

ЗАКОН РЕСПУБЛИ АБХАЗИЯ

Об электронной цифровой подписи в банковской системе

Глава I. Общие положения

Статья 1. Цель и сфера применения настоящего закона

1. Целью настоящего закона является обеспечение правовых условий использования электронной цифровой подписи в электронных документах, при соблюдении которых электронная цифровая подпись в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе.

2. Действие настоящего закона распространяется на отношения, возникающие при совершении банковских операций со счетами физических и юридических лиц и межбанковских расчетах и иных банковских услуг.

Действие настоящего закона не распространяется на отношения, возникающие при использовании иных аналогов собственноручной подписи.

Статья 2. Правовое регулирование отношений в области использования электронной цифровой подписи

Правовое регулирование отношений в области использования электронной цифровой подписи в банковской системе осуществляется в соответствии с настоящим законом и другими законами и принимаемыми в соответствии с ними иными нормативными правовыми актами, а также осуществляется соглашением сторон.

Статья 3. Основные понятия, используемые в настоящем законе

Для целей настоящего закона используются следующие основные понятия:

- электронный документ - документ, в котором информация представлена в электронно-цифровой форме;

- электронная цифровая подпись - реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе;

- владелец сертификата ключа подписи - физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы);

- средства электронной цифровой подписи - аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций - создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создание закрытых и открытых ключей электронных цифровых подписей;

- сертификат средств электронной цифровой подписи - документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средств электронной цифровой подписи установленным

требованиям;

-закрытый ключ электронной цифровой подписи - уникальная последовательность символов известная исключительно владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи;

-открытый ключ электронной цифровой подписи - уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступная пользователю банковской информационной системы и предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе;

-сертификат ключа подписи - документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и которые выдаются удостоверяющим центром участнику банковской информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи;

-подтверждение подлинности электронной цифровой подписи в электронном документе - положительный результат проверки соответствующим сертифицированным средством электронной цифровой подписи с использованием сертификата ключа подписи принадлежности электронной цифровой подписи в электронном документе владельцу сертификата ключа подписи и отсутствия искажений в электронном документе, подписанном данной электронной цифровой подписью;

-пользователь сертификата ключа подписи - физическое лицо, использующее полученные в удостоверяющем центре сведения о сертификате ключа подписи для проверки принадлежности электронной цифровой подписи владельцу сертификата ключа подписи;

-банковская информационная система - информационная система, участниками которой могут быть кредитные организации и иные для использования кредитными организациями и их клиентами;

-корпоративная банковская информационная система - информационная система, участниками которой может быть ограниченный круг кредитных организаций, определенный ее владельцем или соглашением участников этой информационной системы.

Глава II. Условия использования электронной цифровой подписи

Статья 4. Условия признания равнозначности электронной цифровой подписи и собственноручной подписи

1. Электронная цифровая подпись в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе при одновременном соблюдении следующих условий:

-сертификат ключа подписи, относящийся к этой электронной цифровой подписи, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;

-подтверждена подлинность электронной цифровой подписи в электронном документе;

- электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи.

2. Участник банковской информационной системы может быть одновременно владельцем любого количества сертификатов ключей подписей. При этом электронный

документ с электронной цифровой подписью имеет юридическое значение при осуществлении отношений, указанных в сертификате ключа подписи.

Статья 5. Использование средств электронной цифровой подписи

1. Создание ключей электронных цифровых подписей осуществляется для использования в:

- банковской информационной системе;
- корпоративной банковской информационной системе в порядке, установленном в этой системе.

2. При создании ключей электронных цифровых подписей для использования в банковских информационных системах должны применяться только сертифицированные средства электронной цифровой подписи. Возмещение убытков, причиненных в связи с созданием ключей электронных цифровых подписей не сертифицированными средствами электронной цифровой подписи, может быть возложено на создателей и распространителей этих средств в соответствии с законодательством.

