

РЕГЛАМЕНТ
Удостоверяющего Центра
ЗАО «Агропромбанк»

Версия 3.0

Оглавление

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ.....	3
2. ОБЩИЕ ПОЛОЖЕНИЯ	5
2.1. ПРЕДМЕТ РЕГЛАМЕНТА	5
2.2. ДЕЙСТВИЕ РЕГЛАМЕНТА	5
3. ПРАВА И ОБЯЗАННОСТИ СТОРОН.....	6
3.1. ПРАВА УДОСТОВЕРЯЮЩЕГО ЦЕНТРА	6
УДОСТОВЕРЯЮЩИЙ ЦЕНТР ИМЕЕТ ПРАВО:	6
3.2. ПРАВА ПОЛЬЗОВАТЕЛЯ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА	6
ПОЛЬЗОВАТЕЛЬ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА ИМЕЕТ ПРАВО:	6
3.3. ОБЯЗАННОСТИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА.....	7
3.4. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА.....	8
4. ПРАВИЛА ПОЛЬЗОВАНИЯ УСЛУГАМИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА.....	8
4.1. РЕГИСТРАЦИЯ ПОЛЬЗОВАТЕЛЕЙ.....	8
4.2. ГЕНЕРАЦИЯ КЛЮЧЕЙ.....	9
4.3. ИЗГОТОВЛЕНИЕ И ПОЛУЧЕНИЕ СЕРТИФИКАТА ОТКРЫТОГО КЛЮЧА ЭЛЕКТРОННОЙ ПОДПИСИ.....	9
4.4. АННУЛИРОВАНИЕ СЕРТИФИКАТА ОТКРЫТОГО КЛЮЧА ЭЛЕКТРОННОЙ ПОДПИСИ	9
4.5. ПОРЯДОК ОПЛАТЫ КОМИССИОННОГО ВОЗНАГРАЖДЕНИЯ ЗА ОКАЗЫВАЕМЫЕ УСЛУГИ.....	10
4.6. ТОКЕНЫ.....	11
5. ПРОЧИЕ УСЛОВИЯ.....	12
5.1. КОНФИДЕНЦИАЛЬНОСТЬ	12
5.2. ПЛАНОВАЯ СМЕНА КЛЮЧЕЙ УПОЛНОМОЧЕННОГО ЛИЦА УДОСТОВЕРЯЮЩЕГО ЦЕНТРА.....	12
5.3. КОМПРОМЕТАЦИЯ КЛЮЧА УДОСТОВЕРЯЮЩЕГО ЦЕНТРА.....	13
5.4. КОМПРОМЕТАЦИЯ КЛЮЧА ПОЛЬЗОВАТЕЛЯ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА.....	13
5.5. ПРЕКРАЩЕНИЕ ДЕЯТЕЛЬНОСТИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА.....	13
5.6. ОПУБЛИКОВАНИЕ И ОПОВЕЩЕНИЕ	13
5.7. СРОКИ ДЕЙСТВИЯ КЛЮЧЕЙ УПОЛНОМОЧЕННОГО ЛИЦА УДОСТОВЕРЯЮЩЕГО ЦЕНТРА.....	14
5.8. СРОКИ ДЕЙСТВИЯ КЛЮЧЕЙ ПОЛЬЗОВАТЕЛЕЙ	14
5.9. ХРАНЕНИЕ СЕРТИФИКАТОВ ОТКРЫТОГО КЛЮЧА ЭЛЕКТРОННОЙ ПОДПИСИ В УДОСТОВЕРЯЮЩЕМ ЦЕНТРЕ	14
5.10. СТРУКТУРА СЕРТИФИКАТА ОТКРЫТОГО КЛЮЧА ЭЛЕКТРОННОЙ ПОДПИСИ И СПИСКОВ АННУЛИРОВАННЫХ СЕРТИФИКАТОВ	14
6. РАЗРЕШЕНИЕ СПОРОВ	17
7. РИСКИ, СВЯЗАННЫЕ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННОЙ ПОДПИСИ.....	17
8. ОТВЕТСТВЕННОСТЬ СТОРОН	17
9. РЕКВИЗИТЫ УЦ	17
ПРИЛОЖЕНИЕ №1А	18
ПРИЛОЖЕНИЕ №1Б.....	19
ПРИЛОЖЕНИЕ №1В.....	20
ПРИЛОЖЕНИЕ №1Г	21
ПРИЛОЖЕНИЕ №1Д.....	23
ПРИЛОЖЕНИЕ №1Е.....	24
ПРИЛОЖЕНИЕ №1Ж	25
ПРИЛОЖЕНИЕ №2.....	26
ПРИЛОЖЕНИЕ №3.....	30
ПРИЛОЖЕНИЕ №4.....	35

1. Термины и определения

Бизнес-система - обобщенное понятие корпоративной информационной системы, эксплуатирующийся в ЗАО «Агропромбанк» (далее – Банк), в которой используются ключи электронной подписи и сертификаты открытых ключей электронной подписи, и предоставляющей определенные услуги Пользователям - участникам этой системы.

Владелец сертификата открытого ключа электронной подписи (Владелец сертификата) - физическое лицо, которому Удостоверяющим центром Банка выдан Сертификат открытого ключа, и которое владеет соответствующим закрытым ключом, позволяющим с помощью средств электронной подписи создавать свою Электронную подпись в Электронных документах (подписывать Электронные документы).

Закрытый ключ электронной подписи (закрытый ключ) – уникальная последовательность символов, сформированная средствами электронной подписи и предназначенная для создания электронной подписи.

Ключ электронной подписи действует на определенный момент времени если:

- наступил момент времени начала действия ключа электронной подписи;
- срок действия ключа электронной подписи не истек;
- сертификат открытого ключа электронной подписи, соответствующий данному ключу электронной подписи, не аннулирован.

Компрометация ключа – нарушение конфиденциальности закрытого ключа.

Область действия сертификата открытого ключа электронной подписи– включенные в сертификат открытого ключа электронной подписи сведения об отношениях, при которых электронный документ с электронной подписью, созданной с использованием соответствующего сертификата открытого ключа электронной подписи, будет иметь юридическое значение.

Обработка заявления на аннулирование сертификата – совокупность действий по занесению сведений об аннулировании сертификата открытого ключа электронной подписи в реестр сертификатов Удостоверяющего Центра и уведомлению владельца сертификата об аннулировании сертификата.

Открытый ключ электронной подписи (открытый ключ) – уникальная последовательность символов, сформированная средствами электронной подписи, однозначно связанная с закрытым ключом и предназначенная для проверки подлинности электронной подписи.

Пользователь Удостоверяющего Центра – физическое лицо, физическое лицо, являющееся индивидуальным предпринимателем, частный нотариус, а также юридическое лицо в лице своего уполномоченного представителя или соответствующего исполнительного органа, присоединившееся к Регламенту Удостоверяющего Центра и внесенное в реестр Удостоверяющего Центра.

Рабочий день Удостоверяющего Центра Банка (далее – рабочий день) – промежуток времени с 09:00 по 17:00 каждого дня недели за исключением выходных и праздничных дней.

Рассмотрение заявления на аннулирование действия сертификата – принятие Оператором УЦ решения об обработке заявления на аннулирование сертификата открытого ключа электронной подписи на основе предоставленных документов.

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

- реестр заявлений Пользователей о присоединении к Регламенту Удостоверяющего Центра;
- реестр зарегистрированных Пользователей Удостоверяющего Центра;
- реестр запросов на сертификат открытого ключа электронной подписи;
- реестр заявлений на аннулирование сертификата открытого ключа электронной подписи;

- реестр сертификатов открытых ключей электронной подписи;
- реестр изготовленных списков аннулированных сертификатов;
- реестр аннулированных сертификатов открытого ключа электронной подписи;
- служебные документы Удостоверяющего Центра.

Сертификат открытого ключа электронной подписи (Сертификат) - электронный документ с электронной подписью уполномоченного лица Удостоверяющего Центра, структура которого определяется настоящим Регламентом и который выдается Удостоверяющим Центром Пользователю для подтверждения подлинности электронной подписи и идентификации владельца сертификата открытого ключа электронной подписи. Сертификат открытого ключа электронной подписи является квалифицированным сертификатом.

Список аннулированных сертификатов (САС) – электронный документ с электронной подписью уполномоченного лица Удостоверяющего Центра, который содержит перечень сертификатов, являющихся аннулированными, с указанием серийного номера сертификата, даты и причины аннулирования. CRL используют информационные системы (ИС) для проверки подлинности сертификата Пользователя.

Средства электронной подписи – программные и (или) технические средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи.

Стороны настоящего договора- ЗАО «Агропромбанк» и Пользователь Удостоверяющего центра ЗАО «Агропромбанк».

Тарифы – внутренний документ Банка, устанавливающий вознаграждение за оказываемые услуги Пользователям Удостоверяющего Центра.

Токен – устройство в виде USB-флеш-накопителя с защищенной паролем картой памяти, являющееся носителем ключей, на котором хранится необходимая информация для создания электронной подписи. Токен обеспечивает двухфазную аутентификацию Пользователя.

