабочих дней с момента поступления заявления в Удостоверяющий центр.

В том случае, если формат электронного документа с ЭП не соответствует стандарту криптографических сообщений Cryptographic Message Syntax (CMS), то проведение экспертных работ по подтверждению подлинности ЭП осуществляется в рамках заключения отдельного договора (соглашения) между Удостоверяющим центром и Стороной, присоединившейся к Порядку. Перечень исходных данных для проведения экспертизы, состав и содержание отчетных документов (акты, заключения и т.д.), сроки проведения работ, размер вознаграждения Удостоверяющего центра определяются указанным договором (соглашением).

9.6 Предоставление Удостоверяющим центром сервисов Службы актуальных статусов Сертификатов и Службы штампов времени

Удостоверяющий центр оказывает услуги по предоставлению актуальной информации о статусе Сертификатов посредством Сервиса службы актуальных статусов Сертификатов. Служба актуальных статусов Сертификатов по запросам пользователей Удостоверяющего центра формирует и предоставляет этим пользователям OCSP-ответы, которые содержат информацию о статусе запрашиваемого Сертификата ключа проверки электронной подписи. OCSP-ответы представляются в форме электронного документа, подписанного электронной подписью с использованием Сертификата ключа проверки электронной подписи Службы актуальных статусов Сертификатов (Оператора Службы актуальных статусов Сертификатов). OCSP-ответ признается действительным при одновременном выполнении следующих условий:

- Подтверждена подлинность ЭП Службы актуальных статусов Сертификатов (Оператора Службы актуальных статусов Сертификатов) в OCSP-ответе;
- Сертификат ключа проверки электронной подписи Службы актуальных статусов Сертификатов (Оператора Службы актуальных статусов Сертификатов) на момент подтверждения подлинности ЭП OCSP-ответа действителен;
- Ключ электронной подписи Службы актуальных статусов Сертификатов (Оператора Службы актуальных статусов Сертификатов) на момент формирования OCSP-ответа действителен;
- Сертификат ключа проверки электронной подписи Службы актуальных статусов Сертификатов (Оператора Службы актуальных статусов Сертификатов) содержит в расширении Extended Key Usage область использования – Подпись ответа службы OCSP (1.3.6.1.5.5.7.3.9);

Адрес обращения к Службе актуальных статусов Сертификатов Удостоверяющего центра – <http://psbank.ru/ocsp/ocsp.srf>

_. Указанный адрес заносится в расширение Authority Information Access (AIA) издаваемых Удостоверяющим центром Сертификатов ключей проверки электронных подписей.

Удостоверяющий центр оказывает услуги по выдаче штампов времени посредством сервиса Службы штампов времени. Штамп времени, относящийся к подписанному ЭП электронному документу, признается действительным при одновременном выполнении следующих условий:

- Подтверждена подлинность ЭП Службы штампов времени (Оператора Службы штампов времени) в штампе времени;
- Сертификат ключа проверки электронной подписи Службы штампов времени (Оператора Службы штампов времени) на момент подтверждения подлинности ЭП штампа времени действителен;
- Ключ электронной подписи Службы штампов времени (Оператора Службы штампов времени) на момент формирования штампа времени действителен;
- Сертификат ключа проверки электронной подписи Службы штампов времени (Оператора Службы штампов времени) содержит в расширении Extended Key Usage область использования – Установка штампа времени (1.3.6.1.5.5.7.3.8);

Адрес обращения к Службе штампов времени Удостоверяющего центра – <http://psbank.ru/tsp/tsp.srf>.

9.7 Прочие условия

9.7.1 Период времени действия ключа, соответствующего выданному Сертификату ключа проверки электронной подписи Пользователя Удостоверяющего центра должен находиться в пределах периода времени, на который Стороной, присоединившейся к Порядку (для юридических лиц) выдана соответствующая доверенность на совершение действий, определенных положениями настоящего Порядка для Пользователя Удостоверяющего центра.