Статья 6. Сертификат ключа подписи

1. Сертификат ключа подписи должен содержать следующие сведения:

- уникальный регистрационный номер сертификата ключа подписи, даты начала и окончания срока действия сертификата ключа подписи, находящегося в реестре удостоверяющего центра;
- фамилия, имя и отчество владельца сертификата ключа подписи или псевдоним владельца. В случае использования псевдонима удостоверяющим центром вносится запись об этом в сертификат ключа подписи;
- открытый ключ электронной цифровой подписи;
- наименование средств электронной цифровой подписи, с которыми используется данный открытый ключ электронной цифровой подписи;
- наименование и место нахождения удостоверяющего центра, выдавшего сертификат ключа подписи;
- сведения об отношениях, при осуществлении которых электронный документ с электронной цифровой подписью будет иметь юридическое значение.

2. В случае необходимости в сертификате ключа подписи на основании подтверждающих документов указываются должность (с указанием наименования и места нахождения организации, в которой установлена эта должность) и квалификация владельца сертификата ключа подписи, а по его заявлению в письменной форме - иные сведения, подтверждаемые соответствующими документами.

3. Сертификат ключа подписи должен быть внесен удостоверяющим центром в реестр сертификатов ключей подписей не позднее даты начала действия сертификата ключа подписи.

4. Для проверки принадлежности электронной цифровой подписи соответствующему владельцу сертификат ключа подписи выдается пользователям с указанием даты и времени его выдачи, сведений о действии сертификата ключа подписи (действует, действие приостановлено, сроки приостановления его действия, аннулирован, дата и время аннулирования сертификата ключа подписи) и сведений о реестре сертификатов ключей подписей. В случае выдачи сертификата ключа подписи в форме документа на бумажном носителе этот сертификат оформляется на бланке удостоверяющего центра и заверяется собственноручной подписью уполномоченного лица и печатью удостоверяющего центра. В случае выдачи сертификата ключа подписи и указанных дополнительных данных в форме электронного документа этот сертификат должен быть подписан электронной

цифровой подписью уполномоченного лица удостоверяющего центра.

Статья 7. Срок и порядок хранения сертификата ключа подписи в удостоверяющем центре

1. Срок хранения сертификата ключа подписи в форме электронного документа в удостоверяющем центре определяется договором между удостоверяющим центром и владельцем сертификата ключа подписи. При этом обеспечивается доступ участников информационной системы в удостоверяющий центр для получения сертификата ключа подписи.

2. Срок хранения сертификата ключа подписи в форме электронного документа в удостоверяющем центре после аннулирования сертификата ключа подписи должен быть не менее установленного законом срока исковой давности для отношений, указанных в сертификате ключа подписи.

По истечении указанного срока хранения сертификат ключа подписи исключается из реестра сертификатов ключей подписей и переводится в режим архивного хранения. Срок архивного хранения составляет не менее чем пять лет. Порядок выдачи копий сертификатов ключей подписей в этот период устанавливается в соответствии с законодательством.

3. Сертификат ключа подписи в форме документа на бумажном носителе хранится в порядке, установленном законодательством об архивах и архивном деле.

Глава III. Удостоверяющий центр

Статья 8. Статус удостоверяющего центра

1. В Республике Абхазия создается Государственный удостоверяющий центр при Национальном банке Республики Абхазия, выдающий сертификаты ключей подписей для использования в банковских информационных системах. При этом удостоверяющий центр должен обладать необходимыми материальными и финансовыми возможностями, позволяющими ему нести гражданскую ответственность перед пользователями сертификатов ключей подписей за убытки, которые могут быть понесены ими вследствие недостоверности сведений, содержащихся в сертификатах ключей подписей.

2. Удостоверяющий центр при Банке Абхазии предназначен для сертификации ключей ЦП при обмене электронными документами в банковской системе Республики Абхазия.

3. Удостоверяющий центр при Национальном банке Республики Абхазия ведет Реестр сертификатов электронных цифровых подписей.