Удостоверяющий Центр Банка (Удостоверяющий Центр, УЦ) - функциональное подразделение Банка, выполняющее следующие основные функции:

- изготавливает сертификаты открытых ключей электронной подписи;
- создает ключи электронных подписей с гарантией сохранения в тайне ключа электронной подписи;
- аннулирует сертификаты ключей электронной подписи;
- ведет реестр Удостоверяющего Центра, обеспечивает его актуальность;
- проверяет уникальность ключей электронной подписи;
- выдает сертификаты открытых ключей электронной подписи с информацией об их действии;
- осуществляет подтверждение подлинности электронной подписи в электронном документе
- осуществляет иные функции, предусмотренные действующим законодательством ПМР.

Уполномоченное лицо Удостоверяющего Центра (Оператор УЦ) – работник Банка, действующий в соответствии с внутренними документами Банка от имени Банка.

Электронный документ – информация, представленная в электронной форме, пригодная для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

Электронная подпись (ЭП) - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Public Key Cryptography Standards (PKCS) – стандарты криптографии с открытым ключом, разработанные компанией RSA Security. Удостоверяющий Центр осуществляют свою работу в соответствии со следующими стандартами PKCS:

- *PKCS#7* – стандарт, определяющий формат и синтаксис криптографических сообщений. Удостоверяющий центр использует описанный в PKCS#7 тип данных PKCS#7 signed – подписанные данные. Электронный документ, оформленный с соблюдением требований PKCS#7 signed, является электронным документом, содержащим электронную подпись;
- *PKCS#10* – стандарт, определяющий формат и синтаксис запроса на сертификат открытого ключа электронной подписи. Электронный документ, оформленный с соблюдением требований PKCS#10, содержит информацию о сертифицируемом ключе проверки электронной подписи, используемом криптографическом средстве и данные, необходимые для идентификации владельца сертифицируемого открытого ключа электронной подписи.

Internet Assigned Numbers Authority (IANA, ассоциация IANA) – международная организация, координирующая выделение объектных идентификаторов, предназначенных для идентификации телекоммуникационных объектов.

XAdES – XML Advanced Electronic Signatures (XAdES). Набор форматов усовершенствованной подписи документов XML. Спецификация размещена по адресу http://uri.etsi.org/01903/v1.3.2/ts_101903v010302p.pdf

2. Общие положения

2.1. Предмет Регламента

2.1.1. Настоящий Регламент Удостоверяющего Центра ЗАО «Агропромбанк» (далее - Регламент) определяет условия предоставления и правила пользования услугами Удостоверяющего Центра Банка, включая права, обязанности, ответственность Удостоверяющего Центра и Пользователей Удостоверяющего Центра, форматы данных, основные организационно-технические мероприятия, направленные на обеспечение работы Удостоверяющего Центра.

2.1.2. Данный Регламент не определяет и не рассматривает отношения между Удостоверяющим Центром и Пользователями Удостоверяющего Центра, являющимися работниками Банка при исполнении трудовых обязанностей. Данные отношения регламентируются внутренними документами Банка.

2.1.3. Настоящий Регламент является договором присоединения.

2.2. Действие Регламента

2.2.1. С момента регистрации Заявления о присоединении к Регламенту Удостоверяющего центра ЗАО «Агропромбанк» в Удостоверяющем центре лицо, подавшее Заявление, считается присоединившемся к Регламенту и является Стороной Регламента.

2.2.2. Удостоверяющий центр вправе отказать любому лицу в приёме и регистрации Заявления о присоединении к Регламенту Удостоверяющего центра ЗАО «Агропромбанк» без объяснения причин.

2.2.3. Стороны согласны с тем, что условия настоящего Регламента принимаются Пользователем полностью без каких-либо изъятий, изменений и протоколов разногласий.

2.2.4. Настоящий Регламент размещен в электронной форме по адресу – <http://ca.agroprombank.com/pki/policies.html>

2.2.5. Внесение изменений (дополнений) в Регламент, включая приложения к нему, производится Удостоверяющим Центром в одностороннем порядке.

2.2.6. Уведомление о внесении изменений или дополнений в Регламент и уточненная редакция Регламента размещаются на Internet странице Удостоверяющего Центра Банка, расположенной по адресу – <http://ca.agroprombank.com/pki/policies.html>

2.2.7. Все изменения (дополнения), вносимые Удостоверяющим Центром в Регламент по собственной инициативе, и не связанные с изменением действующего законодательства вступают в силу и становятся обязательными по истечении 10 рабочих дней с даты размещения новой редакции Регламента на сайте Удостоверяющего Центра по адресу – <http://ca.agroprombank.com/pki/policies.html>

2.2.8. Все изменения (дополнения), вносимые Удостоверяющим Центром в Регламент в связи с изменением действующего законодательства вступают в силу одновременно с вступлением в силу изменений (дополнений) в соответствующих нормативных актах.

2.2.9. 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.

2.2.10. В случае, если Пользователь Удостоверяющего Центра не согласен со внесенными изменениями и дополнениями он имеет право прекратить использование сертификата открытого ключа электронной подписи, в порядке, предусмотренном п.4.4.4 настоящего Регламента, при этом комиссионное вознаграждение, уплаченное Банку в соответствии с Тарифами, не возвращается.

3. Права и обязанности сторон

3.1. Права Удостоверяющего Центра

Удостоверяющий Центр имеет право:

3.1.1. Аннулировать сертификат открытого ключа электронной подписи Пользователя Удостоверяющего Центра в случае установленного факта компрометации соответствующего ключа электронной подписи, с уведомлением владельца аннулированного сертификата открытого ключа электронной подписи (а в случае, если сертификат выдан юридическому лицу – с уведомлением и владельца сертификата и юридического лица) и указанием обоснованных причин.

3.1.2. Отказать в изготовлении сертификата открытого ключа электронной подписи Пользователя в случае, если использованное Пользователем для формирования запроса на сертификат открытого ключа электронной подписи средство криптографической защиты информации не поддерживается Удостоверяющим Центром.

3.1.3. Пользоваться иными правами, предусмотренными действующим законодательством ПМР и настоящим Регламентом.

3.2. Права Пользователя Удостоверяющего Центра

Пользователь Удостоверяющего Центра имеет право:

3.2.1. Получить сертификат открытого ключа электронной подписи Удостоверяющего Центра в порядке, предусмотренном настоящим Регламентом.

3.2.2. Получить список аннулированных сертификатов, изготовленный Удостоверяющим Центром.

3.2.3. Применять сертификат открытого ключа электронной подписи Удостоверяющего Центра для проверки электронной подписи Удостоверяющего Центра в сертификатах, изготовленных Удостоверяющим Центром.

3.2.4. Применять сертификат открытого ключа электронной подписи Пользователя Удостоверяющего Центра для проверки электронной подписи электронных документов в соответствии со сведениями, указанными в сертификате открытого ключа электронной подписи.

3.2.5. Применять список аннулированных сертификатов, изготовленный Удостоверяющим Центром, для проверки статуса сертификатов открытых ключей электронной подписи.

3.2.6. Обратиться в Удостоверяющий центр за подтверждением подлинности электронных подписей в электронных документах.

3.2.7. Обратиться в Удостоверяющий центр за подтверждением подлинности электронных подписей Удостоверяющего Центра в изготовленных им сертификатах открытых ключей электронной подписи.

3.2.8. Сформировать ключ электронной подписи на своем рабочем месте с использованием средства криптографической защиты информации, предоставленной Удостоверяющим центром.

3.2.9. Для хранения закрытого ключа электронной подписи использовать любой носитель, поддерживаемый средством криптографической защиты информации.

3.2.10. Воспользоваться предоставляемыми Удостоверяющим центром программными средствами для передачи по линиям связи в Удостоверяющий Центр запроса на создание и выдачу сертификата открытого ключа электронной подписи в электронном виде.

3.2.11. Обратиться в Удостоверяющий центр для формирования сертификата открытого ключа электронной подписи с областями действия отличными от областей действия действующего сертификата Пользователя. Список возможных областей действия сертификата приведен в Приложении 2 «Области действия сертификатов открытых ключей электронной подписи».

3.2.12. Воспользоваться предоставляемыми Удостоверяющим центром программными средствами, чтобы получить и установить на свое рабочее место изготовленный Удостоверяющим Центром сертификат открытого ключа электронной подписи в электронном виде.

3.2.13. Обратиться в Удостоверяющий центр для аннулирования сертификата открытого ключа электронной подписи в течение срока действия соответствующего ключа электронной подписи.

3.2.14. Обратиться в Удостоверяющий центр за получением нового сертификата открытого ключа электронной подписи в течение срока действия Сертификата (при плановой смене ключа ЭП Пользователя).

3.2.15. Обратиться в Удостоверяющий центр за получением Токена для генерации и хранения открытого и закрытого ключа.

3.2.16. Пользоваться иными правами, предусмотренными действующим законодательством ПМР и настоящим Регламентом.

3.3. Обязанности Удостоверяющего Центра

Удостоверяющий Центр обязан:

3.3.1. Использовать Ключ электронной подписи Удостоверяющего Центра только для подписи издаваемых им сертификатов открытых ключей электронной подписи Пользователей Удостоверяющего Центра и списков аннулированных сертификатов.

3.3.2. Принять меры по защите ключа электронной подписи Удостоверяющего Центра от несанкционированного доступа.

3.3.3. Организовать свою работу по GMT (Greenwich Mean Time) с учетом часового пояса города г. Тирасполь. Удостоверяющий Центр обязан синхронизировать по времени все свои программные и технические средства обеспечения деятельности.

