УТВЕРЖДЕНЫ
ТОО «Удостоверяющий Центр КАЗАХСТАН»
Приказ № 01-03/003702 от 06.07.2013

ПРАВИЛА

использования электронного документооборота и электронной цифровой подписи ТОО «Удостоверяющий центр «Казахстан»

I. Общие положения

1. Настоящие Правила использования электронного документооборота и электронной цифровой подписи ТОО «Удостоверяющий центр «Казахстан» (далее - Правила) разработаны на основании Гражданского кодекса Республики Казахстан, Закона Республики Казахстан №370-II от 07.01.2003 г. «Об электронном документе и электронной цифровой подписи» и других нормативно-правовых актов.

2. Настоящие Правила регламентируют:

2.1. выдачу, регистрацию, хранение, отзыв (аннулирование) регистрационных свидетельств, в том числе их копий на бумажном носителе и ведения регистра регистрационных свидетельств;

2.2. порядок выдачи, регистрации, хранения, отзыва (аннулирования) регистрационных свидетельств, в том числе их копий на бумажном носителе;

2.3. ведение регистра действующих и отозванных (аннулированных) регистрационных свидетельств открытых ключей электронной цифровой подписи удостоверяющими центрами;

2.4. централизованную генерацию открытых и закрытых ключей и выпуск Регистрационных свидетельств в электронной форме, включая распространение средств ЭЦП по обращениям Участников[1];

2.5. подтверждение подлинности ЭЦП в документах, представленных в электронной форме, по обращениям Участников;

2.6. подтверждение подлинности ЭЦП уполномоченного лица Центра в изготовленных им Регистрационных свидетельств по обращениям Участников;

2.7. общие принципы взаимодействия между Участниками и Удостоверяющим центром, владеющим системой документооборота, а так же расчетов в электронной форме с использованием электронных платежных документов в Системе «www.e-kz.com» в ходе финансово-хозяйственной деятельности и иных гражданско-правовых отношений Участниками с Центром и третьими лицами при использовании ЭЦП, предоставленного Центром Участникам.

2.8. порядок организации документооборота при осуществлении Участниками конкретных операций. Формы используемых документов, правила их оформления определяются Инструкциями, Руководствами и иными актами, размещенными на информационном сервере Системы по адресу: http://www.e-kz.com.

[1] Участник системы электронного документооборота (Участник) - физическое или юридическое лицо, государственный орган или должностное лицо, участвующие в процессах сбора, обработки, хранения, передачи, поиска и распространения электронных документов с наделёнными Удостоверяющим центром правами заявлять Владельцев регистрационного свидетельства. Участник системы электронного документооборота – физическое лицо является Владельцем регистрационного свидетельства по умолчанию

2.9. Порядок использования ЭЦП регламентируется нормами Закона Республики Казахстан от 7 января 2003 года N 370-II «Об электронном документе и электронной цифровой подписи»[2]

II. **Термины и определения**

Электронный документ – документ, в котором информация представлена в электронно-цифровой форме и удостоверена посредством электронной цифровой подписи.

Электронная цифровая подпись (ЭЦП) - набор электронных цифровых. символов, созданный средствами электронной цифровой подписи и подтверждающий достоверность электронного документа, его принадлежность Владельцу и неизменность содержания.

Регистрационное свидетельство - документ на бумажном носителе или электронный документ, выдаваемый Удостоверяющим центром для подтверждения соответствия электронной цифровой подписи требованиям, установленным настоящими Правилами.

Владелец регистрационного свидетельства - физическое или юридическое лицо, на имя которого выдано регистрационное свидетельство, правомерно владеющее закрытым ключом, который соответствует открытому ключу, указанному в регистрационном свидетельстве.

Закрытый (секретный) ключ электронной цифровой подписи - последовательность электронных цифровых символов, известная Владельцу регистрационного свидетельства и предназначенная для создания электронной цифровой подписи с использованием средств электронной цифровой подписи, а также и расшифрования информации с использованием средств криптографической защиты информации и известная только Владельцу регистрационного свидетельства.

