

**О внесении изменений в приказ исполняющего обязанности Министра
по инвестициям и развитию Республики Казахстан от 26 июня 2015 года № 727 "Об утверждении Правил выдачи, хранения, отзыва регистрационных свидетельств и подтверждения принадлежности и действительности открытого ключа электронной цифровой подписи корневым удостоверяющим центром Республики Казахстан, удостоверяющим центром государственных органов и национальным удостоверяющим центром Республики Казахстан"**

Приказ Министра по инвестициям и развитию Республики Казахстан от 9 декабря 2015 года № 1183. Зарегистрирован в Министерстве юстиции Республики Казахстан 29 февраля 2016 года № 13336

      В соответствии с подпунктом 1) статьи 43-1 Закона Республики Казахстан от 24 марта 1998 года «О нормативных правовых актах» **ПРИКАЗЫВАЮ:**  
      1. Внести в приказ исполняющего обязанности Министра по инвестициям и развитию Республики Казахстан от 26 июня 2015 года № 727 «Об утверждении Правил выдачи, хранения, отзыва регистрационных свидетельств и подтверждения принадлежности и действительности открытого ключа электронной цифровой подписи корневым удостоверяющим центром Республики Казахстан, удостоверяющим центром государственных органов и национальным удостоверяющим центром Республики Казахстан» (зарегистрированный в Реестре государственной регистрации нормативных правовых актов за № 12181, опубликованный 29 октября 2015 года в информационно-правовой системе «Әділет») следующие изменения:  
      в название вносится изменение на государственном языке, текст на русском языке не меняется;  
      преамбулу изложить в следующей редакции:  
      «В соответствии с подпунктом 12) пункта 1 статьи 5 Закона Республики Казахстан от 7 января 2003 года «Об электронном документе и электронной цифровой подписи», **ПРИКАЗЫВАЮ**:»;  
      в Правилах выдачи, хранения, отзыва регистрационных свидетельств и подтверждения принадлежности и действительности открытого ключа электронной цифровой подписи корневым удостоверяющим центром Республики Казахстан, утвержденных указанным приказом:  
      пункт 1 изложить в следующей редакции:  
      «1. Настоящие Правила выдачи, хранения, отзыва регистрационных свидетельств и подтверждения принадлежности и действительности открытого ключа электронной цифровой подписи корневым удостоверяющим центром Республики Казахстан (далее - Правила) разработаны в соответствии с подпунктом 12) пункта 1 статьи 5 Закона Республики Казахстан от 7 января 2003 года «Об электронном документе и электронной цифровой подписи» (далее - Закон), и определяют порядок выдачи, хранения, отзыва регистрационных свидетельств и подтверждения принадлежности и действительности открытого ключа электронной цифровой подписи корневым удостоверяющим центром Республики Казахстан.»;  
      пункт 8 изложить в следующей редакции:  
      «8. КУЦ РК отказывает удостоверяющему центру в выдаче регистрационного свидетельства в следующих случаях:  
      1) неполноты представленных документов;  
      2) представления недостоверных сведений;  
      3) в соответствии со вступившим в законную силу решением суда;  
      4) недостижения лицом шестнадцатилетнего возраста.  
      Письменный мотивированный ответ об отказе в выдаче регистрационного свидетельства удостоверяющему центру выдается заявителю посредством почтовой или специальной почтовой связью, а также нарочно в течение пятнадцати рабочих дней со дня обращения заявителя в КУЦ РК.»;  
      пункт 13 изложить в следующей редакции:  
      «13. Отзыв регистрационного свидетельства удостоверяющего центра, осуществляется в следующих случаях:  
      1) по требованию владельца регистрационного свидетельства либо его представителя на основании заявления на отзыв регистрационного свидетельства по форме, согласно приложению 4 к настоящим Правилам;  
      2) установления факта предоставления недостоверных сведений при получении регистрационного свидетельства;  
      3) смерти владельца регистрационного свидетельства;  
      4) изменения фамилии, имени или отчества (если оно указано в документе, удостоверяющем личность) владельца регистрационного свидетельства;  
      5) смены наименования, реорганизации, ликвидации юридического лица-владельца регистрационного свидетельства;  