3.3.4. Обеспечить регистрацию Пользователей Удостоверяющего Центра в соответствии с порядком регистрации, изложенным в настоящем Регламенте. Удостоверяющий Центр обязан обеспечить уникальность регистрационной информации Пользователей Удостоверяющего Центра, используемой для идентификации владельцев сертификатов открытых ключей электронной подписи.

3.3.5. Изготовить сертификат открытого ключа электронной подписи зарегистрированного Пользователя в соответствии с порядком, определенным в настоящем Регламенте.

3.3.6. Обеспечить уникальность серийных номеров изготавливаемых сертификатов открытых ключей электронной подписи Пользователей Удостоверяющего Центра.

3.3.7. Обеспечить уникальность значений открытых ключей электронной подписи в изготовленных сертификатах открытых ключей электронной подписи Пользователей Удостоверяющего Центра.

3.3.8. Аннулировать сертификат открытого ключа электронной подписи по заявлению на аннулирование сертификата открытого ключа электронной подписи, не позднее рабочего дня, следующего за рабочим днем, в течение которого было подано заявление внести сведения об аннулированном сертификате в список аннулированных сертификатов с указанием даты и времени занесения и причины аннулирования.

3.3.9. Вести реестр Удостоверяющего Центра.

3.3.10. Исполнять поручения Пользователя о безакцептном списании денежных средств с его текущих счетов в случаях и порядке, установленных в Регламенте.

3.3.11. Отказать в аннулировании сертификата открытого ключа электронной подписи Пользователя Удостоверяющего Центра в случае, если истек установленный срок действия ключа электронной подписи, соответствующего этому сертификату.

3.3.12. Исполнять иные обязанности, предусмотренные действующим законодательством ПМР и настоящим Регламентом.

3.4. Обязанности Пользователя Удостоверяющего Центра

Пользователь Удостоверяющего центра обязан:

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

3.4.2. Не применять закрытый ключ электронной подписи, если Пользователю стало известно, что этот ключ использовался ранее другими лицами, используется или возможно будет использоваться другими лицами.

3.4.3. Применять закрытый ключ электронной подписи только в соответствии с областями действия, указанными в соответствующем данному ключу электронной подписи сертификате открытого ключа электронной подписи, если такие области действия установлены.

3.4.4. Немедленно обратиться в Удостоверяющий центр с заявлением на аннулирование сертификата открытого ключа электронной подписи в случае потери, раскрытия, искажения закрытого ключа электронной подписи, а также в случае если Пользователю стало известно, что этот ключ использовался ранее другими лицами, используется или возможно будет использоваться другими лицами.

3.4.5. Не использовать закрытый ключ электронной подписи, связанный с сертификатом открытого ключа электронной подписи, заявление на аннулирование которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на аннулирование сертификата в Удостоверяющий центр по момент времени официального уведомления Пользователя об аннулировании сертификата.

3.4.6. Не использовать закрытый ключ электронной подписи, связанный с сертификатом открытого ключа электронной подписи, который аннулирован.

3.4.7. Регулярно, не реже чем один раз в 10 дней, просматривать Internet страницу Удостоверяющего Центра Банка, расположенную по адресу <http://ca.agroprombank.com/pki/policies.html> на предмет изменения Регламента.

3.4.8. Оплачивать комиссионное вознаграждение за услуги, оказываемые Удостоверяющим Центром, в соответствии с Тарифами.

3.4.9. Обеспечить Банку возможность списания в безакцептном порядке с текущих счетов Пользователя денежные средства в соответствии с порядком, предусмотренным Регламентом, с целью оплаты услуг Удостоверяющего Центра.

3.4.10. Ежедневно просматривать изменения в реестре аннулированных сертификатов открытого ключа электронной подписи Удостоверяющего Центра, опубликованный в сети Интернет по адресу <http://ca.agroprombank.com/>.

3.4.11. Исполнять иные обязанности, предусмотренные действующим законодательством ПМР и настоящим Регламентом.

4. Правила пользования услугами Удостоверяющего Центра

4.1. Регистрация Пользователей

Порядок регистрации Пользователей в Удостоверяющем Центре изложен в приложениях к данному Регламенту, которые описывают процедуры регистрации

Пользователей, генерации ключей, управления сертификатами открытого ключа электронной подписи.

Временем подписания электронного документа, на основании которого была проведена регистрация Пользователя, считается время внесения документа в реестр Удостоверяющего Центра.

4.2. Генерация ключей

Порядок генерации ключей электронной подписи Пользователей Удостоверяющего Центра изложен в приложениях к данному Регламенту, которые описывают процедуры регистрации Пользователей, генерации ключей, управления сертификатами открытого ключа электронной подписи.

4.3. Изготовление и получение сертификата открытого ключа электронной подписи

Порядок изготовления и получения сертификатов открытого ключа электронной подписи Пользователей Удостоверяющего Центра изложен в приложениях к данному Регламенту, которые описывают процедуры регистрации Пользователей, генерации ключей, управления сертификатами открытого ключа электронной подписи.

Временем подписания электронного документа, на основании которого было проведено изготовление сертификата открытого ключа электронной подписи, считается время внесения документа в реестр Удостоверяющего Центра.

4.4. Аннулирование сертификата открытого ключа электронной подписи

4.4.1. Удостоверяющий Центр аннулирует сертификат открытого ключа электронной подписи Пользователя Удостоверяющего Центра в следующих случаях:

- по заявлению Пользователя Удостоверяющего Центра;
- по истечении срока его действия;
- при компрометации ключа электронной подписи уполномоченного лица Удостоверяющего Центра;
- при обнаружении недостоверности сведений, указанных в Заявлении на создание и выдачу сертификата открытого ключа электронной подписи или в сертификате открытого ключа;
- в связи со смертью или потерей дееспособности владельца сертификата открытого ключа, в связи с ликвидацией юридического лица, выданного такому юридическому лицу;
- по решению суда, вступившему в законную силу, в частности, если решением суда установлено, что сертификат открытого ключа содержит недостоверную информацию;
- в иных случаях, установленных действующим законодательством ПМР или настоящим Регламентом.

4.4.2. В случае аннулирования сертификата Пользователя Удостоверяющего Центра по истечении срока его действия временем аннулирования сертификата Пользователя Удостоверяющего Центра признается время, хранящееся в поле notAfter поля Validity сертификата. В данном случае информация об аннулированном сертификате Пользователя Удостоверяющего Центра в список аннулированных сертификатов не заносится.

4.4.3. В случае компрометации ключа электронной подписи Удостоверяющего Центра временем аннулирования сертификата 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 Пользователя Удостоверяющего Центра в список аннулированных сертификатов не заносится.

4.4.4. Аннулирование сертификата открытого ключа электронной подписи по заявлению Пользователя (отзыв Сертификата):

Для осуществления аннулирования сертификата открытого ключа электронной подписи Пользователь подает Заявление на аннулирование сертификата открытого ключа

электронной подписи в Удостоверяющий центр, составленное по форме, указанной в приложениях в Регламенте.

Аннулирование сертификата открытого ключа электронной подписи Пользователя Удостоверяющего Центра осуществляется Удостоверяющим Центром на основании заявления, поступающего в бумажной или в электронной форме, также в порядке, предусмотренном в Инструкции по работе с программой «АПБ: управление ключами», расположенной в сети Интернет по адресу <http://ca.agroprombank.com/>

Заявление на аннулирование сертификата открытого ключа электронной подписи в электронной форме представляет собой электронный документ формата XAdES-T. В качестве подписываемых данных используется запрос на аннулирование сертификата, а электронная подпись осуществляется на действующем ключе электронной подписи Пользователя.

Запрос на аннулирование сертификата представляет собой XML со следующими данными «SN»=CertificateSerialNumber, «RC»=ReasonCode, «SC»=SomeComment, где:

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

Заявление на аннулирование сертификата открытого ключа электронной подписи формируется и подается в электронном виде в Удостоверяющий центр с использованием программного обеспечения Удостоверяющего центра.

Подача заявления на аннулирование сертификата, оформленного в бумажном виде, в Удостоверяющий Центр и его рассмотрение осуществляется только в течение рабочего дня.

4.4.5. В случае аннулирования сертификата по заявлению Пользователя Удостоверяющий Центр должен официально уведомить Пользователя и всех лиц, зарегистрированных в Удостоверяющем Центре, об аннулировании сертификата не позднее одного рабочего дня с момента подачи заявления в Удостоверяющий Центр путем размещения соответствующей информации в реестре аннулированных сертификатов открытого ключа электронной подписи, опубликованный в сети Интернет по адресу <http://ca.agroprombank.com/>.

4.4.6. Официальным уведомлением о факте аннулирования сертификата подписи является опубликование первого (наиболее раннего) списка аннулированных сертификатов, содержащего сведения об аннулированном сертификате, и изданного не ранее времени наступления произошедшего случая. Временем аннулирования сертификата ключа подписи признается время издания указанного списка аннулированных сертификатов, хранящееся в поле thisUpdate списка аннулированных сертификатов.

4.4.7. Информация о размещении списка аннулированных сертификатов заносится в изданные Удостоверяющим Центром сертификаты в расширение САС.

4.5. Порядок оплаты комиссионного вознаграждения за оказываемые услуги

4.5.1 За услуги, оказываемые Удостоверяющим Центром, Пользователь уплачивает Банку комиссионное вознаграждение в порядке и в размере, указанном в

настоящем Регламенте и Тарифах. Комиссионное вознаграждение рассчитывается и уплачивается в валюте, указанной в Тарифах.