Открытый ключ электронной цифровой подписи - последовательность электронных цифровых символов, доступная любому лицу и предназначенная для подтверждения подлинности электронной цифровой подписи в электронном документе, а также для зашифрования[3] информации с использованием средств криптографической защиты информации.

Носитель закрытого и открытого ключей ЭЦП – микропроцессорное устройство (микропроцессорная мульти аппликационная карточка, е-токены и т. п.) с возможностью хранения и использования **не извлекаемого из устройства закрытого ключа** ЭЦП и **генерации ЭЦП непосредственно самим устройством**.

Объектный идентификатор (OID) - объектный идентификатор в Казахстанском сегменте 1.2.398.3.4. в соответствии с разрешением Международной Организации по Стандартизации/Международной электротехнической Комиссии- ISO/IEC JTC1/SW6/WG9 на право ведения объектных идентификаторов, присваивается

---

[2] **Статья 10**. Закона Республики Казахстан от 7 января 2003 года N 370-II «Об электронном документе и электронной цифровой подписи»: Использование электронной цифровой подписи

1. Электронная цифровая подпись равнозначна собственноручной подписи подписывающего лица и влечет одинаковые юридические последствия при выполнении следующих условий:

1) удостоверена подлинность электронной цифровой подписи при помощи открытого ключа, имеющего регистрационное свидетельство;

2) лицо, подписавшее электронный документ, правомерно владеет закрытым ключом электронной цифровой подписи;

3) электронная цифровая подпись используется в соответствии со сведениями, указанными в регистрационном свидетельстве.

2. Закрытые ключи электронной цифровой подписи являются собственностью лиц, владеющих ими на законных основаниях. Лицо может иметь неограниченное количество закрытых ключей электронной цифровой подписи. Закрытые ключи электронной цифровой подписи не могут быть переданы другим лицам без согласия владельцев этих ключей.

3. Подписывающее лицо вправе передавать полномочия на использование электронной цифровой подписи своему представителю в соответствии с законодательством Республики Казахстан.

[3] Так как открытый ключ является публичным, его можно получить с сайта удостоверяющего центра или у владельца закрытого ключа. При необходимости отправки владельцу закрытого ключа конфиденциального или секретного зашифрованного сообщения или, документа, то зашифрование производится открытым ключом, а расшифрование такого сообщения возможно только закрытым ключом его владельца.

Товарищество с ограниченной ответственностью «Удостоверяющий центр «Казахстан» и указывается в заявлениях и регистрационных свидетельствах открытого ключа электронной цифровой подписи **для ограничения юридической силы документов, подписанных (удостоверенных) электронной цифровой подписи.**

Средства криптографической защиты информации (СКЗИ) - любые средства, алгоритмы и методы преобразования информации с целью сокрытия ее содержания и/или обеспечения аутентификации, использующие криптографические ключи, включая средства изготовления этих ключей.

Криптографические ключи - параметры процесса преобразования информации с целью сокрытия ее содержания и/или обеспечения аутентификации, которые, или часть которых, содержатся в секрете;

Зашифрование данных - процесс преобразования исходных данных в зашифрованные, с целью сокрытия их содержания, использующий криптографические ключи.

Расшифрование данных - процесс преобразования зашифрованных данных в исходные, использующий криптографические ключи.

Шифрование данных - зашифрование и/или расшифрование данных.

Ключи шифрования - криптографические ключи, используемые для шифрования данных.

Компрометация ключа – констатация лицом, владеющим закрытым (секретным) ключом электронной подписи и/или шифрования, обстоятельств, при которых возможно несанкционированное использование данного ключа неуполномоченными лицами.

Подписывающее лицо - физическое или юридическое лицо, правомерно владеющее закрытым ключом электронной цифровой подписи и обладающее правом на ее использование на электронном документе.

Средства электронной цифровой подписи - совокупность программных и технических средств, используемых для создания и проверки подлинности электронной цифровой подписи;

Удостоверяющий центр (Центр) - Товарищество с ограниченной ответственностью «Удостоверяющий центр «Казахстан», действующее на основании лицензии дающй право на предоставление услуг удостоверения соответствия открытого ключа ЭЦП закрытому ключу ЭЦП, а так же подтверждения регистрационного свидетельства (АБА № 002073 от 08.06.2009г.) и обладающее сертифицированной технологией выпуска криптографических ключей и правами их распространения - лицензия на разработку и реализацию СКЗИ (СК № 017 от 13.11.2008г.)