10. СТРУКТУРА СЕРТИФИКАТОВ КЛЮЧЕЙ ПРОВЕРКИ ЭЛЕКТРОННЫХ ПОДПИСЕЙ И СРОКИ ДЕЙСТВИЯ КЛЮЧЕВЫХ ДОКУМЕНТОВ

10.1 Структура Сертификата ключа проверки электронной подписи 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 34.11-2012/34.10-2012 256 бит
Issuer	Издатель Сертификата	CommonName = ПАО «Промсвязьбанк» – псевдоним Удостоверяющего центра Organization (Организация) = ПАО «Промсвязьбанк» STREET = Улица Смирновская дом 10 строение 22 L = Москва S = 77 Москва C = RU ИНН = 007744000912 ОГРН = 1027739019142
Validity Period	Срок действия Сертификата	Действителен с (notBefore): дд.мм.гггг чч:мм:сс UTC Действителен по(notAfter): дд.мм.гггг чч:мм:сс UTC
Subject	Владелец Сертификата	CommonName = ПАО «Промсвязьбанк» – псевдоним Удостоверяющего центра Organization (Организация) = ПАО «Промсвязьбанк» STREET = Улица Смирновская дом 10 строение 22 L = Москва S = 77 Москва C = RU ИНН = 007744000912 ОГРН = 1027739019142
Public Key	Открытый ключ	Открытый ключ (алгоритм ГОСТ 34.10-2012 256 бит)
Issuer Signature Algorithm	Алгоритм подписи издателя Сертификата	ГОСТ Р 34.11-2012/34.10-2012 256 бит
Issuer Sign	ЭП издателя Сертификата	Подпись издателя в соответствии с ГОСТ Р 34.11-2012/34.10-2012 256 бит
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 Identifier	Идентификатор ключа владельца Сертификата	Идентификатор ключа электронной подписи Удостоверяющего центра, соответствующего данному Сертификату
BasicConstraints	Основные ограничения	SubjectType (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 Удостоверяющего центра

10.2 Структура Сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра (клиентский Сертификат ключа проверки электронной подписи)

Название	Описание	Содержание
Базовые поля Сертификата		
Version	Версия	V3
Serial Number	Серийный номер	Уникальный серийный номер Сертификата
Signature Algorithm	Алгоритм подписи	ГОСТ Р 34.11-2012/34.10-2012 256 бит
Issuer	Издатель Сертификата	CN = ПАО "Промсвязьбанк" O = ПАО "Промсвязьбанк" STREET = Улица Смирновская дом 10 строение 22 L = Москва S = 77 Москва C = RU ИНН = 007744000912 ОГРН = 1027739019142
Validity Period	Срок действия Сертификата	Действителен с (notBefore): дд.мм.гггг чч:мм:сс UTC Действителен по(notAfter): дд.мм.гггг чч:мм:сс UTC
Subject	Владелец Сертификата	CN = Фамилия Имя Отчество владельца Сертификата C = RU Компонента имени CN обязательна для заполнения, необходимость заполнения остальных значений определяется владельцем Сертификата. В поле Subject Сертификата могут быть добавлены дополнительные компоненты имени согласно RFC 3280
Public Key	Открытый ключ	Открытый ключ (алгоритм подписи ГОСТ 34.10-2012 256 би)
Issuer Signature Algorithm	Алгоритм подписи издателя Сертификата	ГОСТ Р 34.11-2012/34.10-2012 256 бит
Issuer Sign	ЭП издателя Сертификата	Подпись издателя в соответствии с ГОСТ Р 34.11-2012/34.10-2012 256 бит
Расширения Сертификата		
Key Usage (critical)	Использование ключа	Неотрекаемость - невозможность осуществления отказа от совершенных действий; Цифровая подпись, Шифрование ключей, Шифрование данных
Extended Key Usage	Улучшенный ключ	Набор областей использования ключей и Сертификатов из перечня областей использования, зарегистрированных в Удостоверяющем центре за исключением области использования – Проверка подлинности сервера (1.3.6.1.5.5.7.3.1)
Application Policy	Политика применения	Набор областей использования ключей и Сертификатов из перечня областей использования, зарегистрированных в Удостоверяющем центре за исключением области использования – Проверка подлинности сервера (1.3.6.1.5.5.7.3.1)
Subject Key Identifier	Идентификатор ключа владельца Сертификата	Идентификатор ключа владельца Сертификата
Authority Key Identifier	Идентификатор ключа издателя Сертификата	Идентификатор ключа электронной подписи Удостоверяющего центра, на котором подписан данный Сертификат
CRL Distribution Point	Точка распространения списка аннулированных Сертификатов	Набор адресов точек распространения списков аннулированных Сертификатов следующего вида: URL=http://ResourceServer/Path/hex.crl, где ResourceServer – имя сервера, Path – путь к файлу списка аннулированных Сертификатов, hex – шестнадцатеричное значение идентификатора ключа электронной подписи Удостоверяющего центра, с использованием которого издан Сертификат и список аннулированных 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