4.5.2 В случае наличия денежных средств на текущем счете Пользователя в валюте комиссионного вознаграждения, определенной в Тарифах, и наступлении срока уплаты комиссионного вознаграждения, Пользователь поручает Банку списывать в безакцептном порядке суммы комиссионного вознаграждения, подлежащие уплате с текущего счета Пользователя, открытом в Банке или в ином обслуживающем банке, в валюте комиссионного вознаграждения, определенной в Тарифах.

4.5.3 В случае недостаточности денежных средств для уплаты вышеуказанных сумм или отсутствия денежных средств на вышеуказанном текущем счете Пользователя, открытом в Банке или в ином обслуживающем банке, Пользователь поручает списывать в безакцептном порядке вышеуказанные суммы со всех своих текущих счетов, открытых в Банке или в ином обслуживающем банке. В таком случае пересчет суммы комиссионного вознаграждения в валюту списания производится по курсу, установленному Банком в соответствии с его внутренними документами.

При этом, если текущие счета Пользователя открыты в ином обслуживающем банке, Пользователь обеспечивает Банку возможность списания в безакцептном порядке суммы комиссионного вознаграждения путем предоставления в обслуживающий банк поручения (распоряжения), оформленного в соответствии с требованиями этого банка и действующего законодательства ПМР. Пользователь обязуется не отзываться предоставленные распоряжения из иных обслуживающих банков до окончания срока действия Регламента.

4.5.4 В случае невозможности списания денежных средств с текущих счетов Пользователя, Пользователь обязуется произвести перечисление Банку вышеуказанных сумм денежных средств в течение 5 (пяти) дней со дня возникновения обязанности их уплаты.

4.5.5 Между сторонами может быть заключено отдельное соглашение, регулирующее иной порядок оплаты комиссионного вознаграждения за оказываемые услуги.

4.6. Токены

4.6.1. Для создания открытого и закрытого ключей, создания ЭП, а также совершения иных действий в рамках возможностей Токена Пользователь может воспользоваться Токеном.

4.6.2. Удостоверяющий центр выдает Токен по запросу Пользователя.

В работе с Токеном Пользователь обязуется руководствоваться Инструкцией по работе с Токенами, размещенной по адресу <http://ca.agroprombank.com>

4.6.3. Удостоверяющий центр передает Токен Пользователю после оплаты комиссионного вознаграждения согласно Тарифам по акту приема-передачи.

При приеме Токена Пользователь обязан осмотреть Токен на предмет выявления видимых признаков повреждений, и при их наличии сообщить в Удостоверяющий центр.

4.6.4. Пользователь обязан хранить Токен в месте, недоступном для третьих лиц.

4.6.5. Запрещено передавать Токен третьим лицам, а также сообщать третьим лицам ПИН-код доступа к закрытому ключу ЭП. В случае если Токен или ПИН-код станут доступны третьим лицам Пользователь обязан обратиться в Удостоверяющий центр с заявлением на аннулирование сертификата открытого ключа электронной подписи в порядке, определенном в Регламенте.

4.6.6. Пользователь обязан использовать Токен на те цели, на которые он был выдан.

4.6.7. Удостоверяющий центр обязан безвозмездно заменить поврежденный Токен на аналогичный качественный Токен:

- если во время подписания Акта приема-передачи будет обнаружены повреждения Токена;
- если Токен перестанет по каким-либо причинам исполнять свои функции в течение 6 месяцев (гарантийный срок) со дня его получения Пользователем.

4.6.8. В случае если Пользователь получил Токен, но не осуществил все необходимые действия для получения Сертификата в течение 2 (двух) месяцев со дня подписания Акта приема-передачи Токена, Удостоверяющий центр не оказывает услуги по изготовлению Сертификата открытого ключа электронной подписи, сформированной с

использованием такого Токена в рамках прошлой оплаты, по истечении вышеуказанного срока.

При этом Удостоверяющий центр не возвращает Пользователю уплаченное комиссионное вознаграждение.

5. Прочие условия

5.1. Конфиденциальность

5.1.1. Типы конфиденциальной информации

Ключ электронной подписи, соответствующий сертификату открытого ключа электронной подписи Пользователя Удостоверяющего Центра, является конфиденциальной информацией данного Пользователя Удостоверяющего Центра. Удостоверяющий Центр не осуществляет хранение ключей электронной подписи Пользователей.

Информация о Пользователях Удостоверяющего Центра, хранящаяся в Удостоверяющем Центре и не подлежащая непосредственной рассылке в качестве части сертификата открытого ключа электронной подписи считается конфиденциальной.

5.1.2. Типы информации, не являющейся конфиденциальной

Информация, не являющаяся конфиденциальной информацией, считается открытой информацией.

Открытая информация может публиковаться по решению Удостоверяющего Центра. Место, способ и время публикации открытой информации определяется Удостоверяющим Центром.

Персональные данные, включаемые в сертификаты открытых ключей электронной подписи Пользователей Удостоверяющего Центра и списки аннулированных сертификатов, издаваемые Удостоверяющим Центром, относятся к общедоступным персональным данным и могут быть переданы третьим лицам в целях обеспечения работоспособности и информационной целостности инфраструктуры открытых ключей.

Обработка персональных данных Удостоверяющим Центром осуществляется в целях выдачи сертификата открытых ключей электронной подписи, выпуска списков аннулированных сертификатов и обеспечения работоспособности и информационной целостности инфраструктуры открытых ключей.

Информация, содержащаяся в настоящем Регламенте, не считается конфиденциальной.

5.1.3. Исключительные полномочия Удостоверяющего Центра

Удостоверяющий Центр имеет право раскрывать конфиденциальную информацию третьим лицам только в случаях, установленных законодательством Приднестровской Молдавской Республики.

5.2. Плановая смена ключей уполномоченного лица Удостоверяющего Центра

Плановая смена ключей (ключа электронной подписи и соответствующего ему открытого ключа электронной подписи) 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 формирует новый Ключ электронной подписи и соответствующий ему открытый Ключ электронной подписи;
- Уполномоченное лицо Удостоверяющего Центра изготавливает сертификат нового открытого ключа электронной подписи и подписывает его

электронной подписью с использованием нового ключа электронной подписи.

Старый Ключ электронной подписи Удостоверяющего Центра используется в течение своего срока действия для формирования списков аннулированных сертификатов в электронной форме, изданных Удостоверяющим Центром в период действия старого ключа электронной подписи Удостоверяющего Центра.

5.3. Компрометация ключа Удостоверяющего Центра

В случае компрометации или угрозы компрометации ключа электронной подписи Удостоверяющего Центра выполняется внеплановая смена ключей Удостоверяющего Центра.

Процедура внеплановой смены ключей Удостоверяющего Центра выполняется в порядке, определенном процедурой плановой смены ключей Удостоверяющего Центра.

В случае компрометации ключа Удостоверяющего Центра после выполнения процедуры внеплановой смены ключей, сертификат открытого ключа электронной подписи Удостоверяющего Центра аннулируется путем занесения в реестр аннулированных сертификатов лицом, выдавшим его Удостоверяющему Центру.

5.4. Компрометация ключа Пользователя Удостоверяющего Центра

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

В случае компрометации или угрозы компрометации ключа электронной подписи Пользователь подает в Удостоверяющий центр Заявление на аннулирование сертификата открытого ключа электронной подписи в соответствии с правилами, установленными в данном Регламенте.

5.5. Прекращение деятельности Удостоверяющего Центра

Прекращение деятельности Удостоверяющего Центра может быть осуществлено на основании решения Банка и в порядке, установленном внутренними документами Банка.

Все сертификаты открытого ключа электронной подписи Пользователей, выданные Удостоверяющим Центром, аннулируются.

5.6. Опубликование и оповещение

Удостоверяющий Центр обязан уведомить о факте аннулирования сертификата открытого ключа электронной подписи его владельца, а в случае выдачи сертификата юридическому лицу – уведомить и владельца сертификата и юридическое лицо.

Срок уведомления – не позднее рабочего дня, следующего за рабочим днем, в течение которого было подано заявление в Удостоверяющий Центр на аннулирование сертификата.

Официальным уведомлением о факте аннулирования сертификата является опубликование списка аннулированных сертификатов, содержащего сведения об аннулированном сертификате. Временем опубликования считается время издания списка аннулированных сертификатов, указанное в поле thisUpdate изданного списка аннулированных сертификатов.

Информация о размещении списка аннулированных сертификатов заносится в сертификат открытого ключа электронной подписи Пользователя Удостоверяющего Центра в поле CRL Distribution Point.

5.7. Сроки действия ключей уполномоченного лица 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 его генерации.

Срок действия сертификата открытого ключа электронной подписи, соответствующего ключу электронной подписи Удостоверяющего Центра, составляет 10 лет.

5.8. Сроки действия ключей Пользователей

Установленные сроки действия ключей электронной подписи и сертификатов открытого ключа электронной подписи приведены в приложении к данному Регламенту.

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

5.9. Хранение сертификатов открытого ключа электронной подписи в Удостоверяющем Центре

Срок хранения сертификата открытого ключа электронной подписи в Удостоверяющем Центре осуществляется в течение всего периода его действия и 5 лет после его аннулирования.

По истечении указанного срока хранения сертификаты открытого ключа электронной подписи переводятся в режим архивного хранения.