Уполномоченный орган - государственный орган, осуществляющий реализацию государственной политики и государственное регулирование деятельности в сфере информатизации;

Участник системы электронного документооборота (Участник) - физическое или юридическое лицо, государственный орган или должностное лицо, участвующие в процессах сбора, обработки, хранения, передачи, поиска и распространения электронных документов с наделёнными Удостоверяющим центром правами заявлять Владельцев регистрационного свидетельства. Участник системы электронного документооборота – физическое лицо является Владельцем регистрационного свидетельства по умолчанию.

Корпоративная система электронного документооборота - система электронного документооборота, участниками которой может быть ограниченный круг организаций или пользователей, определяемый ведомственными, функциональными или иными информационными отношениями.

Система электронного документооборота на портале «doc.e-kz.com» (Система)– система электронного документооборота, представляющая собой совокупность программного, информационного и аппаратного обеспечения, обеспечивающая обмен электронными документами между Участниками в рамках их

гражданско-правовой деятельности и призванная автоматизировать и частично заменить существующий бумажный документооборот между ними. Адрес информационного сервера Системы - https://doc.e-kz.com.

III. **Условия получения ЭЦП и регистрации в Системе**

3. Центр, используя СКЗИ, создает и сохраняет закрытый и открытый ключи для ЭЦП. Выбор формы и масштаба[4] использования и хранения ключей ЭЦП оговариваются в договоре между Участниками и Центром.

4. Объем полномочий, которые могут быть предоставлены уполномоченным лицам Участника, зарегистрированных Центром, как Владельцы регистрационных свидетельств, при осуществлении электронного документооборота в Системе определяются условиями договора между Центром и Участником, либо заявлениями, оформленными в соответствии с образцами, опубликованными на сайте www.e-kz.com.

5. Участник допускается к осуществлению электронного документооборота в Системе после выполнения им одного следующих условий:

5.1. обращение Участника в Центр для заключения договора об оказании удостоверяющих и сопутствующих услуг, что позволяет Участнику и/или его уполномоченным лицам получить Регистрационное свидетельство и защищённые носители Открытого и Закрытого ключей ЭЦП;

5.2. подписание заявления Заявление на изготовление ключей и регистрационного свидетельства и/или регистрацию регистрационного свидетельства, согласно образцам опубликованных на портале http://www.e-kz.com, https://doc.e-kz.com, а также предусмотренных договорами с Центром. и поданные в том числе через организации - участников ЭДО на портале https://doc.e-kz.com.

6. Допускается подача Заявлений на изготовление ключей и регистрационного свидетельства и/или регистрацию регистрационного свидетельства, согласно образцам опубликованных на портале http://www.e-kz.com, https://doc.e-kz.com доверенными лицами на основании доверенности или имеющихся у них регистрационных свидетельств (для случаев подачи заявления в форме электронного документа) с указанием следующих полномочий:

1) запросить изготовление ключей электронной цифровой подписи и регистрационное свидетельство открытого ключа электронной цифровой подписи;
2) запросить регистрацию на открытый ключ электронной цифровой подписи, указанный в регистрационном свидетельстве (указывается реквизиты свидетельства), выданного (указывается название выдавшего удостоверяющего центра) и выдачу регистрационного свидетельства открытого ключа электронной цифровой подписи;
3) отозвать (аннулировать) регистрационное свидетельство (указывается реквизиты свидетельства), зарегистрированного (выданного) (указывается название выдавшего удостоверяющего центра).
4) запросить объектные идентификаторы (OID) или приостановить действие OID на имеющиеся у заявителя объекты делопроизводства (номенклатуры дел, должностей, структур и т.п.).