10.3 Структура Сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра (серверный Сертификат ключа проверки электронной подписи)

Название	Описание	Содержание
Базовые поля Сертификата		
Version	Версия	V3
Serial Number	Серийный номер	Уникальный серийный номер Сертификата
Signature Algorithm	Алгоритм подписи	ГОСТ Р 34.11-2012/34.10-2012 256 бит
Issuer	Издатель Сертификата	CN = ПАО "Промсвязьбанк" O = ПАО "Промсвязьбанк" STREET = Улица Смирновская дом 10 строение 22 L = Москва S = 77 Москва C = RU ИНН = 007744000912 ОГРН = 1027739019142
Validity Period	Срок действия Сертификата	Действителен с (not Before): дд.мм.гггг чч:мм:сс UTC Действителен по (not After): дд.мм.гггг чч:мм:сс UTC
Subject	Владелец Сертификата	CommonName = Псевдоним (как правило, DNS-имя сервера) L = Москва S = 77 Москва C = RU Компонента имени CN обязательна для заполнения, необходимость заполнения остальных значений определяется владельцем Сертификата. В поле Subject Сертификата могут быть добавлены дополнительные компоненты имени согласно RFC 3280
Public Key	Открытый ключ	Открытый ключ (алгоритм подписи ГОСТ 34.10-2012 256 би)
Issuer Signature Algorithm	Алгоритм подписи издателя Сертификата	ГОСТ Р 34.11-2012/34.10-2012 256 бит
Issuer Sign	ЭП издателя Сертификата	Подпись издателя в соответствии с ГОСТ Р 34.11-2012/34.10-2012 256 бит
Расширения Сертификата		
Key Usage (critical)	Использование ключа	Неотрекаемость - невозможность осуществления отказа от совершенных действий; Цифровая подпись, Шифрование ключей, Шифрование данных
Extended Key Usage	Улучшенный ключ	Набор областей использования ключей и Сертификатов из перечня областей использования, зарегистрированных в Удостоверяющем центре, включающий область использования – Проверка подлинности сервера (1.3.6.1.5.5.7.3.1)
Application Policy	Политика применения	Набор областей использования ключей и Сертификатов из перечня областей использования, зарегистрированных в Удостоверяющем центре, включающий область использования – Проверка подлинности сервера (1.3.6.1.5.5.7.3.1)
Subject Key Identifier	Идентификатор ключа владельца Сертификата	Идентификатор ключа владельца Сертификата
Authority Key Identifier	Идентификатор ключа издателя Сертификата	Идентификатор ключа электронной подписи Удостоверяющего центра, на котором подписан данный Сертификат
CRL Distribution Point	Точка распространения списка аннулированных Сертификатов	Набор адресов точек распространения списков аннулированных Сертификатов следующего вида: URL=http://ResourceServer/Path/hex.crl, где ResourceServer – имя сервера, Path – путь к файлу списка аннулированных Сертификатов, hex – шестнадцатеричное значение идентификатора ключа электронной подписи Удостоверяющего центра, с использованием которого издан Сертификат и список аннулированных 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

