«Утверждено»
Правлением
ЗАО «Агропромбанк»
«__» _____ года
Протокол № ___

Председатель Правления
_____ Ю.Ю. Кучеренко

РЕГЛАМЕНТ
Удостоверяющего центра
ЗАО «Агропромбанк»

Версия 5.0

Оглавление

1. Термины и определения

Автоматическое создание и автоматическая проверка электронной подписи – способ создания и проверки электронной подписи, при котором данные действия выполняются без непосредственного участия человека, за счет применения программных и (или) технических средств.

Банк- Закрытое акционерное общество «Агропромбанк» (ЗАО «Агропромбанк»)

Бизнес-система - обобщенное понятие корпоративной информационной системы, эксплуатирующейся в Банке, 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, на имя которого Удостоверяющим центром Банка выдан Сертификат открытого ключа электронной подписи, и которое хранит и использует соответствующий закрытый ключ, позволяющий с помощью средств электронной подписи создавать свою Электронную подпись в Электронных документах (подписывать Электронные документы) или юридическое лицо при использовании Сертификата открытого ключа для автоматического создания и (или) автоматической проверки электронных подписей в информационных системах.

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

Закрытый ключ электронной подписи действует на определенный момент времени если:

- наступил момент времени начала действия Сертификата;
- срок действия Сертификата не истек;
- Сертификат не аннулирован.

Компрометация ключа – нарушение конфиденциальности закрытого ключа.

Место своего нахождения – персональный компьютер или иное устройство, на котором Пользователь совершает действия, указанные в Регламенте.

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. Открытый ключ сертифицируется Удостоверяющим центром и является доступным для всех участников электронного взаимодействия.

Пользователь Удостоверяющего центра – юридическое лицо, в том числе орган государственной власти, исполнительной власти и орган местного самоуправления (далее – «юридическое лицо»), физическое лицо, присоединившееся к Регламенту Удостоверяющего центра и внесенное в реестр Удостоверяющего центра.

Правовой статус Владельца Сертификата – специальное обозначение в документах и запросах, оформляемых на основании настоящего Регламента, физических лиц, на имя которых выдается Специальный Сертификат, а также частных нотариусов:

– Нотариус (notary)

- Судебный исполнитель (marshal)

- Следователь, дознаватель (coroner)

- Налоговый инспектор (taxer)

– Частный нотариус (private notary)

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

Распорядитель Сертификата – юридическое лицо, в том числе орган государственной власти, исполнительной власти и орган местного самоуправления, которому выдается Сертификат.

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.

Секретное слово – комбинация букв, цифр, символов в количестве не менее шести, сгенерированная Пользователем при формировании запроса на создание Сертификата открытого ключа электронной подписи.

Сертификат открытого ключа электронной подписи (Сертификат) - электронный документ с электронной подписью 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.

Специальный Сертификат открытого ключа электронной подписи (Специальный Сертификат) – Сертификат открытого ключа электронной подписи специального назначения, который выдается Удостоверяющим центром Пользователю для подтверждения подлинности электронной подписи и идентификации Владельца Сертификата открытого ключа электронной подписи, у которого есть полномочия для подписания запросов в электронной форме, направляемых в Банк для получения информации, составляющей банковскую тайну в соответствии с действующим законодательством ПМР. Все условия, указанные в Регламенте в отношении Сертификата, распространяются на Специальный Сертификат в части не противоречащей сути Специального Сертификата.

Список аннулированных сертификатов (CAC) – электронный документ с электронной подписью уполномоченного лица Удостоверяющего центра, который содержит перечень сертификатов, являющихся аннулированными, с указанием серийного номера сертификата, даты и причины аннулирования. CAC 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 (Стороны, Сторона) - Банк 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) - ЗАО «Агропромбанк», осуществляющий в рамках Регламента следующие основные функции:

- создание Сертификатов открытых ключей электронной подписи;
- аннулирование Сертификатов ключей электронной подписи;
- ведение реестра Удостоверяющего центра, обеспечение актуальности сведений, содержащихся в реестре;
- проверка уникальности открытых ключей электронной подписи;
- выдача Сертификатов открытых ключей электронной подписи с информацией об их действии;
- подтверждение подлинности электронной подписи в электронном документе;
- осуществление иных функций, предусмотренных действующим законодательством ПМР и настоящим Регламентом.