7. Передача ключей ЭЦП производится только лицу, указанному в Заявлении на изготовление ключей и регистрационного свидетельства и/или регистрацию регистрационного свидетельства без доверенности по предъявлению удостоверения

[4] Масштаб использования ЭЦП мера ответственности, при использовании ЭЦП, подтверждаемая Центром в пределах объектных идентификаторов (OID) для Владельца регистрационного свидетельства. Такая мера запрашивается в заявлении на получение средств и ключей ЭЦП!.

личности, либо по доверенности на получение товарно-материальных ценностей с указанием Регистрационных свидетельств на получаемы средства и ключи ЭЦП.

IV. **Использование ЭЦП через Систему или иные информационные системы;**

8. В соответствии с настоящими Правилами для подтверждения подлинности и авторства электронных документов, применяется ЭЦП. Удостоверяющим центром предоставляются только средства формирования ЭЦП.

9. Участники и Подписывающие лица самостоятельно определяют технологии использования подготовки электронного документа для формирования ЭЦП при помощи средств, полученных от Центра.

10. Основными условиями использования ЭЦП являются:

10.1. возможность участников документооборота принимать/пересылать электронные документы и проверять электронную цифровую подпись;

10.2. договорённости сторон о реквизитах электронных адресов получения электронных документов;

10.3. признание того, что переданная/полученная информация в Системе является удостоверенной (Центром) по времени и авторству и является подлинной;

10.4. использование электронных устройств (картридеры, е-токены и т.п.), а также специального программного обеспечения, полученного от Центра, через сотрудников центра, непосредственно с портала: http://www.e-kz.com, https://doc.e-kz.com;

10.5. наличие выхода в сеть Интернет персонального компьютера или иного телекоммуникационного устройства для типов которых которого Центром предоставлены необходимые программно-технические компоненты, через которые Владелец регистрационного свидетельства намеревается сформировать электронный документ/сообщение;

10.6. выход на официальный сайт Системы www.e-kz.com, для инициализации электронных устройств, и загрузки программных компонентов, указанных в п. 10.1, следуя представленным на сайте инструкциям;

11. Дополнительными условиями использования ЭЦП для автоматизации и оптимизации собственного делопроизводства[5], по отдельным договорам является установка Участнику Системы аккредитованными[6] Центром организациями необходимых аппаратных средств, клиентского программного обеспечения электронного документооборота и платежей при использовании ЭЦП и Системы;

12. Для подтверждения юридической значимости электронного документа, подписанного ЭЦП, введенного в обращение в соответствии с Правилами, по обращению заинтересованной стороны через Систему, Центр подтверждает следующие свойства:

12.1. отсутствия изменений в электронном документе во время пересылки адресату;

12.2. подтверждение Владельца регистрационного свидетельства и его ЭЦП при помощи, которой подписан электронный документ.

13. Подлинность электронного документа может быть удостоверена только Центром. ЭЦП неразрывно связана с конкретным документом и только с ним!

14. Защита электронного документа обеспечивает СКЗИ а именно:

[5] Системы корпоративного электронного документооборота, бухгалтерского, кадрового и материального учёта с использованием ЭЦП и т.п.

[6] Аккредитованные организации- организации, состоящие в договорных отношениях с Центром и имеющие соответствующие полномочия на предоставление компонентов использования средств ЭЦП и Системы.

14.1. предотвращение несанкционированного доступа к электронному документу;

14.2. расшифрование электронного документа;

14.3. зашифрование электронного документа.

15. Центр и Участники системы признают и согласны с тем, что использование документов в электронной форме, заверенных ЭЦП с использованием Системы, юридически равнозначно использованию соответствующих документов на бумажных носителях, оформленных собственноручными подписями уполномоченных лиц сторон.

V. **Период действия Правил и порядок внесения в них изменений**

16. Условия Правил являются обязательными для Участника с момента подписания им договора о присоединении к Системе или подписания документа, имеющего ссылку на Правила или подачи заявления в соответствии с п. 5 Правил.

17. Изменения и дополнения в настоящие Правила могут вноситься Центром в силу необходимости и целесообразности для расширения дополнительных условий использования ЭЦП Участникам Системы.

18. Изменения и дополнения в настоящие Правила доводятся до сведения Участника посредством опубликовании электронных документов на портале http://www.e-kz.com.