10.4 Структура списка аннулированных Сертификатов (CRL) Удостоверяющего центра

Название	Описание	Содержание
Базовые поля списка аннулированных Сертификатов		
Version	Версия	V2
Issuer	Издатель СОС	CN = ПАО "Промсвязьбанк" O = ПАО "Промсвязьбанк" STREET = Улица Смирновская дом 10 строение 22 L = Москва S = 77 Москва C = RU ИНН = 007744000912 ОГРН = 1027739019142
thisUpdate	Время издания СОС	дд.мм.гггг чч.мм.сс UTC
nextUpdate	Время, по которое действителен СОС	дд.мм.гггг чч.мм.сс UTC
revokedCertificates	Список аннулированных 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 34.11-2012/34.10-2012 256 бит
Issuer Sign	Подпись издателя СОС	Подпись издателя в соответствии с ГОСТ Р 34.11-2012/34.10-2012 256 бит
Расширения списка аннулированных Сертификатов		
Authority Key Identifier	Идентификатор ключа издателя	Идентификатор ключа электронной подписи Удостоверяющего центра, на котором подписан СОС
SzOID_CertSrv_CA_Version	Объектный идентификатор Сертификата издателя	Версия Сертификата Удостоверяющего центра

10.5 Расширения Key Usage, Extended Key Usage, Application Policy Сертификата ключа проверки электронной подписи содержат объектные идентификаторы (OID), определяющие области использования ключей электронных подписей и Сертификатов ключей проверки электронных подписей.

10.6 Список объектных идентификаторов, зарегистрированных в Удостоверяющем центре и определяющих отношения, возникающие между Удостоверяющим центром и пользователями Удостоверяющего центра, приведен в Приложении № 12 настоящего Порядка.

10.7 Список объектных идентификаторов, зарегистрированных в Удостоверяющем центре и определяющих отношения, возникающие между Пользователями Удостоверяющего центра - участниками конкретных информационных систем, устанавливается документами данной конкретной информационной системы.

10.8 Сертификат ключа проверки электронной подписи пользователя Удостоверяющего центра (клиентский Сертификат) в расширении Extended Key Usage или Application Policy должен содержать, включая, но не ограничиваясь, следующие области использования:

- Проверка подлинности клиента (1.3.6.5.5.7.3.2);
- Защищенная электронная почта (1.3.6.1.5.5.7.3.4).

10.9 Сертификат ключа проверки электронной подписи пользователя Удостоверяющего центра (серверный Сертификат) в расширении Extended Key Usage или Application Policy должен содержать, включая, но не ограничиваясь, следующие области использования:

- Проверка подлинности сервера (1.3.6.5.5.7.3.1).

10.10 Сроки действия ключевых документов

10.10.1 Сроки действия ключевых документов Удостоверяющего центра

Срок действия ключа электронной подписи 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 Удостоверяющего центра исчисляется с даты и времени генерации ключа электронной подписи Удостоверяющего центра.

Срок действия Сертификата ключа проверки электронной подписи Удостоверяющего центра не превышает 30 (Тридцать) лет. Время начала периода действия Сертификата ключа проверки электронной подписи Удостоверяющего центра и его окончания заносится в поля «notBefore» и «not After» поля «Validity Period» соответственно.

10.10.2 Сроки действия ключевых документов Пользователей Удостоверяющего центра

Срок действия ключа электронной подписи Пользователя Удостоверяющего центра составляет 15 (Пятнадцать) месяцев.

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

Срок действия Сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра (клиентский Сертификат ключа проверки электронной подписи) не превышает 30 (Тридцать) лет. Время начала периода действия Сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра и его окончания заносится в поля «notBefore» и «not After» поля «Validity Period» соответственно.