5.10. Структура сертификата открытого ключа электронной подписи и списков аннулированных сертификатов

Удостоверяющий Центр издает сертификаты открытых ключей электронной подписи Пользователей в электронной форме формата X.509 версии 3 и список отозванных сертификатов (САС) в электронной форме формата X.509 версии 2.

5.10.1. Структура сертификата открытого ключа электронной подписи Удостоверяющего Центра

Название	Описание	Содержание
Базовые поля сертификата		
Version	Версия	V3
Serial Number	Серийный номер	Уникальный серийный номера сертификата
Signature Algorithm	Алгоритм подписи	Алгоритм подписи Удостоверяющего Центра, соответствующий требованиям Регламента
Issuer	Издатель сертификата	CN = APB Root Certification Authority O = Agroprombank CJSC C = MD
Validity Period	Срок действия сертификата	Действителен с: дд.мм.гггг чч:мм:сс GMT Действителен по: дд.мм.гггг чч:мм:сс GMT

Subject	Владелец сертификата	CN = APB External CA O = Agroprombank CJSC C = MD
Public Key	Ключ проверки электронной подписи	Ключ проверки электронной подписи (Алгоритм подписи Удостоверяющего Центра, соответствующий требованиям Регламента)
Issuer Signature Algorithm	Алгоритм подписи издателя сертификата	Алгоритм подписи Удостоверяющего Центра, соответствующий требованиям Регламента
Issuer Sign	ЭП издателя сертификата	Подпись издателя в соответствии с sha256 RSA
Дополнения сертификата		
Key Usage (critical)	Использование ключа 2.5.29.15	Неотрекаемость – невозможность осуществления отказа от совершенных действий; Подписывание сертификатов, Автономное подписание списка отзыва (CRL), Подписание списка отзыва (CRL) – сведения об отношениях, при осуществлении которых электронный документ с электронной подписью будет иметь юридическое значение
Subject Key Identifier	Идентификатор ключа владельца сертификата 2.5.29.14	Идентификатор ключа электронной подписи Удостоверяющего Центра, соответствующего данному сертификату
Certificate Policies	Политики сертификата 2.5.29.32	[1] Политика сертификата: Идентификатор политики=1.3.6.1.4.1.50561.1.1 Agroprombank CPS, Класс средства УЦ КС1 [2] Размещение CPS: http://ca.agroprombank.com/pki/policies.html
BasicConstraints	Основные ограничения	SubjectType (Тип владельца сертификата) =CA Path Length Constraint (Ограничение на длину пути – ограничивает количество уровней иерархии при создании подчиненных Удостоверяющих Центров)=0
SzOID_CertSrv_CA_Version	Объектный идентификатор сертификата	Версия сертификата уполномоченного лица Удостоверяющего Центра
Thumbprint Algorithm	Алгоритм хэш-функции сертификата	sha1
Thumbprint	Значение хэш-функции сертификата	Значение хэш-функции сертификата в соответствии с алгоритмом sha1

5.10.2. Структура списка аннулированных сертификатов Удостоверяющего Центра

Название	Описание	Содержание
Базовые поля списка отозванных сертификатов		

Version	Версия	V2
Issuer	Издатель CAC	CN = APB External CA O = Agroprombank CJSC C = MD
thisUpdate	Время издания CAC	дд.мм.гггг чч:мм:сс GMT
nextUpdate	Время, по которое действителен CAC	дд.мм.гггг чч:мм:сс GMT
revokedCertificates	Список отозванных сертификатов	Последовательность элементов следующего вида .1.1.1. Серийный номер сертификата (CertificateSerialNumber) .1.1.2. Время обработки заявления на аннулирование (отзыв) и приостановление действия сертификата (Time)
signatureAlgorithm	Алгоритм подписи	Алгоритм подписи уполномоченного лица Удостоверяющего Центра, соответствующий требованиям Регламента
Issuer Sign	Подпись издателя CAC	Подпись издателя в соответствии с sha256
Расширения списка отозванных сертификатов		
Reason Code	Код причины аннулирования сертификата	"0" Не указана "1" Компрометация ключа "2" Компрометация ключа электронной подписи уполномоченного лица Удостоверяющего Центра "3" Изменение принадлежности "4" Сертификат заменен "5" Прекращение работы
Authority Key Identifier	Идентификатор ключа издателя	Идентификатор ключа электронной подписи уполномоченного лица Удостоверяющего Центра, на котором подписан CAC
SzOID_CertSrv_CA_Version	Объектный идентификатор сертификата издателя	Версия сертификата уполномоченного лица Удостоверяющего Центра

5.10.3. Структура сертификата открытого ключа электронной подписи Пользователя Удостоверяющего Центра

Структура сертификата открытого ключа электронной подписи Пользователя Удостоверяющего Центра в конкретной Бизнес-системе Банка приведена в приложении к данному Регламенту, описывающему процедуры управления сертификатами в этой Бизнес-системе.

6. Разрешение споров

6.1. При возникновении споров, стороны предпринимают все необходимые шаги для урегулирования спорных вопросов, которые могут возникнуть в рамках настоящего Регламента, путем переговоров.

7. Риски, связанные с использованием электронной подписи

При использовании ЭП Пользователь должен учитывать, возникновение следующих явных рисков:

- 7.1. Риски, связанные с несоответствием условий использования электронной подписи установленному порядку. В случае использования электронной подписи в порядке, не соответствующем требованиям законодательства или соглашений между участниками электронного взаимодействия, юридическая сила подписанных в данном случае документов может быть поставлена под сомнение.
- 7.2. Риски, связанные с компрометацией ключа ЭП или несанкционированного доступа к средствам ЭП. В данном случае может быть получен документ, порождающий юридически значимые последствия и исходящий от имени Пользователя, ключ которого был скомпрометирован.

8. Ответственность сторон

- 8.1. Удостоверяющий Центр не несет ответственность за неисполнение либо ненадлежащее исполнение своих обязанностей по настоящему Регламенту, а также возникшие в связи с этим убытки в случаях:
 - подделки, подлога либо иного искажения присоединившейся Стороной, Владелец Сертификата либо третьими лицами информации, содержащейся в заявлениях либо иных документах, представленных в Удостоверяющий центр;
 - если Пользователь не исполняет или ненадлежащим образом исполняет свои обязанности, что делает невозможным исполнение Удостоверяющим центром своих обязанностей;
 - если Пользователь своевременно не осуществил процедуру по аннулированию Сертификата при компрометации Ключа электронной подписи.
- 8.2. Удостоверяющий Центр несет ответственность за убытки, возникшие вследствие компрометации Ключа электронной подписи уполномоченного лица Удостоверяющего Центра, либо вследствие несоответствия сведений в Сертификате сведениям, указанным в заявлении на выдачу Сертификата.
- 8.3. Ответственность Удостоверяющего Центра регулируется законодательством Приднестровской Молдавской Республики.

9. Реквизиты УЦ

Закрытое акционерное общество «Агропромбанк», зарегистрировано на территории Приднестровской Молдавской Республики, г. Тирасполь.
Свидетельство о регистрации 0006092 АА, дата регистрации 25.12.2003г., регистрационный номер 01-022-3330.
Удостоверяющий центр ЗАО «Агропромбанк» аккредитован Государственной службой связи ПМР (Свидетельство об аккредитации удостоверяющего центра, регистрационный номер № 1 от 28.12.2018 года).

Полное наименование: Закрытое акционерное общество «Агропромбанк»
Сокращенное наименование: ЗАО «Агропромбанк»

Место нахождения: ПМР, г. Тирасполь, ул. Ленина, 44
Почтовый адрес: ПМР, г. Тирасполь, ул. Ленина, 44

Адрес электронной почты: [http://ca@agroprombank.com](mailto:ca@agroprombank.com)
Адрес в сети Интернет: <http://ca.agroprombank.com>

Приложение № 1а
к Регламенту Удостоверяющего центра ЗАО «Агропромбанк»

Для юридических лиц

Заявление о присоединении к Регламенту
Удостоверяющего центра ЗАО «Агропромбанк»

_____ (наименование юридического лица), в лице
_____ (должность, Ф.И.О. уполномоченного лица),
действующего на основании _____ (наименование и дата документа)
полностью и безусловно присоединяется к Регламенту Удостоверяющего центра ЗАО
«Агропромбанк», условия которого определены ЗАО «Агропромбанк» и опубликованы на
сайте Удостоверяющего центра ЗАО «Агропромбанк» по адресу
<http://ca.agroprombank.com/pki/policies.html>

С Регламентом Удостоверяющего центра ЗАО «Агропромбанк» и приложениями к
нему ознакомлен, согласен и обязуюсь соблюдать все положения указанного документа.

Заявитель:

_____ (наименование юридического лица)

_____ (должность)

_____/_____

(подпись) (фамилия, имя, отчество)

М.П.

Удостоверяющий центр ЗАО «Агропромбанк»

Адрес: MD-3300. Г. Тирасполь, ул. Ленина 44

Данное Заявление о присоединении к Регламенту Удостоверяющего центра ЗАО
«Агропромбанк» зарегистрировано в реестре Удостоверяющего центра.

Регистрационный № _____ от ____ . ____ .20 ____ г.