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

Штамп времени – информация, представленная в электронной форме, которая присоединена или иным образом связана с электронным документом и которая подтверждает, посредством электронной подписи, факт существования данного электронного документа в определенный момент времени с сохранением его целостности.

Электронный документ –информация, представленная в электронной форме, пригодная для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах. Электронный документ существует только на материальном носителе. Все экземпляры электронного документа, идентичные один другому, являются оригиналами. В случае, когда одним лицом создается документ на бумажном носителе и электронный документ, идентичные по содержанию, оба документа имеют одинаковую юридическую силу. В этом случае документ на бумажном носителе не является копией электронного документа. Копией электронного документа является его форма внешнего представления на бумажном носителе. Копия электронного документа заверяется в установленном действующим законодательством Приднестровской Молдавской Республики порядке заверения копий документов на бумажном носителе и должна содержать отметку о том, что она является копией электронного документа.

Электронный документ, подписанный электронной подписью с использованием средств электронной подписи для автоматического создания и (или) автоматической проверки электронных подписей в информационной системе имеет юридическую силу как и документ, подписанный собственноручно.

Электронная подпись (ЭП) - информация в электронной форме, которая присоединена к другой информации в электронной форме или иным образом связана с такой информацией (подписываемой информации) 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 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, сторонами которого являются Банк и любое лицо (физическое лицо, юридическое лицо в том числе орган государственной власти, исполнительной власти и орган местного самоуправления), принявшее все условия Регламента не иначе, как путем присоединения к Регламенту в целом в порядке, определенном в Регламенте.

2.2. Действие Регламента

2.2.1. С даты регистрации Заявления о присоединении к Регламенту Удостоверяющего центра ЗАО «Агропромбанк» в Удостоверяющем центре лицо, подавшее Заявление, считается присоединившимся 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 – https://ca.agroprombank.com/pki/certificate/regulations

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

2.2.6. Уведомления о внесении изменений или дополнений в Регламент и об утверждении новых редакций Регламента размещаются на Internet странице Удостоверяющего центра Банка, расположенной по адресу – https://ca.agroprombank.com/

2.2.7. Все изменения (дополнения), вносимые Банком в Регламент, вступают в силу и становятся обязательными для Сторон в срок, указанный в соответствующем уведомлении о внесении изменений и дополнений в Регламент, размещенном в порядке, указанном в п. 2.2.6 Регламента. Если срок в уведомлении о внесении изменений и дополнений в Регламент не указан, все изменения (дополнения) Регламента вступают в силу по истечении 10 рабочих дней с даты размещения новой редакции Регламента на сайте Удостоверяющего центра по адресу https://ca.agroprombank.com/pki/certificate/regulations.

2.2.8. Любые изменения и дополнения в Регламент со дня вступления в силу равно распространяются на всех лиц, присоединившихся к Регламенту, в том числе присоединившихся к Регламенту ранее даты вступления изменений (дополнений) в силу.

2.2.9. 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.4.4.5 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 в случае установленного факта компрометации соответствующего ключа электронной подписи, с уведомлением Владельца аннулированного Сертификата открытого ключа электронной подписи (а в случае, если Сертификат выдан Распорядителю Сертификата – с уведомлением и Владельца Сертификата и Распорядителя Сертификата) и указанием обоснованных причин.

3.1.2. Отказать в создании Сертификата открытого ключа электронной подписи в случае, если использованное Пользователем для формирования запроса на Сертификат открытого ключа электронной подписи средство криптографической защиты информации не поддерживается Удостоверяющим центром, а также если Пользователем не соблюден порядок получения Сертификата, определенный Регламентом.