      6) предусмотренных соглашением между удостоверяющим центром и владельцем регистрационного свидетельства;  
      7) по вступившему в законную силу решению суда.»;  
      в Правилах выдачи, хранения, отзыва регистрационных свидетельств и подтверждения принадлежности и действительности открытого ключа электронной цифровой подписи удостоверяющим центром государственных органов Республики Казахстан, утвержденных указанным приказом:  
      пункт 1 изложить в следующей редакции:  
      «1. Настоящие Правила выдачи, хранения, отзыва регистрационных свидетельств и подтверждения принадлежности и действительности открытого ключа электронной цифровой подписи удостоверяющим центром государственных органов Республики Казахстан (далее – Правила) разработаны в соответствии с подпунктом 12) пункта 1 статьи 5 Закона Республики Казахстан от 7 января 2003 года «Об электронном документе и электронной цифровой подписи» (далее – Закон) и определяют порядок выдачи, хранения, отзыва регистрационных свидетельств и подтверждения принадлежности и действительности открытого ключа электронной цифровой подписи удостоверяющим центром государственных органов Республики Казахстан.»;  
      пункт 12 изложить в следующей редакции:  
      «12. УЦ ГО отказывает в выдаче регистрационного свидетельства в следующих случаях если:  
      1) неполноты представленных документов;  
      2) представления недостоверных сведений;  
      3) в соответствии со вступившим в законную силу решением суда;  
      4) недостижения лицом шестнадцатилетнего возраста.»;  
      пункт 18 изложить в следующей редакции:  
      «18. Оператор УЦ ГО отзывает регистрационное свидетельство:  
      1) по требованию владельца регистрационного свидетельства либо его представителя на основании письма на отзыв регистрационного свидетельства, согласно приложению 4 к настоящим Правилам;  
      2) установления факта предоставления недостоверных сведений при получении регистрационного свидетельства;  
      3) смерти владельца регистрационного свидетельства;  
      4) изменения фамилии, имени или отчества (если оно указано в документе, удостоверяющем личность) владельца регистрационного свидетельства;  
      5) смены наименования, реорганизации, ликвидации юридического лица-владельца регистрационного свидетельства;  
      6) предусмотренных соглашением между удостоверяющим центром и владельцем регистрационного свидетельства;  
      7) по вступившему в законную силу решению суда.»;  
      Правила выдачи, хранения, отзыва регистрационных свидетельств и подтверждения принадлежности и действительности открытого ключа электронной цифровой подписи национальным удостоверяющим центром Республики Казахстан, утвержденные указанным приказом, изложить в новой редакции согласно приложению к настоящему приказу.  
      2. Комитету связи, информатизации и информации Министерства по инвестициям и развитию Республики Казахстан (Қазанғап Т.Б.) обеспечить:  
      1) государственную регистрацию настоящего приказа в Министерстве юстиции Республики Казахстан;  
      2) в течение десяти календарных дней после государственной регистрации настоящего приказа в Министерстве юстиции Республики Казахстан направление его копии в печатном и электронном виде на официальное опубликование в периодических печатных изданиях и информационно-правовой системе «Әділет», а также в Республиканский центр правовой информации для внесения в эталонный контрольный банк нормативных правовых актов Республики Казахстан;  
      3) размещение настоящего приказа на интернет-ресурсе Министерства по инвестициям и развитию Республики Казахстан и на интранет-портале государственных органов;  
      4) в течение десяти рабочих дней после государственной регистрации настоящего приказа в Министерстве юстиции Республики Казахстан представление в Юридический департамент Министерства по инвестициям и развитию Республики Казахстан сведений об исполнении мероприятий, предусмотренных подпунктами 1), 2) и 3) пункта 2 настоящего приказа.  
      3. Контроль за исполнением настоящего приказа возложить на курирующего вице-министра по инвестициям и развитию Республики Казахстан.  
      4. Настоящий приказ вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования.