Срок действия Сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра (серверный Сертификат ключа проверки электронной подписи) составляет 15 (Пятнадцать) месяцев.

11. ДОПОЛНИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

11.1 Плановая смена ключей Удостоверяющего центра

Плановая смена ключей Удостоверяющего центра выполняется в период действия ключа электронной подписи Удостоверяющего центра.

Процедура плановой смены ключей Удостоверяющего центра осуществляется в следующем порядке:

- Уполномоченное лицо Удостоверяющего центра генерирует новый ключ ЭП и соответствующий ему ключ проверки ЭП;
- Уполномоченное лицо Удостоверяющего центра изготавливает новый Сертификат ключа проверки электронной подписи Удостоверяющего центра.

Уведомление пользователей о проведении смены ключей Удостоверяющего центра осуществляется посредством электронной почты.

Старый ключ электронной подписи Удостоверяющего центра используется в течение своего срока действия для формирования списков аннулированных Сертификатов, изданных Удостоверяющим центром в период действия старого ключа электронной подписи Удостоверяющего центра.

11.2 Компрометация ключевых документов Удостоверяющего центра, внеплановая смена ключей Удостоверяющего центра

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

После аннулирования Сертификата Удостоверяющего центра выполняется процедура внеплановой смены ключей Удостоверяющего центра. Процедура внеплановой смены ключей Удостоверяющего центра выполняется в порядке, определенном процедурой плановой смены ключей Удостоверяющего центра (пункт 11.1 настоящего Порядка).

Все действовавшие на момент компрометации ключа электронной подписи Удостоверяющего центра Сертификаты ключей проверки электронных подписей, а также Сертификаты, действие которых было приостановлено, подлежат внеплановой смене.

11.3 Компрометация ключевых документов Пользователя Удостоверяющего центра

Пользователь Удостоверяющего центра самостоятельно принимает решение о факте или угрозе компрометации своего ключа ЭП.

В случае компрометации или угрозы компрометации ключа ЭП Пользователь подает заявление на аннулирование (отзыв) Сертификата ключа проверки электронной подписи посредством почтовой или курьерской связи по форме Приложения № 5.

Пользователь Удостоверяющего центра осуществляет внеплановую смену ключей в соответствии с пунктом 10.2 настоящего Порядка.

11.4 Конфиденциальность информации

11.4.1 Типы конфиденциальной информации

11.4.1.1 Ключ электронной подписи, соответствующий Сертификату ключа проверки электронной подписи, является конфиденциальной информацией лица, зарегистрированного в Удостоверяющем центре. Удостоверяющий центр не

осуществляет хранение ключей электронных подписей Пользователей Удостоверяющего центра

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

11.4.2 Типы информации, не являющейся конфиденциальной

11.4.2.1 Информация, не являющаяся конфиденциальной информацией, считается открытой информацией

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

11.4.2.3 Информация, включаемая в Сертификаты ключей подписи и списки аннулированных Сертификатов, издаваемые Удостоверяющим центром, не считается конфиденциальной

11.4.2.4 Персональные данные, включаемые в Сертификаты ключей проверки электронных подписей, издаваемые Удостоверяющим центром, относятся к общедоступным персональным данным

11.4.2.5 Информация, содержащаяся в настоящем Порядке, не считается конфиденциальной

11.4.3 Исключительные полномочия Удостоверяющего центра

11.4.3.1 Удостоверяющий центр имеет право раскрывать конфиденциальную информацию третьим лицам только в случаях, установленных законодательством Российской Федерации

11.5 Хранение Сертификатов ключей проверки электронных подписей в Удостоверяющем центре

Срок хранения Сертификата ключа проверки электронной подписи в Удостоверяющем Центре осуществляется в течение всего периода его действия и 5 (Пять) лет после его аннулирования (отзыва). По истечении указанного срока хранения Сертификаты ключа проверки электронной подписи переводятся в режим архивного хранения.