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 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, созданных 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 при наличии у Удостоверяющего центра такой технической возможности подтверждения.

3.2.7. Обратиться в Удостоверяющий центр за подтверждением подлинности электронных подписей Удостоверяющего центра в созданных х им Сертификатах открытых ключей электронной подписи.

3.2.8. Сформировать ключ электронной подписи в месте своего нахождения 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. Пользоваться 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. Пользоваться предоставляемыми Удостоверяющим центром программными средствами, чтобы получить и установить на место своего нахождения Токен и/или 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 Сертификата.

3.2.14. Обратиться в Удостоверяющий центр за получением нового Сертификата открытого ключа электронной подписи в течение срока действия Сертификата до окончания срока действия Сертификата (плановая смена Сертификата).

3.2.15. 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 созданных им Сертификатов открытых ключей электронной подписи Пользователей Удостоверяющего центра и реестр аннулированных Сертификатов.

3.3.2. Принимать 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. Создавать Сертификаты открытого ключа электронной подписи зарегистрированных Пользователей в соответствии с порядком, определенным в настоящем Регламенте.

3.3.6. Обеспечить уникальность серийных номеров созданных Сертификатов открытых ключей электронной подписи Пользователей Удостоверяющего центра.

3.3.7. Обеспечить уникальность значений открытых ключей электронной подписи в созданных Сертификатах открытых ключей электронной подписи Пользователей Удостоверяющего центра.

3.3.8. Аннулировать Сертификаты открытого ключа электронной подписи в случаях и в порядке, установленных Регламентом.

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 закрытый 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;
- если Пользователю стало известно, что этот ключ использовался ранее другими лицами, используется или возможно будет использоваться другими лицами;
- если Владелец Специального Сертификат утратил по каким-либо причинам свои полномочия на подписание запросов в электронной форме для получения информации, составляющей банковскую тайну в соответствии с действующим законодательством ПМР.

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 https://ca.agroprombank.com/pki/certificate/regulations на предмет изменения Регламента.

3.4.8. Оплачивать комиссионное вознаграждение за услуги, оказываемые Удостоверяющим центром, в соответствии с Тарифами и в установленными ими порядке.

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. Незамедлительно уведомлять Удостоверяющий центр о смене руководителя Распорядителя Сертификата, предоставив документы, подтверждающие данный факт.

3.4.12. 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 Приложении №2 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 Приложении №2 к данному Регламенту, которые описывают процедуры регистрации Пользователей, генерации ключей, управления сертификатами открытого ключа электронной подписи.

4.3. Создание и получение Сертификата открытого ключа электронной подписи

Порядок создания и получения Сертификатов открытого ключа электронной подписи Пользователей Удостоверяющего центра изложен в Приложении №2 к данному Регламенту, которые описывают процедуры регистрации Пользователей, генерации ключей, управления Сертификатами открытого ключа электронной подписи.

Физические лица, получившие Сертификаты открытого ключа электронной подписи, вправе использовать ЭП при подписании ЭД при осуществлении ими законной предпринимательской деятельности, в том числе, если они являются Главами крестьянских (фермерских) хозяйств.

Физические лица, являющиеся уполномоченными представителями юридических лиц, получившие Сертификаты открытого ключа электронной подписи или Специальные сертификаты, обязаны использовать ЭП при подписании ЭД при осуществлении ими своей деятельности в пределах предоставленных полномочий Распорядителями Сертификатов.

Физические лица, получившие Сертификаты открытого ключа электронной подписи для использования ЭП при осуществлении своей деятельности в качестве частных нотариусов в соответствии с действующим законодательством, обязаны использовать ЭП только в пределах полномочий, предоставленных действующим законодательством.

Удостоверяющий центр не контролирует основания и законность применения ЭП в вышеуказанных случаях.