Статья 9. Деятельность удостоверяющего центра

1. Удостоверяющий центр:

- изготавливает сертификаты ключей подписей;
- создает ключи электронных цифровых подписей по обращению участников информационной системы с гарантией сохранения в тайне закрытого ключа электронной цифровой подписи;
- приостанавливает и возобновляет действие сертификатов ключей подписей, а также аннулирует их;

- ведет реестр сертификатов ключей подписей, обеспечивает его актуальность и возможность свободного доступа к нему участников информационных систем;
- проверяет уникальность открытых ключей электронных цифровых подписей в реестре сертификатов ключей подписей и архиве удостоверяющего центра;
- выдает сертификаты ключей подписей в форме документов на бумажных носителях и (или) в форме электронных документов с информацией об их действии;
- осуществляет по обращениям пользователей сертификатов ключей подписей подтверждение подлинности электронной цифровой подписи в электронном документе в отношении выданных им сертификатов ключей подписей.

2.Изготовление сертификатов ключей подписей осуществляется на основании заявления участника информационной системы, которое содержит сведения, указанные в статье 6 настоящего закона и необходимые для идентификации владельца сертификата ключа подписи и передачи ему сообщений. Заявление подписывается собственноручно владельцем сертификата ключа подписи. Содержащиеся в заявлении сведения подтверждаются предъявлением соответствующих документов.

3.При изготовлении сертификатов ключей подписей удостоверяющим центром оформляются в форме документов на бумажных носителях два экземпляра сертификата ключа подписи, которые заверяются собственноручными подписями владельца сертификата ключа подписи и уполномоченного лица удостоверяющего центра, а также печатью удостоверяющего центра. Один экземпляр сертификата ключа подписи выдается владельцу сертификата ключа подписи, второй - остается в удостоверяющем центре.

4.Услуги по выдаче или аннулированию участникам информационных систем сертификатов ключей подписей, зарегистрированных удостоверяющим центром, одновременно с информацией об их действии в форме электронных документов оказываются безвозмездно.

Статья 10. Обязательства удостоверяющего центра по отношению к владельцу сертификата ключа подписи

Удостоверяющий центр при изготовлении сертификата ключа подписи принимает на себя следующие обязательства по отношению к владельцу сертификата ключа подписи:

- вносить сертификат ключа подписи в реестр сертификатов ключей подписей;
- обеспечивать выдачу сертификата ключа подписи обратившимися к нему участниками информационных систем;
- приостанавливать действие сертификата ключа подписи по обращению его владельца;
- уведомлять владельца сертификата ключа подписи о фактах, которые стали известны удостоверяющему центру и которые существенным образом могут сказаться на возможности дальнейшего использования сертификата ключа подписи;
- иные установленные нормативными правовыми актами или соглашением сторон обязательства.

Статья 11. Обязательства владельца сертификата ключа подписи

1. Владелец сертификата ключа подписи обязан:

- не использовать для электронной цифровой подписи открытые и закрытые ключи электронной цифровой подписи, если ему известно, что эти ключи используются или использовались ранее;
- хранить в тайне закрытый ключ электронной цифровой подписи;
- немедленно требовать приостановления действия сертификата ключа подписи при наличии оснований полагать, что тайна закрытого ключа электронной цифровой подписи нарушена.

2. При несоблюдении требований, изложенных в настоящей статье, возмещение

причиненных вследствие этого убытков возлагается на владельца сертификата ключа подписи.

Статья 12. Приостановление действия сертификата ключа подписи

1. Действие сертификата ключа подписи может быть приостановлено удостоверяющим центром на основании указания лиц или органов, имеющих такое право в силу закона или договора, а в корпоративной информационной системе также в силу установленных для нее правил пользования.

2. Период от поступления в удостоверяющий центр указания о приостановлении действия сертификата ключа подписи до внесения соответствующей информации в реестр сертификатов ключей подписей должен устанавливаться в соответствии с общим для всех владельцев сертификатов ключей подписей правилом. По договоренности между удостоверяющим центром и владельцем сертификата ключа подписи этот период может быть сокращен.