19. Центр в праве прекратить предоставление услуг доступа к Системе, а также удостоверяющих услуг по подтверждению соответствия закрытого ключа открытому для использования Владельцами регистрационных свидетельств Участника при подписании электронных документов и/или электронных платёжных документов в случае получения информации о компрометации закрытого ключа ЭЦП и/или нарушения порядка и сроков оплаты Участником услуг Центра.

VI. **Требования к информационной безопасности**

20. Центр и Участник обязуются предпринять все разумные меры для обеспечения сохранности своих закрытых ключей посредством применения программно-технических средств и организационных мер.

21. Участник обязан эксплуатировать программное обеспечение Системы в соответствии с техническими требованиями, инструкциями и только для связи с определенными в этих документах серверами Системы. Безопасность и надежность передачи и обработки данных связана не только с использованием ЭЦП, но и строго определенного программного обеспечения и адресов, по которым происходит информационное взаимодействие между Участником и Центром.

22. Перечень критических событий, связанных с нарушением информационной безопасности в Системе:

22.1. потеря контроля доступа к ключам;

22.2. потеря контроля над программным обеспечением для генерации ключей;

22.3. увольнение, перевод на другое место работы сотрудника, имевшего доступ к ключам;

22.4. другие события, влияющие на безопасность электронного документооборота в Системе.

23. При возникновении критического события Участник или любой заявленный им Владелец Регистрационного свидетельства обязан уведомить об этом Центр. Заявление владельца об отзыве (аннулировании) регистрационного свидетельства может быть подано им на бумажном носителе или в форме электронного документа по форме

согласно образцам, опубликованным на порталах http://www.e-kz.com, https://doc.e-kz.com. При наличии у заявителя действующей электронной цифровой подписи, заявление об отзыве (аннулировании), регистрационного свидетельства, может быть представлено в форме электронного документа. При этом сведения, содержащиеся в заявлении, подтверждаются действующей электронной цифровой подписью заявителя.

24. Исполнение заявок отзыва регистрационных свидетельств осуществляется Центром с 9 до 22 часов в течение одного часа после получения сообщения от Участника. Результатом исполнения заявки является прекращение проведения, каких бы то ни было операций с использованием скомпрометированного ключа, и опубликование (обновление) на сайте http://www.e-kz.com сведений об отозванных (аннулированных) регистрационных свидетельствах, с момента чего ключи ЭЦП считаются недействительными. ЭЦП документов, доступ в Систему с момента блокирования указанного ключа, считается недействительной.

25. В случае, если Участник обладает доступом к программному обеспечению электронного документооборота Центра по администрированию процессов электронного документооборота, то Участник имеет возможность самостоятельно осуществлять блокирование скомпрометированных ключей заявленных им Владельцев регистрационных свидетельств.

26. Центр обязуется немедленно уведомлять Участника обо всех неправильно произведенных операциях и о потере контроля над программным обеспечением и носителями криптографических ключей по реквизитам, указанным в подписанных между Участником и Центром договорах или, указанных в заявления, следствием, которых стало присоединение к настоящим Правилам. В противном случае Участник не несет ответственности за проведенные операции.

27. После получения уведомления о компрометации Участник не должен использовать скомпрометированные ключи электронной подписи и/или шифрования при выполнении проверки подлинности электронных документов, полученных после уведомления о компрометации, а также для шифрования новых электронных документов.

VII. **Порядок разрешения конфликтных ситуаций**

28. В случае возникновения споров о подлинности электронных документов, подписанных ЭЦП, применяется процедура согласования разногласий, предусмотренная настоящим Разделом Правил.

29. Бремя доказывания лежит на стороне, заявившей о нарушении ее прав и законных интересов.

30. Если одна из сторон утверждает, что документ подписан ЭЦП, а другая эту ЭЦП не признает, в 5-дневный срок путем обмена письмами стороны создают Согласительную комиссию. Полномочия членов Согласительной комиссии подтверждаются доверенностями. Члены Согласительной комиссии равноправны.

31. Если стороны не договорятся об ином, в состав Согласительной комиссии входит равное количество представителей каждой из конфликтующих сторон, но не менее, чем по одному уполномоченному представителю.