*Министр*  
*по инвестициям и развитию*  
*Республики Казахстан                       А. Исекешев*

*«СОГЛАСОВАН»*  
*Министр финансов*  
*Республики Казахстан*  
*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Б. Султанов*  
*26 января 2016 года*

*«СОГЛАСОВАН»*  
*Министр культуры и спорта*  
*Республики Казахстан*  
*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_А. Мухамедиулы*  
*28 января 2016 года*

*«СОГЛАСОВАН»*  
*Министр иностранных дел*  
*Республики Казахстан*  
*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Е. Идрисов*  
*19 январь 2016 года*

Приложение          
к приказу Министра      
по инвестициям и развитию  
Республики Казахстан     
от 9 декабря 2015 года № 1183

Приложение 3        
к приказу исполняющего   
обязанности Министра    
по инвестициям и развитию  
Республики Казахстан     
от 26 июня 2015 года № 727

**Правила**  
**выдачи, хранения, отзыва регистрационных свидетельств**  
**и подтверждения принадлежности и действительности**  
**открытого ключа электронной цифровой подписи национальным**  
**удостоверяющим центром Республики Казахстан 1. Общие положения**

      1. Настоящие Правила выдачи, хранения, отзыва регистрационных свидетельств и подтверждения принадлежности и действительности открытого ключа электронной цифровой подписи национальным удостоверяющим центром Республики Казахстан (далее – Правила) разработаны в соответствии с подпунктом 12) пункта 1 статьи 5 Закона Республики Казахстан от 7 января 2003 года «Об электронном документе и электронной цифровой подписи» (далее – Закон) и определяют порядок выдачи, хранения, отзыва регистрационных свидетельств и подтверждение принадлежности и действительности открытого ключа электронной цифровой подписи национальным удостоверяющим центром Республики Казахстан.  
      2. В настоящих Правилах используются следующие понятия:  
      1) объектный идентификатор (далее – OID) – уникальный набор цифр, который связан с объектом и однозначно идентифицирует его в мировом адресном пространстве объектов;  
      2) средство криптографической защиты информации (далее – СКЗИ) – средство, реализующее алгоритмы криптографических преобразований, генерацию, формирование, распределение или управление ключами;  
      3) отозванное регистрационное свидетельство – регистрационное свидетельство, аннулированное в порядке, установленном настоящими Правилами;  
      4) список отозванных регистрационных свидетельств (далее – СОРС) – часть регистра регистрационных свидетельств, содержащая сведения о регистрационных свидетельствах, действие которых прекращено, их серийные номера, дату и причину отзыва;  
      5) национальный удостоверяющий центр Республики Казахстан (далее – НУЦ) – удостоверяющий центр, обслуживающий участников «электронного правительства», государственных и негосударственных информационных систем;  
      6) заявитель – физическое или юридическое лицо, подавшее документы на выдачу или отзыв регистрационного свидетельства;  
      7) регистрационное свидетельство – документ на бумажном носителе или электронный документ, выдаваемый удостоверяющим центром для подтверждения соответствия электронной цифровой подписи требованиям, установленным Законом;  
      8) владелец регистрационного свидетельства – физическое или юридическое лицо, на имя которого НУЦ выдано регистрационное свидетельство, правомерно владеющее закрытым ключом, соответствующим открытому ключу, указанному в регистрационном свидетельстве;  
      9) участник системы электронного документооборота – физическое или юридическое лицо, государственный орган или должностное лицо, участвующие в процессах сбора, обработки, хранения, передачи, поиска и распространения электронных документов;  
      10) система электронного документооборота (далее – СЭД) – система обмена электронными документами, отношения между участниками которой регулируются Законом и иными нормативными правовыми актами Республики Казахстан;  
      11) электронная цифровая подпись (далее – ЭЦП) – набор электронных цифровых символов, созданный средствами электронной цифровой подписи и подтверждающий достоверность электронного документа, его принадлежность и неизменность содержания;  
      12) средства ЭЦП – совокупность программных и технических средств, используемых для создания и проверки подлинности ЭЦП.  
      3. Регистрационные свидетельства выдаются физическим и юридическим лицам, в том числе владельцам доменного имени интернет-ресурса, участникам информационной системы «Казначейство – клиент», физическим и юридическим лицам иностранных государств.