Уполномоченное лицо:

_____/_____
(подпись) (фамилия, имя, отчество)
М.П.

«Агропромбанк»

Для физических лиц/
индивидуальных предпринимателей/
частых нотариусов

**Заявление о присоединении к Регламенту
Удостоверяющего центра ЗАО «Агропромбанк»**

Я, _____ (ФИО), _____ (наименование документа удостоверяющего личность, серия, номер, дата выдачи, кем выдан)/

Я, Индивидуальный предприниматель _____ (ФИО), действующий на основании _____ (наименование документа, серия, номер, дата выдачи)/

Я, Частный нотариус _____ (ФИО), действующий на основании _____ (наименование документа, серия, номер, дата выдачи),

полностью и безусловно присоединяюсь к Регламенту Удостоверяющего центра ЗАО «Агропромбанк», условия которого определены ЗАО «Агропромбанк» и опубликованы на сайте Удостоверяющего центра ЗАО «Агропромбанк» по адресу <http://ca.agroprombank.com/pki/policies.html>

С Регламентом Удостоверяющего центра ЗАО «Агропромбанк» и приложениями к нему ознакомлен, согласен и обязуюсь соблюдать все положения указанного документа.

Заявитель: _____ / _____
(подпись) (фамилия, имя, отчество)

Удостоверяющий центр ЗАО «Агропромбанк»
Адрес: MD-3300. Г. Тирасполь, ул. Ленина 44

Данное Заявление о присоединении к Регламенту Удостоверяющего центра ЗАО «Агропромбанк» зарегистрировано в реестре Удостоверяющего центра.

Регистрационный № _____ от ____ . ____ .20 ____ г.

Уполномоченное лицо: _____ / _____
(подпись) (фамилия, имя, отчество)
М.П.

«Агропромбанк»

к Регламенту Удостоверяющего центра ЗАО

Приложение № 1 в

Для юридических лиц

Заявление

Я,

_____'
(Ф.И.О., документ удостоверяющий личность, его серия и номер, кем и когда
выдан)

являясь, _____ уполномоченным
представителем _____ (наименование юридического лица), и
получая Сертификат на основании письма № _____ от _____ г.

понимаю и соглашаюсь с тем, что в случаях:

- обнаружения недостоверности сведений, указанных в настоящем Заявлении или в Сертификате;

- нарушения конфиденциальности закрытого ключа (компрометация закрытого ключа),

а также в иных случаях, установленных действующим законодательством Приднестровской Молдавской Республики и Регламентом Удостоверяющего центра ЗАО «Агропромбанк»,

выданный Сертификат может быть аннулирован Удостоверяющим центром ЗАО «Агропромбанк».

Владелец Сертификата:

_____/_____
(подпись) (фамилия, имя, отчество)

Принято:

Удостоверяющий центр ЗАО «Агропромбанк»

Адрес: MD-3300. Г. Тирасполь, ул. Ленина 44

Уполномоченное лицо: _____/
(подпись) (фамилия, имя, отчество)
М.П.

«Агропромбанк»

к Регламенту Удостоверяющего центра ЗАО

Приложение №1г

Для физических лиц/
индивидуальных предпринимателей/
частых нотариусов

**Заявление
на создание и выдачу сертификата открытого
ключа электронной подписи № ____**

Место QR кода

г. Тирасполь

« ____ » _____ 20__ г.

Я, нижеподписавшийся _____ (ФИО), _____ (наименование документа удостоверяющего личность, серия, номер, дата выдачи, кем выдан),

Я, нижеподписавшийся _____ Индивидуальный предприниматель (ФИО), действующий на основании _____ (наименование документа, серия, номер, дата выдачи)/

Я, нижеподписавшийся Частный нотариус _____ (ФИО), действующий на основании _____ (наименование документа, серия, номер, дата выдачи),

прошу создать и выдать мне сертификат открытого ключа электронной подписи (далее –« Сертификат») со следующими данными:

Идентификатор открытого ключа

_____ Область действия Сертификата

OID	Название	Значение
1.3.6.1.4.1.50561.5.1.1	Сертификат Пользователя	

Я, заявляю, что любые действия, которые будут мной совершены на основании

этого Сертификата, являются действиями, совершаемыми от моего имени.

Я понимаю и соглашаюсь с тем, что в случаях:

- обнаружения недостоверности сведений, указанных в настоящем Заявлении или в Сертификате;

- нарушения конфиденциальности закрытого ключа (компрометация закрытого ключа),

а также в иных случаях, установленных действующим законодательством Приднестровской Молдавской Республики и Регламентом Удостоверяющего центра ЗАО «Агропромбанк»,

выданный мне Сертификат может быть аннулирован Удостоверяющим центром ЗАО «Агропромбанк».

Заявитель: _____ / _____
(подпись) (фамилия, имя, отчество)

Принято:

Удостоверяющий центр ЗАО «Агропромбанк»

Адрес: MD-3300. Г. Тирасполь, ул. Ленина 44

Уполномоченное лицо: _____ / _____
(подпись) (фамилия, имя, отчество)
М.П.

«Агропромбанк» к Регламенту Удостоверяющего центра ЗАО Приложение №1д

Для юридических лиц

**Заявление
на аннулирование сертификата открытого ключа электронной подписи**

Место QR кода

г. Тирасполь

« ____ » _____ 20__ г.

_____ (наименование юридического лица), в лице
_____ (должность, Ф.И.О. уполномоченного лица),
действующего на основании _____ (наименование и дата документа)
просит аннулировать Сертификат открытого ключа электронной подписи (далее –
«Сертификат»), выданный _____ (наименование юридического лица) в
Удостоверяющем центре ЗАО «Агропромбанк», владельцем которого является
_____ (Ф.И.О., документ удостоверяющий личность, его серия и номер, кем и когда
выдан)

Данные Сертификата:

Идентификатор открытого ключа

Серийный номер сертификата

В СВЯЗИ С _____

(причина аннулирования Сертификата)

Заявитель:

_____ (наименование юридического лица)

_____ (должность)
_____/_____
(подпись) (фамилия, имя, отчество)

М.П.

Принято:

Удостоверяющий центр ЗАО «Агропромбанк»
Адрес: MD-3300. Г. Тирасполь, ул. Ленина 44

Уполномоченное лицо: _____/_____
(подпись) (фамилия, имя, отчество)
М.П.

«Агропромбанк» к Регламенту Удостоверяющего центра ЗАО
Приложение № 1е

Для юридических лиц

**Заявление
на аннулирование сертификата открытого ключа электронной подписи**

Место QR кода

г. Тирасполь

« ___ » _____ 20__ г.

Я, _____ (ФИО), _____,
(наименование документа удостоверяющего личность, серия, номер, дата выдачи, кем
выдан)

являющийся владельцем Сертификата открытого ключа электронной подписи
(далее – «Сертификат»), выданного _____ (наименование юридического
лица) в Удостоверяющем центре ЗАО «Агропромбанк», прошу аннулировать Сертификат.

Данные Сертификата:

Идентификатор ключа

Серийный номер сертификата

В СВЯЗИ С _____

(причина аннулирования Сертификата)

Владелец Сертификата: _____/_____
(подпись) (фамилия, имя, отчество)

Принято:

Удостоверяющий центр ЗАО «Агропромбанк»

Адрес: MD-3300. Г. Тирасполь, ул. Ленина 44

Уполномоченное лицо:

_____/_____
(подпись) (фамилия, имя, отчество)
М.П.

«Агропромбанк» к Регламенту Удостоверяющего центра ЗАО
Приложение №1ж

*Для физических лиц/
индивидуальных предпринимателей/
частых нотариусов*

**Заявление
на аннулирование сертификата открытого ключа электронной подписи**

Место QR кода

г. Тирасполь

« ___ » _____ 20__ г.

Я, _____ (ФИО), _____ (наименование документа
удостоверяющего личность, серия, номер, дата выдачи, кем выдан),

Я, _____ (ФИО), _____ (наименование документа, серия, номер, дата выдачи) /
нижеподписавшийся Индивидуальный предприниматель
_____ (ФИО), действующий на основании _____

Я, нижеподписавшийся Частный нотариус _____ (ФИО),
действующий на основании _____ (наименование документа, серия,
номер, дата выдачи),

прошу аннулировать выданный мне в Удостоверяющем центре ЗАО
«Агропромбанк» Сертификат открытого ключа электронной подписи (далее –
«Сертификат»).

Данные Сертификата:

Идентификатор открытого ключа

Серийный номер сертификата

В СВЯЗИ С _____

(причина аннулирования Сертификата)

Владелец Сертификата:

_____/_____
(подпись) (фамилия, имя, отчество)

Принято:

Удостоверяющий центр ЗАО «Агропромбанк»

Адрес: MD-3300. Г. Тирасполь, ул. Ленина 44

Уполномоченное лицо: _____/_____
(подпись) (фамилия, имя, отчество)

М.П.

Приложение №2
к Регламенту Удостоверяющего центра ЗАО «Агропромбанк»

Области действия сертификатов открытых ключей электронной подписи

1. Принципы построения объектных идентификаторов областей применения сертификатов открытых ключей электронной подписи Пользователей Удостоверяющего Центра ЗАО «Агропромбанк» (OID).

В международной ассоциации IANA за ЗАО «Агропромбанк» зарегистрировано значение 1.3.6.1.4.1.50561.

В качестве корневого объектного идентификатора для построения структуры идентификаторов областей применения сертификатов открытых ключей электронной подписи Удостоверяющим Центром Банка используется значение, зарегистрированное в международной ассоциации IANA.