Временем подписания электронного документа, на основании которого было проведено создание 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 обязан аннулировать Сертификат открытого ключа электронной подписи Пользователя Удостоверяющего центра в следующих случаях:

- по заявлению Пользователя Удостоверяющего центра (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);
- 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 (если в Удостоверяющем центре имеется достоверная информация о вышеуказанном);
- 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. Удостоверяющий центр обязан аннулировать Специальный Сертификат без заявления Пользователя или Владельца Специального Сертификата, если Удостоверяющему центру стало достоверно известно о том, что Владелец Специального Сертификата утратил по каким-либо причинам свои полномочия на подписание запросов в электронной форме для получения информации, составляющей банковскую тайну в соответствии с действующим законодательством ПМР, а также в случаях, указанных в п. 4.4.1.

4.4.3. 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.

4.4.4. 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.

4.4.5. Аннулирование Сертификата открытого ключа электронной подписи по заявлению Пользователя.

Аннулирование Сертификата открытого ключа электронной подписи Пользователя Удостоверяющего центра осуществляется Удостоверяющим центром:

- на основании Заявления на аннулирование Сертификата открытого ключа электронной подписи, составленного в бумажной форме, указанной в приложениях в Регламенту. Подача такого заявления в Удостоверяющий центр и его рассмотрение осуществляется в течение рабочего дня;
- на основании заявления (запроса) на аннулирование Сертификата, составленного в электронной форме с использованием Секретного слова, в порядке, предусмотренном в Приложением № 3 к Регламенту и Инструкцией по работе с программой «АПБ: управление ключами», расположенной в сети Интернет по адресу http://ca.agroprombank.com/

4.4.6. В случае аннулирования Сертификата по заявлению Пользователя Удостоверяющий центр должен 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, опубликованном в сети Интернет по адресу http://ca.agroprombank.com/.

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

4.4.8. Информация о размещении списка аннулированных сертификатов заносится в созданные Удостоверяющим центром Сертификаты в расширение CAC.

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 до оказания соответствующей услуги Удостоверяющим центром.

4.5.2 В случае наличия денежных средств на текущем счете Пользователя в валюте комиссионного вознаграждения, определенной в Тарифах Пользователь предоставляет Банку право 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 предоставляет Банку право списывать в безакцептном порядке вышеуказанные суммы со всех своих текущих счетов, открытых в Банке и/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 требования этого банка и действующего законодательства ПМР. Пользователь обязуется не отзывать 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 срок, установленный Регламентом.

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

4.5.6 В случае если Пользователь оплатил комиссионное вознаграждение за выдачу Сертификата открытого ключа электронной подписи, но не осуществил все необходимые действия для получения Сертификата в течение 2 (двух) месяцев со дня оплаты, Удостоверяющий центр вправе не оказывать услуги по изготовлению Сертификата открытого ключа электронной подписи в рамках ранее заказанной и оплаченной услуги, по истечении вышеуказанного срока. В таком случае, осуществление Удостоверяющим центром услуги по изготовлению Сертификата открытого ключа электронной подписи возможно только после повторной оплаты комиссионного вознаграждения за выдачу Сертификата открытого ключа электронной подписи (при условии совершения Пользователем всех необходимых действий для получения Сертификата).

При этом, Удостоверяющий центр не возвращает Пользователю уплаченное ранее комиссионное вознаграждение.

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, полученным в Удостоверяющем центре или у третьих лиц.

4.6.2. Удостоверяющий центр выдает Токен по запросу Пользователя, при наличии такой возможности у Удостоверяющего центра.

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 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. Удостоверяющий центр обязан безвозмездно заменить поврежденный Токен на аналогичный качественный Токен ,если Токен был выдан Удостоверяющим центром:

- если во время подписания Акта приема-передачи были обнаружены повреждения Токена.

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, создаваемых 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 закрытый ключ электронной подписи и соответствующий ему открытый ключ электронной подписи;
- Уполномоченное лицо Удостоверяющего центра создает 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, созданных 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 закрытого ключа электронной подписи.