3. Действие сертификата ключа подписи по указанию полномочного лица приостанавливается на исчисляемый в днях срок, если иное не установлено нормативными правовыми актами или договором. Удостоверяющий центр возобновляет действие сертификата ключа подписи по указанию полномочного лица. В случае, если по истечении указанного срока не поступает указание о возобновлении действия сертификата ключа подписи, он подлежит аннулированию.

4. В соответствии с указанием полномочного лица о приостановлении действия сертификата ключа подписи удостоверяющий центр оповещает об этом пользователей сертификатов ключей подписей путем внесения в реестр сертификатов ключей подписей соответствующей информации с указанием даты, времени и срока приостановления действия сертификата ключа подписи, а также извещает об этом владельца сертификата ключа подписи и полномочное лицо, от которого получено указание о приостановлении действия сертификата ключа подписи.

Статья 13. Аннулирование сертификата ключа подписи

1. Удостоверяющий центр, выдавший сертификат ключа подписи, обязан аннулировать его:

- по истечении срока его действия;

- при утрате юридической силы сертификата соответствующих средств электронной цифровой подписи, используемых в информационных системах общего пользования;

- в случае если удостоверяющему центру стало достоверно известно о прекращении действия документа, на основании которого оформлен сертификат ключа подписи;

- по заявлению в письменной форме владельца сертификата ключа подписи;

- в иных установленных нормативными правовыми актами или соглашением сторон случаях.

3. В случае аннулирования сертификата ключа подписи удостоверяющий центр оповещает об этом пользователей сертификатов ключей подписей путем внесения в реестр сертификатов ключей подписей соответствующей информации с указанием даты и времени аннулирования сертификата ключа подписи, за исключением случаев аннулирования сертификата ключа подписи по истечении срока его действия, а также извещает об этом владельца сертификата ключа подписи и полномочное лицо (орган), от которого получено указание об аннулировании сертификата ключа подписи.

Глава IV. Особенности использования электронной цифровой подписи

Статья 14. Использование электронной цифровой подписи в корпоративной информационной системе

1.Порядок использования электронных цифровых подписей в корпоративной банковской информационной системе устанавливается решением владельца корпоративной информационной системы или соглашением участников этой системы.

2.Случаи утраты указанными сертификатами юридической силы в корпоративной банковской информационной системе определяется решением владельца этой системы или соглашением участников корпоративной банковской информационной системы.

Статья 15. Признание иностранного сертификата ключа подписи

Иностранный сертификат ключа подписи, удостоверенный в соответствии с законодательством иностранного государства, в котором этот сертификат ключа подписи зарегистрирован, признается на территории Республики Абхазия в случае выполнения установленных законодательством процедур признания юридического значения иностранных документов.

Статья 16. Случаи замещения печатей

1.Содержание документа на бумажном носителе, заверенного печатью и преобразованного в электронный документ, в соответствии с нормативными правовыми актами или соглашением сторон может заверяться электронной цифровой подписью уполномоченного лица.

2.В случаях, установленных законами и иными нормативными правовыми актами или соглашением сторон, электронная цифровая подпись в электронном документе, сертификат которой содержит необходимые при осуществлении данных отношений сведения о полномочиях его владельца, признается равнозначной собственноручной подписи лица в документе на бумажном носителе, заверенном печатью.

Глава V. Заключительные и переходные положения

Статья 18. Приведение нормативных правовых актов в соответствие с настоящим Законом

1. Нормативные правовые акты Республики Абхазия подлежат приведению в соответствие с настоящим Законом в течение трех месяцев со дня вступления в силу настоящего Закона.

Принят Народным Собранием –
Парламентом Республики Абхазия
28 июля 2006 года

**ПРЕЗИДЕНТ
РЕСПУБЛИКИ АБХАЗИЯ**

С. БАГАПШ

г. Сухум
2 августа 2006 года
№ 1442-с-XIV