11.6 Прекращение оказания услуг Удостоверяющим центром

11.6.1 В случае расторжения договора, заключенного путем присоединения к Порядку, одной из Сторон все Сертификаты ключей проверки электронных подписей, владельцами которых являются Пользователь УЦ - Сторона Порядка (если Сторона Порядка – физическое лицо) и Пользователи УЦ – полномочные представители Стороны Порядка (если Сторона Порядка – юридическое лицо), аннулируются (отзываются) Удостоверяющим центром.

11.7 Форс-мажор

11.7.1 Стороны освобождаются от ответственности за полное или частичное неисполнение своих обязательств по настоящему Порядку, если это неисполнение

явилось следствием форс-мажорных обстоятельств, возникших после присоединения к настоящему Порядку

11.7.2 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 аппаратно-программного обеспечения, пожары, взрывы и иные техногенные катастрофы, действия (бездействие) государственных и муниципальных органов, повлекшие невозможность исполнения Стороной/Сторонами своих обязательств по настоящему Порядку.

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

11.7.4 Сторона, для которой создалась невозможность исполнения своих обязательств по настоящему Порядку, 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

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

11.7.6 В случае, если невозможность полного или частичного исполнения Сторонами какого-либо обязательства по настоящему Порядку 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

12. ПРИЛОЖЕНИЯ

Приложение №1
к Порядку реализации функций удостоверяющего центра
Публичного акционерного общества «Промсвязьбанк»

(Форма заявления на отзыв доверенности Пользователя Удостоверяющего центра)

Заявление на отзыв доверенности

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

в лице _____,
(должность)

_____ (фамилия, имя, отчество)

действующего на основании _____

Заявляет, что отзывает Доверенность № ____ от « ____ » _____ 20__ года, выданную для представления в Удостоверяющий центр ПАО «Промсвязьбанк»

своему полномочному представителю _____
(фамилия, имя, отчество)

и просит аннулировать (отозвать) все действующие Сертификаты ключей проверки электронных подписей, владельцем которых является

(фамилия, имя, отчество)

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

Приложение №2
к Порядку реализации функций удостоверяющего центра
Публичного акционерного общества «Промсвязьбанк»

(Форма заявления на получение информации о статусе Сертификата)

Для юридических лиц

Заявление на получение информации о статусе Сертификата ключа проверки
электронной подписи, изданного Удостоверяющим центром ПАО «Промсвязьбанк»

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

в лице _____,
(должность руководителя)

_____ (фамилия, имя, отчество руководителя)

действующего на основании _____

Просит предоставить информацию о статусе следующего Сертификата ключа проверки
электронной подписи:

SerialNumber (SN)	Серийный номер Сертификата ключа проверки электронной подписи
Title (T)	Должность
CommonName (CN)	Фамилия, Имя, Отчество (псевдоним)
OrganizationUnit (OU)	Наименование подразделения
Organization (O)	Наименование организации
Locality (L)	Город
State (S)	Область
Contry (C)	Страна
E-Mail (E)	Адрес электронной почты

Время¹ (период времени) на момент наступления которого требуется установить статус
Сертификата: с «_____» по «_____».

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

¹ Время и дата должны быть указаны с учетом часового пояса г. Москвы (по Московскому времени). Если время и дата не указаны, то статус Сертификата устанавливается на момент времени принятия заявления Удостоверяющим центром

Приложение №3
к Порядку реализации функций Удостоверяющего центра
Публичного акционерного общества «Промсвязьбанк»

(Форма заявления на получение информации о статусе Сертификата)

Для физических лиц

Заявление на получение информации о статусе Сертификата ключа проверки
электронной подписи, изданного Удостоверяющим центром ПАО «Промсвязьбанк»

Я, _____
(фамилия, имя, отчество)

Прошу предоставить информацию о статусе следующего Сертификата ключа проверки
электронной подписи:

SerialNumber (SN)	Серийный номер Сертификата ключа проверки электронной подписи
Title (T)	Должность
CommonName (CN)	Фамилия, Имя, Отчество (псевдоним)
OrganizationUnit (OU)	Наименование подразделения
Organization (O)	Наименование организации
Locality (L)	Город
State (S)	Область
Contry (C)	Страна
E-Mail (E)	Адрес электронной почты

Время² (период времени) на момент наступления которого требуется установить статус Сертификата: с « _____ » по « _____ ».