Структура объектных идентификаторов областей применения сертификатов открытых ключей электронной подписи Пользователей Удостоверяющего Центра Банка имеет вид:

1.3.6.1.4.1.50561.X.YY, где:

- X – Бизнес-система, обозначаемая одним из следующих числовых значений:
 - 1 – Системный раздел
 - 2 – Процессинг и Пластиковые карты
 - 3 – Система продажи билетов
 - 4 – Дистанционное банковское обслуживание
 - 5 – Сертификаты ЭП физических и юридических лиц
 - 6 – Система «Платежный шлюз»
 - 7 – Корпоративная информационная система
- YY – область действия сертификата, приведенная в п.2. настоящего приложения:

- Области применения сертификатов Удостоверяющего Центра Банка
 - Технологические объекты сертификатов ключей проверки электронной подписи (принадлежат Государственной службе связи)

Объектный идентификатор (OID)	Название
1.3.6.1.4.1.52072.1.1	Идентификатор физического лица
1.3.6.1.4.1.52072.1.2	Регистрационный номер юридического лица/ Регистрационный номер Индивидуального предпринимателя/частного нотариуса
1.3.6.1.4.1.52072.1.3	Сертификат государственной структуры
1.3.6.1.4.1.52072.2.1	Сертификат оператора фискальных данных
1.3.6.1.4.1.52072.2.2	Сертификат кассы ОФД

- Области применения сертификатов, относящиеся к Бизнес-системам Банка:

2.

OID	Название	Область действия
1.3.6.1.4.1.50561.1	Системный раздел	
1.3.6.1.4.1.50561.1.1	Политики сертификатов CPS	Ссылка на опубликованные политики выдачи сертификатов центром сертификации ЗАО «Агропромбанк»
1.3.6.1.4.1.50561.1.2	Политики сервера штампов времени	
1.3.6.1.4.1.50561.1.2.1	RSA 2048	Алгоритм подписи штампа времени
1.3.6.1.4.1.50561.2	Процессинг и Пластиковые карты	
1.3.6.1.4.1.50561.2.1	Система E-Commerce	
1.3.6.1.4.1.50561.2.1.1	Сертификат сервера системы E-Commerce	Расширение сертификата для работы с электронной подписью ответов сервера E-Commerce
1.3.6.1.4.1.50561.2.1.2	Сертификат E-Commerce терминала	Расширение сертификата для работы с подписью транзакций или запросов терминала.
1.3.6.1.4.1.50561.2.2	Система Loyalty	
1.3.6.1.4.1.50561.2.2.1	Сертификат сервера системы Loyalty	Расширение сертификата для работы с электронной подписью запросов на авторизацию или ответов сервера системы Loyalty

1.3.6.1.4.1.50561.2.2.2	Сертификат сервера эмитента	Расширение сертификата для работы с электронной подписью ответов сервера эмитента
1.3.6.1.4.1.50561.2.2.3	Сертификаты оператора	Расширение сертификата для работы с подписью запросов оператора к серверу эмитента
1.3.6.1.4.1.50561.2.3	Система выдачи карт по агентской схеме	
1.3.6.1.4.1.50561.2.3.1	Сертификат сервера системы выдачи карт по агентской схеме	Расширение сертификата для работы с подписью ответов системы выдачи карт по агентской схеме
1.3.6.1.4.1.50561.2.3.2	Сертификат оператора системы выдачи карт по агентской схеме	Сертификат оператора для подписи запросов на удаленную выдачу карты
1.3.6.1.4.1.50561.3		
1.3.6.1.4.1.50561.3.1	Система приема платежей при продаже билетов клиентами (далее – «система продажи билетов»)	
1.3.6.1.4.1.50561.3.1.1	Сертификат сервера системы	Расширение сертификата для работы с электронной подписью ответов сервера системы продажи билетов
1.3.6.1.4.1.50561.3.1.2	Сертификат терминала	Расширение сертификата для работы с электронной подписью информационных и транзакционных запросов терминала
1.3.6.1.4.1.50561.3.1.3	Сертификат администратора	Сертификат администратора системы, для доступа к настройке и изменению параметров мероприятий
1.3.6.1.4.1.50561.3.1.4	Сертификат оператора продажи	Расширение сертификата для работы с билетной системой. Сертификат оператора системы продажи билетов
1.3.6.1.4.1.50561.4	Дистанционное банковское обслуживание	
1.3.6.1.4.1.50561.4.1	Система клиент-банк	
1.3.6.1.4.1.50561.4.1.1	Сертификат сервера системы	Расширение сертификата для работы с подписью электронных документов от имени системы «Клиент-банк»
1.3.6.1.4.1.50561.4.1.2	Сертификат Пользователя	Расширение сертификата для работы с подписью электронных запросов, необходимых для функционирования системы. Не может использоваться для подписи документов от имени Пользователя системы.
1.3.6.1.4.1.50561.5	Сертификаты Пользователей	
1.3.6.1.4.1.50561.5.1	Сертификат клиента банка	

1.3.6.1.4.1.50561.5.1.1	Сертификат Пользователя	Расширение сертификата для идентификации клиента либо подписи финансовых электронных документов. Область действия Сертификата устанавливается на основании заявлений Пользователей
1.3.6.1.4.1.50561.6	Платежный шлюз	
1.3.6.1.4.1.50561.6.1	Платежный шлюз	
1.3.6.1.4.1.50561.6.1.1	Сертификат платежного сервиса	Расширение сертификата использоваться только для подписи информационных и транзакционных запросов к платежному шлюзу. Обязательно наличие в поле Subject объекта OID.2.5.4.13 (Description) с указанием наименования платежного шлюза

Сертификаты ЭП физических и юридических лиц

1. Генерация ключевой информации

Пользователь на своем рабочем месте осуществляет генерацию ключевой информации на ключевом носителе, формирует запрос на изготовление сертификата открытого ключа электронной подписи в формате PKCS#10 и отправляет запрос на изготовление сертификата открытого ключа электронной подписи в систему Банка.

Одновременно Пользователь передает пакет документов на бумажном носителе, подтверждающий достоверность данных, представленных в запросе на изготовление сертификата открытого ключа электронной подписи. Владелец сертификата вместе с собственноручно подписанным Заявлением на создание и выдачу сертификата открытого ключа электронной подписи подлежит обязательному фотографированию Оператором УЦ.

Если Пользователем является юридическое лицо, заявление на создание и выдачу сертификата оформляется в письменной произвольной форме, подписывается уполномоченным лицом Пользователя и скрепляется печатью Пользователя, с обязательным указанием следующей информации:

- фамилия, имя и отчество, уполномоченного представителя, который будет являться Владельцем сертификата;
- документ, удостоверяющий личность будущего Владельца сертификата (его серия, номер, когда и кем выдан);
- данные Сертификата (идентификатор открытого ключа, область действия Сертификата).

После получения вышеуказанного письма Удостоверяющим Центром Владелец сертификата вместе с собственноручно подписанным Заявлением (Приложение № 1в) подлежит обязательному фотографированию Оператором УЦ.

После успешной проверки документов Пользователя в системе Банка Оператор УЦ формирует и отправляет запрос на регистрацию и электронный запрос на изготовление сертификата открытого ключа электронной подписи в Удостоверяющий Центр.

Пользователь регистрируется в Удостоверяющем Центре на основании данных, полученных от системы Банка.

2. Генерация ключей электронной подписи Пользователей

Генерация ключа электронной подписи Пользователя осуществляется в следующих случаях:

- при формировании первого ключа электронной подписи Пользователя;
- при плановой смене ключа электронной подписи Пользователя.

Пользователь с помощью средства криптографической защиты информации генерирует Ключ электронной подписи и формирует на ключевом носителе контейнер ключа электронной подписи.

Пользователь имеет право сформировать контейнер ключа электронной подписи на любом носителе, поддерживаемом используемым средством криптографической защиты информации.

3. Изготовление и получение сертификата открытого ключа электронной подписи Пользователя

Изготовление сертификата открытого ключа электронной подписи Пользователя Удостоверяющего Центра производится на основании собственноручно подписанного заявления Пользователя, содержащего сведения, необходимые для идентификации Владельца сертификата открытого ключа электронной подписи. Система осуществляет проверку достоверности сведений, содержащихся в заявлении на изготовление сертификата открытого ключа электронной подписи и хранение указанных заявлений, оформленных на бумажном носителе.

Формирование сертификата открытого ключа электронной подписи Пользователя осуществляется Удостоверяющим Центром на основании заявления на создание и выдачу сертификата открытого ключа электронной подписи, которое направляется в электронном виде с использованием программного обеспечения Удостоверяющего центра.

Заявление на создание и выдачу сертификата открытого ключа электронной подписи, направляемое впервые в Удостоверяющий центр, в электронной форме представляет собой электронный документ формата XML. В качестве данных используется запрос на изготовление сертификата открытого ключа электронной подписи в формате PKCS#10.

Запрос на создание сертификата открытого ключа электронной подписи Пользователя при плановой смене сертификата ключа электронной подписи в электронной форме при обращении Пользователя за перевыпуском сертификата представляет собой электронный документ формата XADES. В качестве подписываемых данных используется запрос на изготовление сертификата открытого ключа электронной подписи в формате PKCS#10, а электронная подпись осуществляется на действующем ключе электронной подписи Пользователя.

Удостоверяющий Центр осуществляет создание сертификата открытого ключа электронной подписи в виде электронного документа в соответствии с поступившим запросом.