В случае компрометации или угрозы компрометации закрытого 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 создает Сертификаты открытых ключей электронной подписи Пользователей в электронной форме формата X.509 версии 3 и список отозванных сертификатов (CAC) 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 Idendifier	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	SybjectType (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 №2 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 умышленного или неумышленного искажения Пользователем информации, содержащейся в заявлениях либо иных документах, представленных в Удостоверяющий центр;

-если Пользователь не исполняет или ненадлежащим образом исполняет свои обязанности, что приводит к ненадлежащему или невозможному исполнению Удостоверяющим центром своих обязанностей;

- если Пользователь своевременно не осуществил процедуру по аннулированию Сертификата.

8.2. Удостоверяющий центр несет ответственность за убытки, возникшие у Пользователей 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. Данные об 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 Министерством цифрового развития, связи и массовых коммуникаций ПМР (номер и дата аккредитации: № 4 от 28.12.2023 года).

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

Место нахождения: ПМР, г. Тирасполь, ул. 25 Октября, 65/1
Почтовый адрес: ПМР, г. Тирасполь, ул. 25 Октября, 65/1

Адрес электронной почты: http://ca@agroprombank.com
Адрес в сети Интернет: http://ca.agroprombank.com

Приложение №1
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 (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
  - 8 – Автоматизированная система оплаты проезда
- YY – область действия Сертификата, приведенная в п.2. настоящего приложения:
- Области применения сертификатов Удостоверяющего центра Банка
  - Технологические объекты Сертификатов открытых ключей электронной подписи (принадлежат Министерству цифрового развития, связи и массовых коммуникаций ПМР)

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
1.3.6.1.4.1.52072.1.3	Сертификат органа государственной, исполнительной власти или органа местного самоуправления
1.3.6.1.4.1.52072.1.4	Специальный Сертификат
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 Удостоверяющим центром
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
1.3.6.1.4.1.50561.2.4	Межбанковское взаимодействие	
1.3.6.1.4.1.50561.2.4.1	Сертификат сервера платежной системы «Клевер»	Подписание запросов сервера платежной системы «Клевер»
1.3.6.1.4.1.50561.2.4.2	Сертификат участника платежной системы «Клевер»	Подписание запросов участников платежной системы «Клевер»

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.
1.3.6.1.4.1.50561.4.1.3	Идентификатор физического лица	Идентификатор физического лица EPH клиента банка для внутренних сервисов
1.3.6.1.4.1.50561.4.1.4	Идентификатор юридического лица	Идентификатор клиента Банка (юридического лица) для внутренних сервисов
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 используется 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
1.3.6.1.4.1.50561.7	Корпоративная система	
1.3.6.1.4.1.50561.8	Автоматизированная система оплаты проезда (АСОП)	
1.3.6.1.4.1.50561.8.1	Субъекты АСОП	
1.3.6.1.4.1.50561.8.1.1	Участник информационной системы оператора АСОП	Расширение сертификата используется для идентификации участника информационной системы оператора АСОП: • Оператор АСОП • Операторы автомобильных перевозок • Министерства и ведомства • Перевозчики Обязательно наличие в поле Subject объекта OID.2.5.4.13 (Description) с указанием наименования Участника.
1.3.6.1.4.1.50561.8.1.2	Агенты по продаже билетов	Расширение сертификата используется для идентификации агентов по продаже билетов. Обязательно наличие в поле Subject объекта OID.2.5.4.13 (Description) с указанием наименования Агента.
1.3.6.1.4.1.50561.8.1.3	Пользователи портала АСОП	Расширение сертификата используется для идентификации пользователей портала АСОП. Обязательно наличие в поле Subject объекта OID.2.5.4.13 (Description) с указанием ФИО лица получившего доступ к порталу АСОП, указанием идентификатора физического лица в поле 1.3.6.1.4.1.52072.1.1 и принадлежность к агенту 1.3.6.1.4.1.50561.8.1.1
1.3.6.1.4.1.50561.8.1.4	Сервисы	Расширение сертификата используется для идентификации сервисов и информационных систем, взаимодействующих с АСОП. Обязательно наличие в поле Subject объекта OID.2.5.4.13 (Description) с указанием названия сервиса или информационной системы.