Пользователь Удостоверяющего центра
ПАО «Промсвязьбанк»

_____/_____/_____
« ____ » _____ 20__ г.

² Время и дата должны быть указаны с учетом часового пояса г. Москвы (по Московскому времени). Если время и дата не указаны, то статус Сертификата устанавливается на момент времени принятия заявления Удостоверяющим центром

Приложение №4
к Порядку реализации функций Удостоверяющего центра
Публичного акционерного общества «Промсвязьбанк»

(Форма заявления на подтверждение подлинности ЭП)

Для юридических лиц

Заявление на подтверждение подлинности электронной подписи в электронном документе

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

в лице _____,
(должность руководителя)

_____ (фамилия, имя, отчество руководителя)

действующего на основании _____

Просит подтвердить подлинность ЭП в электронном документе на основании следующих данных:

1. Файл формата CMS, содержащий Сертификат ключа проверки электронной подписи, с использованием которого необходимо осуществить подтверждение подлинности ЭП в электронном документе на прилагаемом к заявлению магнитном носителе – рег. № МД–XXX;
2. Файл, содержащий подписанные ЭП данные и значение ЭП формата CMS, либо файл, содержащий исходные данные и файл, содержащий значение ЭП формата CMS, на прилагаемом к заявлению магнитном носителе – рег. № МД–XXX
3. Время³ на момент наступления которых требуется подтвердить подлинность ЭП:
« ____ : ____ » « ____ / ____ / ____ »;
Час минута день месяц год

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

³ Время и дата должны быть указаны с учетом часового пояса г. Москвы (по Московскому времени). Если время и дата не указаны, то подтверждение подлинности ЭП устанавливается на момент времени принятия заявления Удостоверяющим центром

Приложение №5
к Порядку реализации функций удостоверяющего центра
Публичного акционерного общества «Промсвязьбанк»

(Форма заявления на подтверждение подлинности ЭП)

Для физических лиц

Заявление на подтверждение подлинности электронной подписи в электронном документе

Я, _____
(фамилия, имя, отчество)

прошу подтвердить подлинность ЭП в электронном документе на основании следующих данных:

1. Файл формата CMS, содержащий Сертификат ключа проверки электронной подписи, с использованием которого необходимо осуществить подтверждение подлинности ЭП в электронном документе на прилагаемом к заявлению магнитном носителе – рег. № МД–XXX;
2. Файл, содержащий подписанные ЭП данные и значение ЭП формата CMS, либо файл, содержащий исходные данные и файл, содержащий значение ЭП формата CMS, на прилагаемом к заявлению магнитном носителе – рег. № МД–XXX
3. Время⁴ на момент наступления которых требуется подтвердить подлинность ЭП:
« ____ : ____ » « ____ / ____ / ____ »;
Час минута день месяц год

Пользователь Удостоверяющего центра
ПАО «Промсвязьбанк»

« ____ » ____ / ____ / ____ /
« ____ » ____ 20 ____ г.

⁴ Время и дата должны быть указаны с учетом часового пояса г. Москвы (по Московскому времени). Если время и дата не указаны, то подтверждение подлинности ЭП устанавливается на момент времени принятия заявления Удостоверяющим центром

Приложение №6
к Порядку реализации функций удостоверяющего центра
Публичного акционерного общества «Промсвязьбанк»

(Форма печати копии Сертификата ключа проверки электронной подписи)