32. В состав Согласительной комиссии, как правило, назначаются специалисты из числа сотрудников технических служб или служб информационной безопасности сторон. Лица, входящие в состав Согласительной комиссии, должны обладать необходимыми знаниями в области построения системы криптозащиты, работы компьютерных информационных систем.

33. По инициативе любой из сторон к работе Согласительной комиссии для проведения технической экспертизы могут привлекаться независимые эксперты, соответствующие требованиям, указанным в п. 32 настоящих Правил, в том числе и разработчики Системы, средств криптографической защиты информации. Сторона, привлекающая независимых экспертов, самостоятельно решает вопрос об оплате экспертных услуг.

34. Стороны обязаны в 2-дневный срок после создания Согласительной комиссии предоставить в Согласительную комиссию следующие материалы:

1) изъятый в присутствии представителей сторон или одного из независимых экспертов, контрольный экземпляр программного обеспечения, предназначенного для использования ключей ЭЦП;
2) сторона, оспаривающая подлинность подписи, предоставляет подписанный ЭЦП спорный электронный документ в виде файла;
3) контрольное средство хранения и использования ключей ЭЦП.

35. Для проверки подлинности электронного документа со спорной ЭЦП Согласительная комиссия производит следующие действия:

35.1. Сравнивает открытые ключи ЭЦП, предоставленные сторонами. Верным признается экземпляр открытого ключа, комплиментарный закрытому ключу ЭЦП стороны, подлинность ЭЦП которой оспаривается.

35.2. Сравнивает экземпляры программного обеспечения сторон, предназначенного для хранения и использования ЭЦП, с контрольным экземпляром.

35.3. Проверяет правильность ЭЦП под спорным документом, используя контрольный экземпляр программы, предназначенной для проверки ЭЦП.

36. Результаты работы Согласительной комиссии отражаются в акте, который подписывается всеми членами комиссии. Члены комиссии, не согласные с выводами большинства, подписывают указанный акт с возражениями, которые прилагаются к нему. Акт составляется в таком количестве экземпляров, чтобы каждая из конфликтующих сторон имела по одному подлинному экземпляру акта. По требованию члена комиссии ему может быть выдана заверенная копия акта.

37. ЭЦП признается фальшивой или подлинной в зависимости от результатов проверки. Согласительная комиссия делает вывод о причинах возникновения разногласий и определяет виновную сторону.

38. Акт Согласительной комиссии является основанием для предъявления требований к виновной стороне.

39. Акт Согласительной комиссии может быть представлен в качестве доказательства в случае разбирательства спора в судебных органах.

40. Порядок определения подлинности электронного документа и ЭЦП, установленный настоящими Правилами, обязателен для Согласительной комиссии.

41. В случае уклонения какой-либо из сторон от создания Согласительной комиссии, другие стороны вправе самостоятельно назначить трех независимых экспертов для дачи заключения по вопросу подлинности спорной ЭЦП.

42. Письменное заключение экспертов составляется в таком количестве экземпляров, чтобы каждая из конфликтующих сторон имела по одному подлинному экземпляру.

43. Заключение экспертов может быть представлено в качестве доказательства в случае разбирательства спора в судебных органах.

44. Расходы по проведению согласительной процедуры возлагаются на сторону, заявившую о нарушении ее прав и законных интересов.

45. В случае признания требований стороны, заявившей о нарушении ее прав и законных интересов, правомерными, виновная сторона обязана, в течение 5 (пяти) рабочих дней со дня, следующего за днем составления акта Согласительной комиссией или вынесения заключения экспертами, возместить другой стороне убытки.

VIII. **Иные положения**

46. Участники несут ответственность за действия своих сотрудников, уполномоченных Пользователей ключей, а также иных лиц, получивших или имеющих доступ (независимо от того, был ли этот доступ прямо санкционирован Участником или произошел помимо его воли) к аппаратным средствам, программному, информационному обеспечению, криптографическим ключам и иным средствам, обеспечивающим электронный документооборот в соответствии с настоящими Правилами, как за свои собственные.