**2. Порядок выдачи регистрационных свидетельств заявителю НУЦ**

      4. Для получения регистрационных свидетельств физические лица Республики Казахстан предоставляют в НУЦ следующие документы:  
      1) заявление на выдачу регистрационных свидетельств НУЦ (от физического лица) по форме, согласно приложению 1 к настоящим Правилам на бумажном носителе, полученное с веб-портала «электронного правительства» www.egov.kz (далее – портал) или интернет-ресурс www.pki.gov.kz (далее – интернет-ресурс);  
      2) документ, удостоверяющий личность заявителя, содержащий индивидуальный идентификационный номер (далее – ИИН) заявителя;  
      3) доверенность на представителя физического лица, удостоверенную нотариально, с указанием полномочия представлять документы на выдачу регистрационных свидетельств НУЦ и расписываться в соответствующих документах для исполнения поручения, определенного доверенностью – при представлении интересов физического лица третьим лицом.  
      5. Для получения регистрационных свидетельств индивидуальные предприниматели, осуществляющие деятельность в виде совместного предпринимательства, предоставляют в НУЦ следующие документы:  
      1) заявление на выдачу регистрационных свидетельств НУЦ (от юридического лица и индивидуального предпринимателя, осуществляющего деятельность в виде совместного предпринимательства) по форме, согласно приложению 2 к настоящим Правилам на бумажном носителе, полученное с портала или интернет-ресурса и содержащее уникальный номер;  
      2) документ, удостоверяющий личность представителя заявителя, содержащий ИИН заявителя;  
      3) доверенность на представителя физического лица, удостоверенную нотариально, с указанием полномочия представлять документы на выдачу регистрационных свидетельств НУЦ и расписываться в соответствующих документах для исполнения поручения, определенного доверенностью – при представлении интересов физического лица третьим лицом;  
      4) для проверки данных указанных в заявлении заявитель предоставляет справку или свидетельство (при наличии) о государственной регистрации индивидуального предпринимателя – для индивидуального предпринимателя, осуществляющего деятельность в виде совместного предпринимательства.  
      6. Для получения регистрационных свидетельств юридические лица Республики Казахстан предоставляют в НУЦ следующие документы:  
      1) заявление на выдачу регистрационных свидетельств НУЦ (от юридического лица и индивидуального предпринимателя, осуществляющего деятельность в виде совместного предпринимательства) по форме, согласно приложению 2 к настоящим Правилам на бумажном носителе, полученное с портала или интернет-ресурса и содержащее уникальный номер;  
      2) документ, удостоверяющий личность представителя заявителя, содержащий ИИН заявителя;  
      3) доверенность на разовое получение или отзыв регистрационных свидетельств НУЦ от юридического лица, по форме, согласно приложению 3 к настоящим Правилам на бумажном носителе;  
      4) для проверки данных указанных в заявлении заявитель предоставляет справку или свидетельство (при наличии) о государственной регистрации юридического лица, содержащий бизнес-идентификационный номер (далее – БИН) юридического лица или их копии;  
       Для получения регистрационных свидетельств на сотрудника юридического лица до обращения в НУЦ, первый руководитель юридического лица или лицо, исполняющего его обязанности посредством интернет-ресурса подтверждает поданную сотрудником юридического лица заявку на выдачу регистрационных свидетельств путем удостоверения ее своей электронной цифровой подписью.  
      Для первого руководителя юридического лица или лица, исполняющего его обязанности, взамен доверенности представляется справка с места работы либо заверенная печатью юридического лица (при ее наличии) копия приказа (решения, протокола) о назначении на должность первого руководителя или лица, исполняющего его обязанности.  
      7. Для получения регистрационных свидетельств владелец доменного имени интернет-ресурса (физическое лицо) предоставляет в НУЦ следующие документы:  
      1) заявление на выдачу SSL регистрационного свидетельства НУЦ (от физического лица) по форме, согласно приложению 4 к настоящим Правилам на бумажном носителе, полученное с портала или интернет-ресурса и содержащее уникальный номер;  
      2) документ, удостоверяющий личность заявителя, содержащий ИИН заявителя;  
      3) доверенность на представителя физического лица, удостоверенную нотариально, с указанием полномочия представлять документы на выдачу регистрационных свидетельств НУЦ и расписываться в соответствующих документах для исполнения поручения, определенного доверенностью – при представлении интересов физического лица третьим лицом;  
      4) один из подтверждающих документов на право владения доменным именем интернет-ресурса на бумажном носителе:  