**Удостоверяющий центр ПАО "Промсвязьбанк"
Сертификат ключа проверки электронной подписи
сведения о Сертификате:**

Версия: 3

Серийный номер: <уникальный серийный номер Сертификата>

Издатель Сертификата: CN=ПАО "Промсвязьбанк", O=ПАО "Промсвязьбанк",
STREET=Улица Смирновская дом 10 строение 22, L=Москва, S=77 Москва, C=RU,
ИНН=007744000912, ОГРН=1027739019142

Владелец Сертификата: CN=<ФИО владельца Сертификата>, C=RU, O=PSBank

Срок действия:

Действителен с: 13.05.2020 10:21:05

Действителен по: 13.08.2021 10:31:05

Ключ проверки электронной подписи:

Алгоритм: ГОСТ Р 34.10-2012 256 бит (1.2.643.7.1.1.1.1)

Параметры: 30 13 06 07 2A 85 03 02 02 24 00 06 08 2A 85 03 07 01 01 02 02

Значение: <значение открытого ключа>

Расширения Сертификата X.509

Расширение: Использование ключа (критичное)

Идентификатор: 2.5.29.15

Значение: Цифровая подпись, Неотрекаемость, Шифрование ключей, Согласование ключей (e8)

Расширение: Идентификатор ключа субъекта

Идентификатор: 2.5.29.14

Значение: <значение идентификатора ключа владельца Сертификата>

Расширение: Сведения о шаблоне Сертификата

Идентификатор: 1.3.6.1.4.1.311.21.7

Значение: Шаблон=1.2.643.2.2.50.1.9.5795931.2993114.8933208.7485633.43646.14987,
Основная версия=1, Вспомогательная версия=0

Расширение: Улучшенный ключ

Идентификатор: 2.5.29.37

Значение: Проверка подлинности клиента (1.3.6.1.5.5.7.3.2), Защищенная электронная почта (1.3.6.1.5.5.7.3.4)

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://psbank.ru/ocsp/ocsp.srf>, [2]Доступ к сведениям центра сертификации: метод доступа=Поставщик центра сертификации (1.3.6.1.5.5.7.48.2), дополнительное имя=URL= <http://psbank.ru/root/dsspsbxxxx.cer>

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://psbank.ru/cdp/dsspsbxxxx.crl

Расширение: Идентификатор ключа центра Сертификатов

Идентификатор: 2.5.29.35

Значение: Идентификатор ключа=<значение идентификатора ключа центра сертификации>, Поставщик Сертификата: Адрес каталога: CN="ПАО

"Промсвязьбанк"", O="ПАО "Промсвязьбанк"", STREET=Улица Смирновская дом 10 строение 22, L=Москва, S=77 Москва, C=RU,

ИНН=007744000912, ОГРН=1027739019142, Серийный номер Сертификата =

<значение серийного номера>

Расширение: Период использования ключа электронной подписи

Идентификатор: 2.5.29.16

Значение: Действителен с 13 мая 2020 г. 10:21:04 по 13 августа 2021 г. 10:21:04

Подпись Удостоверяющего центра:

Алгоритм подписи: ГОСТ Р 34.11-2012/34.10-2012 256 бит (1.2.643.7.1.1.3.2)

Параметры:

Значение: <значение подписи УЦ>

Подпись владельца Сертификата:

_____/_____
"__"_____
20__ г.

Подпись доверенного лица:

_____/_____
"__"_____
20__ г.

М. П.

Приложение №7
к Порядку реализации функций удостоверяющего центра
Публичного акционерного общества «Промсвязьбанк»

Список объектных идентификаторов (OID), зарегистрированных в удостоверяющем центре ПАО «Промсвязьбанк» и определяющих области использования ключей электронных подписей проверки электронных подписей и Сертификатов ключей проверки электронных подписей

	OID	Область применения
1.	1.3.6.1.5.5.7.3.9	Подпись ответа службы OCSP – формирование электронной подписи ответов Службы актуальных статусов Сертификатов
2.	1.3.6.1.5.5.7.3.8	Установка штампа времени – формирование электронной подписи штампов времени, предоставляемых Службой штампов времени