Приложение №2
к Регламенту Удостоверяющего центра ЗАО «Агропромбанк»

Порядок получения Сертификатов

1. Генерация ключевой информации

Пользователь в месте своего нахождения осуществляет генерацию ключевой информации на ключевом носителе, формирует запрос на создание Сертификата открытого ключа электронной подписи в формате PKCS#10 и отправляет запрос на создание Сертификата открытого ключа электронной подписи в систему УЦ.

Одновременно Пользователь передает документы на бумажном носителе, подтверждающие достоверность данных, указанных в запросе на создание 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 (за исключением случаев, когда Пользователь/Владелец Сертификата обратился за созданием и выдачей нового Сертификата).

В случае получения Сертификата Распорядителем Сертификата заявление на создание и выдачу Сертификата оформляется в письменной произвольной форме на бумажном носителе, подписывается уполномоченным лицом Распорядителем Сертификата и скрепляется печатью Распорядителя Сертификата (или без печати, но на фирменном бланке – для Распорядителей Сертификатов, являющихся органами государственной, исполнительной власти и органами местного самоуправления), с обязательным указанием следующей информации:

- фамилия, имя и отчество уполномоченного лица/частного нотариуса, который будет являться Владельцем Сертификата;
- документ, удостоверяющий личность будущего Владельца Сертификата (его серия, номер, когда и кем выдан);
- область действия Специального Сертификата и категория Владельца Специального сертификата (notary – Нотариус, marshal - Судебный исполнитель, coroner - Следователь, дознаватель, taxer - Налоговый инспектор, private notary – Частный нотариус).

Срок действия заявления на создание и выдачу Сертификата составляет 30 (тридцать) календарных дней со дня его получения Удостоверяющим центром. По истечении вышеуказанного срока Удостоверяющий центр не выдает Сертификат лицам, указанным в таком заявлении.

До выдачи Сертификата его Владельцу Распорядитель Сертификата вправе в любое время отменить полученное Удостоверяющим центром заявление на создание и выдачу Сертификата, направив об этом заявление в произвольной форме в Удостоверяющий центр в письменной форме на бумажном носителе, подписанное уполномоченным лицом Распорядителя Сертификата, или в виде электронного документа, подписанного ЭП уполномоченного лица Распорядителя Сертификата.

После получения вышеуказанного заявления Удостоверяющим центром Владелец Сертификата вместе с собственноручно подписанным Заявлением (Приложение №4в) подлежит обязательному фотографированию Оператором УЦ.

Допускается составление вышеуказанного заявления на создание и выдачу сертификата от Распорядителя Сертификата в письменной форме в виде электронного документа, подписанного ЭП уполномоченного лица Распорядителя Сертификата.

После успешной проверки документов Пользователя в системе Банка Оператор УЦ формирует и отправляет запрос на регистрацию и электронный запрос на создание 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 при формировании первого 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. Создание и получение Сертификата открытого ключа электронной подписи Пользователя

Создание Сертификата открытого ключа электронной подписи Пользователя осуществляется Удостоверяющим центром на основании заявления на создание и выдачу Сертификата открытого ключа электронной подписи.

Подписывая Заявление на создание и выдачу сертификата открытого ключа электронной подписи Пользователь поручает Удостоверяющему центру запрашивать у третьих лиц любые, имеющиеся у них сведения, необходимые для получения Сертификата в Удостоверяющем центре.

При получении заявления на создание сертификата открытого ключа электронной подписи УЦ осуществляет проверку достоверности сведений, содержащихся в заявлении и хранение заявления.