      сертификат о владении доменным именем, выданным Казахстанским центром сетевой информации;  
      выписку из WHOIS (поиск доменного имени.KZ и.ҚАЗ).  
      8. Для получения регистрационных свидетельств владелец доменного имени интернет-ресурса (юридическое лицо) предоставляет в НУЦ следующие документы:  
      1) заявление на выдачу SSL регистрационного свидетельства НУЦ (от юридического лица) по форме, согласно приложению 5 к настоящим Правилам на бумажном носителе, полученное с портала или интернет-ресурса и содержащее уникальный номер;  
      2) документ, удостоверяющий личность представителя заявителя, содержащий ИИН заявителя;  
      3) доверенность на разовое получение или отзыв регистрационных свидетельств НУЦ от юридического лица, по форме, согласно приложению 3 к настоящим Правилам на бумажном носителе;  
      4) один из подтверждающих документов на право владения доменным именем интернет-ресурса на бумажном носителе:  
      сертификат о владении доменным именем, выданным Казахстанским центром сетевой информации;  
      выписку из WHOIS (поиск доменного имени.KZ и.ҚАЗ).  
      9. Для получения регистрационных свидетельств участники информационной системы «Казначейство – клиент» предоставляют в НУЦ следующие документы:  
      1) заявление на выдачу регистрационных свидетельств НУЦ (от юридического лица для пользователей ИС «Казначейство-Клиент») по форме, согласно приложению 6 к настоящим Правилам на бумажном носителе, полученное с портала или интернет-ресурса и содержащее уникальный номер;  
      2) документ, удостоверяющий личность представителя заявителя, содержащий ИИН заявителя;  
      3) соглашение либо дополнительное соглашение об использовании ЭЦП между Комитетом казначейства Министерства финансов Республики Казахстан и клиентом на бумажном носителе (если дата подписания соглашения и дата предоставления соглашения либо дополнительного соглашения в НУЦ превышает три рабочих дня, исключая день подписания соглашения (дополнительного соглашения), то данное соглашения отклоняется);  
      4) доверенность на разовое получение или отзыв регистрационных свидетельств НУЦ от юридического лица, по форме, согласно приложению 3 к настоящим Правилам на бумажном носителе – при представлении интересов заявителя третьим лицом.  
      10. Для получения регистрационных свидетельств физические лица иностранных государств предоставляют в НУЦ следующие документы:  
      1) заявление на выдачу регистрационных свидетельств НУЦ (от физического лица) по форме, согласно приложению 1 к настоящим Правилам на бумажном носителе, полученное с портала или интернет-ресурса и содержащее уникальный номер;  
      2) документ, удостоверяющий личность заявителя;  
      3) один из документов, содержащий ИИН и подтверждающий, что данное физическое лицо иностранного государства зарегистрировано на территории Республики Казахстан:  
      вид на жительство иностранца в Республике Казахстан;  
      удостоверение лица без гражданства;  
      регистрационное свидетельство для иностранцев;  
      4) доверенность на представителя физического лица, удостоверенную нотариально, с указанием полномочия представлять документы на выдачу регистрационных свидетельств НУЦ и расписываться в соответствующих документах для исполнения поручения, определенного доверенностью – при представлении интересов физического лица третьим лицом.  
      11. Для получения регистрационных свидетельств юридические лица иностранных государств предоставляют в НУЦ следующие документы:  
      1) заявление на выдачу регистрационных свидетельств НУЦ (от юридического лица и индивидуального предпринимателя, осуществляющего деятельность в виде совместного предпринимательства) по форме, согласно приложению 2 к настоящим Правилам на бумажном носителе, полученное с портала или интернет-ресурса содержащее уникальный номер;  
      2) документ, удостоверяющий личность представителя заявителя;  
      3) один из документов, содержащий ИИН и подтверждающий, что данный гражданин иностранного государства зарегистрирован на территории Республики Казахстан:  
      вид на жительство иностранца в Республике Казахстан;  
      удостоверение лица без гражданства;  
      регистрационное свидетельство для иностранцев;  
      4) один из документов, содержащий БИН и подтверждающий, что данное юридическое лицо иностранного государства зарегистрировано на территории Республики Казахстан:  
      справку или свидетельство (при наличии) об учетной регистрации (перерегистрации) филиала, представительства – для юридических лиц-нерезидентов, осуществляющих деятельность в Республике Казахстан через филиалы и представительства (с образованием постоянного учреждения);  
      регистрационное свидетельство для юридических лиц-нерезидентов:  
      являющихся налоговыми агентами в соответствии с пунктом 5 статьи 197 Кодекса Республики Казахстан от 10 декабря 2008 года «О налогах и других обязательных платежах в бюджет» (Налоговый кодекс) (далее – Налоговый кодекс);  