При плановой смене сертификата ключа электронной подписи значения полей Subject, Key Usage, Extended Key Usage изготовленного сертификата идентичны значениям этих полей в сертификате, который подвергся смене.

Срок создания сертификата открытого ключа электронной подписи не превышает 3 рабочих дней с момента поступления электронного запроса на создание сертификата в Удостоверяющий Центр.

Сертификат открытого ключа электронной подписи направляется его владельцу по электронной почте на адрес, указанный в запросе на создание сертификата.

4. Формирование и передача заявления на аннулирование сертификата открытого ключа электронной подписи в электронной форме

Заявление на аннулирование сертификата открытого ключа электронной подписи формируется и направляется в электронном виде в Удостоверяющий Центр с использованием программного обеспечения Бизнес-системы.

Заявление на аннулирование сертификата открытого ключа электронной подписи в электронной форме представляет собой электронный документ формата XADES. В качестве подписываемых данных используется запрос на аннулирование сертификата, а электронная подпись осуществляется в соответствии с установленным порядком на действующем ключе электронной подписи Пользователя, либо на ключе электронной подписи уполномоченного лица ЗАО "Агропромбанк".

Запрос на аннулирование сертификата открытого ключа электронной подписи представляет собой строку формата «SN=CertificateSerialNumber, RC=ReasonCode, SC=SomeComment», где:

- CertificateSerialNumber - серийный номер аннулируемого сертификата открытого ключа электронной подписи;
- ReasonCode - код причины аннулирования сертификата из следующего перечня допустимых значений:
 - "0" Не указана
 - "1" Компрометация ключа
 - "2" Компрометация ключа электронной подписи Удостоверяющего Центра
 - "3" Изменение принадлежности
 - "4" Сертификат заменен
 - "5" Прекращение работы
- SomeComment - текстовое значение комментария Пользователя сертификата открытого ключа электронной подписи.

5. Сроки действия ключей электронной подписи и сертификатов открытого ключа электронной подписи Пользователей

Срок действия ключа электронной подписи и сертификата открытого ключа электронной подписи Пользователя Удостоверяющего Центра – 1 год.

Название	Описание	Содержание
Базовые поля сертификата открытого ключа электронной подписи		
Version	Версия	V3
Serial Number	Серийный номер	Уникальный серийный номер сертификата открытого ключа электронной подписи
Signature Algorithm	Алгоритм подписи	Алгоритм подписи уполномоченного лица Удостоверяющего Центра, соответствующий требованиям Регламента
Issuer	Издатель сертификата	CN = APB External CA O = Agroprombank CJSC C = MD
Validity Period	Срок действия сертификата	Действителен с: дд.мм.гггг чч:мм:сс GMT Действителен по: дд.мм.гггг чч:мм:сс GMT
Subject	Владелец сертификата	CN = Общее имя = Фамилия, Имя, Отчество OU = Подразделение владельца сертификата открытого ключа электронной подписи O = Организация владельца сертификата открытого ключа электронной подписи L = Город владельца сертификата открытого ключа электронной подписи C = Страна/Регион владельца сертификата открытого ключа электронной подписи E = Электронная почта владельца сертификата открытого ключа электронной подписи
Public Key:	Открытый ключ электронной подписи	Открытый ключ электронной подписи (Алгоритм подписи Удостоверяющего Центра, соответствующий требованиям Регламента)
Issuer Signature Algorithm	Алгоритм подписи издателя сертификата	Алгоритм подписи Удостоверяющего Центра, соответствующий требованиям Регламента
Issuer Sign	ЭП издателя сертификата	sha256 RSA
Дополнения сертификата открытого ключа электронной подписи		
Certificate Policies	Политики сертификата 2.5.29.32	[1] Политика сертификата: Идентификатор политики=1.3.6.1.4.1.50561.1.1 Agroprombank CPS, Класс средства УЦ КС1 [2] Размещение CPS: http://ca.agroprombank.com/pki/policies.html
Key Usage (critical)	Использование ключа 2.5.29.15	Неотрекаемость - невозможность осуществления отказа от совершенных действий; Подпись, Шифрование ключей, Шифрование данных

Extended Key Usage	Улучшенный ключ 2.5.29.37	Набор идентификаторов (OID), определяющий отношения, при осуществлении которых электронный документ с электронной подписью будет иметь юридическое значение ¹
Subject Key Identifier	Идентификатор ключа владельца сертификата 2.5.29.14	Идентификатор ключа электронной подписи владельца сертификата
Authority Key Identifier	Идентификатор ключа издателя сертификата 2.5.29.35	Идентификатор ключа электронной подписи Удостоверяющего Центра
CRL Distribution Point	Точка распределения списка отозванных сертификатов (CRL) 2.5.29.31	http://ca.agroprombank.com/ext/APB_ExternalCA.crl
Thumbprint Algorithm	Алгоритм хэш-функции сертификата	Sha1
Thumbprint	Значение хэш-функции сертификата	Значение хэш-функции сертификата открытого ключа электронной подписи в соответствии с алгоритмом Sha1
1.3.6.1.4.1.50561.5.1.1	Данные паспорта клиента и идентификатор клиента в системе банка	UTF8String: Passport=<данные паспорта>, ClientId=<Идентификатор клиента>
1.3.6.1.4.1.52072.1.1	Единый регистрационный номер физического лица	IA5String: 6000012345678901234
1.3.6.1.4.1.52072.1.2	Регистрационный номер юридического лица, только для юридических лиц.	IA5String: 1234567890
1.3.6.1.4.1.52072.1.3	Фискальный код государственного учреждения	IA5String: 1234567890

¹ Перечень отношений, при осуществлении которых электронный документ с электронной подписью будет иметь юридическое значение, приведен в Приложении №2 к Регламенту

1.3.6.1.4.1.52072.2.1	Регистрационный номер ОФД	UTF8String: OfdCode=<Регистрационный номер ОФД>
1.3.6.1.4.1.52072.2.2	Данные онлайн-кассы	UTF8String: FiscalCode=<Фискальный код кассы>, OfdCode=<Регистрационный номер ОФД>, DeviceTypeId=<Тип устройства>, DeviceId=<Идентификатор устройства>, Ern=<Единый регистрационный номер физического лица>, RegNumber=<Регистрационный номер юридического лица, только для юридических лиц>

Приложение №4
к Регламенту Удостоверяющего центра ЗАО «Агропромбанк»

Дополнения сертификата открытого ключа электронной подписи

1. Процессинг и пластиковые карты
 - 1.1. Сертификат E-Commerce терминала

Дополнения сертификата открытого ключа электронной подписи		
1.3.6.1.4.1.50561.2.1.2	Идентификатор e-Commerce терминала	UTF8String: TerminalId=<Идентификатор терминала>

- 1.2. Система Loyalty

Дополнения сертификата открытого ключа электронной подписи		
1.3.6.1.4.1.50561.2.2.2	Данные по программе лояльности	UTF8String: ProjectId=<Идентификатор проекта программы лояльности>
1.3.6.1.4.1.50561.2.2.3	Данные по программе лояльности	UTF8String: ProjectId=<Идентификатор проекта программы лояльности>

- 1.3. Система выдачи карт по агентской схеме

Дополнения сертификата открытого ключа электронной подписи		
1.3.6.1.4.1.50561.2.3.2	Идентификатор группы агентов выдачи карт	UTF8String: GroupId=<Идентификатор группы агентов>

2. Система продажи билетов
 - 2.1. Сертификат администратора

Дополнения сертификата открытого ключа электронной подписи		
1.3.6.1.4.1.50561.3.1.3	Идентификатор организации	UTF8String: OrgId=<Id организации>

- 2.2. Сертификат оператора продаж

Дополнения сертификата открытого ключа электронной подписи		
1.3.6.1.4.1.50561.3.1.4	Идентификатор организации продаж	UTF8String: OrgId=<Id организации>

- 2.3. Сертификат терминала

Дополнения сертификата открытого ключа электронной подписи		
1.3.6.1.4.1.50561.3.1.2	Идентификатор терминала продажи билетов	UTF8String: OrgId=<Id организации>, PosId=<Id терминала>

- 3. Дистанционное банковское обслуживание
 - 3.1. Сертификат Пользователя системы

Дополнения сертификата открытого ключа электронной подписи		
1.3.6.1.4.1.50561.4.1.2	Идентификатор клиента банка	ClientId=<Идентификатор клиента>

- 4. Сертификаты ЭП физических и юридических лиц

Дополнения сертификата открытого ключа электронной подписи		
1.3.6.1.4.1.50561.5.1.1	Данные паспорта клиента и идентификатор клиента в системе банка	UTF8String: Passport=<данные паспорта>, ClientId=<Идентификатор клиента>
1.3.6.1.4.1.52072.1.1	Единый регистрационный номер физического лица	IA5String: 6000012345678901234
1.3.6.1.4.1.52072.1.2	Регистрационный номер юридического лица, только для юридических лиц.	IA5String: 1234567890
1.3.6.1.4.1.52072.1.3	Фискальный код государственного учреждения	IA5String: 1234567890

Согласовано:

1-й Заместитель Председателя
Правления

(должность)

С.В.Лупашко

(подпись)

(ф.и.о.)

Юридический отдел

(должность)

Ю.В. Рассказова

(подпись)

(ф.и.о.)

Начальник отдела автоматизации

(должность)

А.М.Звягин

(подпись)

(ф.и.о.)

Руководитель развития проектов

(должность)

А.В.Витюк

(подпись)

(ф.и.о.)