Заявление на создание и выдачу сертификата открытого ключа электронной подписи, направляемое впервые в Удостоверяющий центра, в электронной форме представляет собой электронный документ формата XML. В качестве данных используется запрос на создание 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 связи с приближающимся окончанием срока его действия в электронной форме при обращении Пользователя представляет собой электронный документ формата XADES. В качестве подписываемых данных используется запрос на создание 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 2 недели с момента поступления электронного запроса на создание Сертификата в Удостоверяющий центр при условии соблюдения Владельцем Сертификата всех условий, предусмотренных Регламентом.

Сертификат открытого ключа электронной подписи направляется Владельцу Сертификата 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 (запрос) на аннулирование Сертификата в электронной форме представляет собой электронный документ формата XML со следующими данными:

- серийный номер отзываемого Сертификата открытого ключа электронной подписи;
- код причины аннулирования из следующего перечня допустимых значений:
  "1" Компрометация ключа
  "4" Сертификат заменен

"5" Прекращение работы

- текстовое значение комментария владельца 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.

Срок действия ключа электронной подписи и сертификата открытого ключа электронной подписи Пользователя Удостоверяющего центра при плановой смене Сертификата – 1 год и оставшееся количество дней срока действия ключа электронной подписи и старого Сертификата.

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	Улучшеный 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 Idendifier	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	идентификатор клиента в системе банка	UTF8String: ClientId=<Идентификатор клиента>
1.3.6.1.4.1.52072.1.1	Единый регистрационный номер физического лица	UTF8String 6000012345678901234
1.3.6.1.4.1.52072.1.2	Регистрационный номер юридического лица	UTF8String 1234567890
1.3.6.1.4.1.52072.1.3	Сертификат органа государственной, исполнительной власти или органа местного самоуправления.	UTF8String 1234567890

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

	Фискальный код	
1.3.6.1.4.1.52072.1.4	Специальный Сертификат	UTF8String: notary – Нотариус marshal - Судебный исполнитель coroner - Следователь, дознаватель taxer - Налоговый инспектор private notary – Частный нотариус
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 №3
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 Пользователя	UTF8String: Идентификатор клиента банка Clientid
1.3.6.1.4.1.50561.4.1.3	Единый регистрационный номер физического лица	UTF8String: 6000012345678901234
1.3.6.1.4.1.50561.4.1.4	Идентификатор юридического лица	UTF8String: Идентификатор клиента банка ClientId

4. Сертификаты ЭП физических и юридических лиц

Дополнения сертификата открытого ключа электронной подписи		
1.3.6.1.4.1.50561.5.1.1	Данные идентификатора Пользователя в системе Банка	UTF8String: ClientId=<Идентификатор клиента>
1.3.6.1.4.1.52072.1.1	Единый регистрационный номер физического лица	UTF8String: 6000012345678901234
1.3.6.1.4.1.52072.1.2	Регистрационный номер юридического лица	UTF8String: 1234567890
1.3.6.1.4.1.52072.1.3	Сертификат органа государственной, исполнительной власти или органа местного самоуправления. Фискальный код	UTF8String: 1234567890
1.3.6.1.4.1.52072.1.4	Специальный Сертификат	UTF8String: notary - Нотариус marshal - Судебный исполнитель coroner - Следователь, дознаватель taxer - Налоговый инспектор private notary – Частный нотариус

5. Автоматизированная система оплаты проезда (АСОП)
   5.1. Сертификат участника АСОП

Дополнения сертификата открытого ключа электронной подписи		
1.3.6.1.4.1.50561.8.1.1	Идентификатор участника информационной	UTF8String: ParticipantId=<Идентификатор участника информационной системы оператора АСОП (0001)>

	системы оператора АСОП	

5.2. Сертификат агента по продаже билетов АСОП

Дополнения сертификата открытого ключа электронной подписи		
1.3.6.1.4.1.50561.8.1.2	Идентификатор агента по продаже билетов	UTF8String: OrganizationId=<Идентификатор агента (0001)>