      владеющих в Республике Казахстан объектами налогообложения;  
      являющихся дипломатическими и приравненными к ним представительствами иностранного государства, аккредитованными в Республике Казахстан;  
      осуществляющих деятельность через зависимого агента, который рассматривается как его постоянное учреждение согласно пункту 8 статьи 191 Налогового кодекса;  
      осуществляющих деятельность через постоянное учреждение без открытия филиала, представительства;  
      открывающих текущие счета в банках-резидентах;  
      5) доверенность на разовое получение или отзыв регистрационных свидетельств НУЦ от юридического лица, по форме, согласно приложению 3 к настоящим Правилам на бумажном носителе.  
      Для первого руководителя юридического лица или лица, исполняющего его обязанности, взамен доверенности представляется справка с места работы на бумажном носителе, либо заверенная печатью юридического лица копия приказа (решения, протокола) о назначении на должность первого руководителя или лица, исполняющего его обязанности.  
      12. Для получения регистрационных свидетельств на портале или интернет-ресурсе, в случае повторного получения владелец регистрационного свидетельства НУЦ (за исключением участников информационной системы «Казначейство-клиент») подает запрос в форме электронного документа, содержащего открытый (ые) ключ (и) и удостоверенный его ЭЦП.  
      13. НУЦ и владелец регистрационного свидетельства при необходимости для выпуска или отзыва регистрационного свидетельства могут заключить между собой соглашение о выдаче и отзыве регистрационного свидетельства.  
      14. При приеме пакета документов работник НУЦ проверяет представленные документы заявителя на полноту, сверяет данные из информационной системы государственной базы данных «Физические лица» или «Юридические лица» с оригиналами документов заявителя и возвращает оригиналы заявителю.  
      При приеме документов согласно пунктам 4, 5, 6, 7, 8, 9, 10, 11 настоящих Правил, работник НУЦ выдает заявителю расписку о приеме соответствующих документов с указанием:  
      1) номера и даты приема запроса;  
      2) вида запрашиваемой услуги;  
      3) количества и название приложенных документов;  
      4) даты (времени) и места выдачи документов;  
      5) фамилии, имени, отчества работника НУЦ, принявшего запрос на оформление документов;  
      6) фамилии, имени, отчества заявителя или уполномоченного представителя, и их контактные телефоны.  
      Также заявителю направляется уведомление – отчет на адрес электронной почты, указанный в заявлении о принятии запроса для предоставления услуги.  
      15. Выдача заявителю регистрационных свидетельств осуществляется НУЦ в течение одного рабочего дня, после поступления документов согласно пунктам 4, 5, 6, 7, 8, 9, 10 и 11 настоящих Правил.  
      16. Выдача заявителю регистрационных свидетельств на портале или интернет-ресурсе, после поступления запроса в форме электронного документа, содержащего открытые ключи, при наличии у заявителя действующих регистрационных свидетельств осуществляется в течение одного рабочего дня.  
      17. Выдача регистрационного свидетельства осуществляется в форме электронного документа, со структурами регистрационных свидетельств согласно приложению 7 к настоящим Правилам.  
      18. В случае не предоставления заявителем документов, указанных в пунктах 4, 5, 6, 7, 8, 9, 10, 11 настоящих Правил, заявка, поданная заявителем на получение регистрационных свидетельств через портал или интернет-ресурс в форме электронного документа будет отозвана по истечении одного месяца с момента подачи заявки.  
      19. Регистрация регистрационного свидетельства осуществляется путем формирования в регистре регистрационных свидетельств записей (сведений), составляющих содержание регистрационного свидетельства. Для отличительных особенностей НУЦ присваивает регистрационному свидетельству объектный идентификатор (OID).  
      20. Выдача регистрационных свидетельств владельцу производятся в НУЦ путем записи на удостоверение личности, содержащее электронный носитель информации (чип) и (или) на sim-карту содержащую средства криптографической защиты информации, а также через портал или интернет-ресурс.  
      21. НУЦ отказывает в выдаче регистрационного свидетельства в случаях:  
      1) неполноты представленных документов;  
      2) представления недостоверных сведений;  
      3) в соответствии со вступившим в законную силу решением суда;  
      4) недостижения лицом шестнадцатилетнего возраста.  
      В случае технических сбоев в работе портала или интернет-ресурса выдача регистрационных свидетельств приостанавливается до восстановления работы портала или интернет-ресурса.  
      22. Срок действия регистрационного свидетельства составляет один год с момента его выдачи.