5.3. Пользователи портала АСОП

Дополнения сертификата открытого ключа электронной подписи		
1.3.6.1.4.1.50561.8.1.3	Идентификатор пользователя портала АСОП	UTF8String: ERN=<Идентификатор пользователя (ERN)>
1.3.6.1.4.1.50561.8.1.1	Идентификатор участника информационной системы оператора АСОП	UTF8String: ParticipantId=<Идентификатор участника информационной системы оператора АСОП (0001)>

5.4. Сервисы и информационные системы, взаимодействующие с АСОП

Дополнения сертификата открытого ключа электронной подписи		
1.3.6.1.4.1.50561.8.1.4	Идентификатор сервиса или информационной системы	UTF8String: OrganizationId=<Идентификатор сервиса или информационной системы (0001)>

Приложение №4а
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. 25 Октября, 65/1

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.

Приложение №4б
к Регламенту Удостоверяющего центра ЗАО
«Агропромбанк»

Для физических лиц/
частых нотариусов

Заявление о присоединении к Регламенту Удостоверяющего центра ЗАО «Агропромбанк»

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

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. 25 Октября, 65/1

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.

Приложение №4в
к Регламенту Удостоверяющего центра ЗАО
«Агропромбанк»

Для юридических лиц/
частных нотариусов

Заявление

Я,_____,
(Ф.И.О., документ удостоверяющий личность, его серия и номер, кем и когда выдан)
прошу выдать мне Сертификат открытого ключа электронной подписи на основании письма №___ от _____г.

Распорядитель Сертификата:

_____
(наименование юридического лица)

Данные Сертификата:

Идентификатор открытого ключа

_____

Правовой статус Владельца Сертификата (в случае его наличия)

_____

понимаю и соглашаюсь с тем, что в случаях:

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

- нарушения конфиденциальности закрытого ключа (компрометация 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 Банка.

Владелец Сертификата:

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

Принято:

Удостоверяющий центр ЗАО «Агропромбанк»

Адрес: MD-3300 г. Тирасполь, ул. 25 Октября, 65/1

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

Приложение №4г
к Регламенту Удостоверяющего центра ЗАО
«Агропромбанк»

Для физических лиц

Заявление
на создание и выдачу сертификата открытого
ключа электронной подписи №___

Место QR кода

г. Тирасполь «___»_____20__ г.

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

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

Идентификатор открытого ключа

_____

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. 25 Октября, 65/1

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

Приложение №4д
к Регламенту Удостоверяющего центра ЗАО
«Агропромбанк»

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. 25 Октября, 65/1

Уполномоченное лицо: _____/_____

(подпись) *(фамилия, имя, отчество)*

М.П.

Приложение №4е
к Регламенту Удостоверяющего центра ЗАО
«Агропромбанк»

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. 25 Октября, 65/1

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

Приложение №4ж
к Регламенту Удостоверяющего центра ЗАО
«Агропромбанк»

Для физических лиц/
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)*,

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. 25 Октября, 65/1

Уполномоченное лицо: _____/_____

(подпись) *(фамилия, имя, отчество)*

М.П.

Согласовано:

Первый заместитель Председателя Правления		С.В. Лупашко
(должность)	(подпись)	(Ф.Идело не в регламенте .О.)
Руководитель юридического департамента		А.В. Николаев
(должность)	(подпись)	(Ф.И.О.)
Директор IT-центра		А.М. Звягин
(должность)	(подпись)	(Ф.И.О.)
Руководитель корпоративного блока		О.М. Вакарчук
(должность)	(подпись)	(Ф.И.О.)
Руководитель розничного блока		Ю.С. Дирун
(должность)	(подпись)	(Ф.И.О.)
Руководитель департамента информационных технологий		А.В. Витюк
(должность)	(подпись)	(Ф.И.О.)