**3. Порядок хранения регистрационных свидетельств, выданных НУЦ**

      23. НУЦ обеспечивает хранение копий выданных регистрационных свидетельств в электронной форме.  
      24. Срок хранения отозванных регистрационных свидетельств в регистре регистрационных свидетельств составляет не менее пяти лет.  
      25. По истечении срока, указанного в пункте 24 настоящих Правил, отозванные регистрационные свидетельства поступают на архивное хранение в соответствии с приказом Министра культуры и спорта Республики Казахстан от 26 января 2015 года № 22 «Об утверждении Перечня типовых документов, образующихся в деятельности государственных и негосударственных организаций, с указанием сроков хранения» (зарегистрированный в Реестре государственной регистрации нормативных правовых актов под № 10345).

**4. Порядок отзыва регистрационного свидетельства**

      26. Регистрационное свидетельство отзывается в НУЦ на основании предоставления владельцем регистрационных свидетельств – физического лица Республики Казахстан, физического лица - владельца доменного имени интернет-ресурса, физического лица - нерезидента следующих документов:  
      1) заявление на отзыв регистрационных свидетельств НУЦ от физического лица, физического лица - владельца доменного имени интернет-ресурса, физического лица-нерезидента по форме, согласно приложению 8 к настоящим Правилам на бумажном носителе, полученное с портала или интернет-ресурса;  
      2) документ, удостоверяющий личность владельца регистрационных свидетельств;  
      3) доверенность на представителя физического лица, удостоверенную нотариально, с указанием полномочия представлять документы на отзыв регистрационных свидетельств НУЦ и расписываться в соответствующих документах для исполнения поручения, определенного доверенностью – при представлении интересов физического лица третьим лицом.  
      27. Регистрационное свидетельство отзывается в НУЦ на основании предоставления владельцем регистрационных свидетельств – индивидуального предпринимателя, осуществляющего деятельность в виде совместного предпринимательства Республики Казахстан следующих документов:  
      1) заявление на отзыв регистрационных свидетельств НУЦ от юридического лица, индивидуального предпринимателя, осуществляющего деятельность в виде совместного предпринимательства, юридического лица - владельца доменного имени интернет-ресурса, участника информационной системы «Казначейство-клиент», юридического лица-нерезидента по форме, согласно приложению 9 к настоящим Правилам на бумажном носителе, полученное с портала или интернет-ресурса заверенная печатью юридического лица, либо выписку из приказа об увольнении заявителя. В случае предоставления выписки из приказа об увольнении, подпись руководителя и печать организации не требуется;  
      2) документ, удостоверяющий личность владельца регистрационных свидетельств;  
      3) доверенность на представителя физического лица, удостоверенную нотариально, с указанием полномочия представлять документы на отзыв регистрационных свидетельств НУЦ и расписываться в соответствующих документах для исполнения поручения, определенного доверенностью – при представлении интересов физического лица третьим лицом.  
      28. Регистрационное свидетельство отзывается в НУЦ на основании предоставления владельцем регистрационных свидетельств – юридического лица, юридического лица - владельца доменного имени интернет-ресурса, участника информационной системы «Казначейство-клиент», юридического лица-нерезидента следующих документов:  
      1) заявление на отзыв регистрационных свидетельств НУЦ от юридического лица, индивидуального предпринимателя, осуществляющего деятельность в виде совместного предпринимательства, юридического лица - владельца доменного имени интернет-ресурса, участника информационной системы «Казначейство-клиент», юридического лица-нерезидента по форме, согласно приложению 9 к настоящим Правилам на бумажном носителе, полученное с портала или интернет-ресурса заверенная печатью юридического лица, либо выписку из приказа об увольнении заявителя. В случае предоставления выписки из приказа об увольнении, подпись руководителя и печать организации не требуется;  
      2) документ, удостоверяющий личность владельца регистрационных свидетельств;  
      3) доверенность на разовое получение или отзыв регистрационных свидетельств НУЦ от юридического лица, по форме, согласно приложению 3 к настоящим Правилам на бумажном носителе.  
      29. Регистрационное свидетельство отзывается через портал или интернет-ресурс на основании запроса в форме электронного документа, содержащего открытый (ые) ключ (и) и удостоверенный ЭЦП владельца регистрационного свидетельства.  
      30. Также регистрационное свидетельство отзывается:  
      1) по требованию владельца регистрационного свидетельства либо его представителя;  
      2) установления факта предоставления недостоверных сведений при получении регистрационного свидетельства;  
      3) смерти владельца регистрационного свидетельства;  
      4) изменения фамилии, имени или отчества (если оно указано в документе, удостоверяющем личность) владельца регистрационного свидетельства;  
      5) смены наименования, реорганизации, ликвидации юридического лица-владельца регистрационного свидетельства;  
      6) предусмотренных соглашением между удостоверяющим центром и владельцем регистрационного свидетельства;  
      7) по вступившему в законную силу решению суда.  
      31. В случае технических сбоев в работе портала или интернет-ресурса отзыв регистрационных свидетельств приостанавливается до восстановления работы портала или интернет-ресурса.  
      32. Подтвердив правильность заполнения владельцем регистрационных свидетельств, указанных в пунктах 26, 27, 28 настоящих Правил, своих данных в заявлении, НУЦ вносит записи в регистр регистрационных свидетельств о прекращении действия регистрационного свидетельства с указанием даты, причины и времени отзыва регистрационного свидетельства.  
      33. Отзыв регистрационных свидетельств при обращении в НУЦ, после поступления документов согласно пунктам 26, 27, 28 настоящих Правил осуществляется в течение одного рабочего дня.  
      34. Отзыв регистрационных свидетельств через портал или интернет-ресурс после поступления запроса в форме электронного документа содержащий открытый (ые) ключ (и), при наличии у владельца действующих регистрационных свидетельств осуществляется в течение одного рабочего дня.  
      При этом сведения, содержащиеся в заявлении, подтверждаются действующей ЭЦП владельца регистрационных свидетельств.  
      35. НУЦ опубликовывает в сети Интернет сведения об отозванных регистрационных свидетельствах, их серийные номера, дату и причину отзыва в СОРС.

**5. Порядок подтверждения принадлежности и действительности**  
**открытого ключа электронной цифровой подписи**

      36. Подтверждение принадлежности и действительности открытого ключа ЭЦП осуществляется участником СЭД или информационной системой, в случае ее наличия, при обмене электронными документами между участниками СЭД.  
      37. Участник СЭД при получении электронного документа, содержащего регистрационное свидетельство подписывающей стороны, осуществляет его проверку на подтверждение принадлежности и действительности открытого ключа ЭЦП путем:  
      проверки регистрационного свидетельства подписывающей стороны;  
      проверки ЭЦП в электронном документе.  
      38. Проверка регистрационного свидетельства на действительность подписывающей стороны осуществляется путем выполнения следующих проверок с использованием СКЗИ НУЦ:  
      проверка построения корректной цепочки от проверяемого регистрационного свидетельства до доверенного корневого регистрационного свидетельства удостоверяющего центра, с учетом промежуточных регистрационных свидетельств удостоверяющих центров;  
      проверка срока действия регистрационного свидетельства. Проверка сроков действия от проверяемого регистрационного свидетельства до доверенного корневого регистрационного свидетельства удостоверяющего центра, с учетом промежуточных регистрационных свидетельств удостоверяющих центров;  
      проверка регистрационного свидетельства на отзыв. Проверка регистрационного свидетельства на отзыв подписывающей стороны осуществляется одним из методов:  
      на основе СОРС НУЦ. Данный метод проверки подтверждает, отозвано ли проверяемое регистрационное свидетельство на момент начала срока действия СОРС НУЦ;  
      онлайн проверка регистрационного свидетельства на отзыв, основанная на протоколе OCSP (On-line Certificate Status Protocol). Данный метод проверки подтверждает, отозвано ли проверяемое регистрационное свидетельство на момент отправки запроса (текущее время);  
      на основе дополнительного СОРС. Данный сервис необходимо использовать совместно с сервисом СОРС, что позволяет получить более актуальную информацию, чем в сервисе СОРС. Данный метод проверки подтверждает, отозвано ли проверяемое регистрационное свидетельство на момент начала срока действия дополнительного СОРС НУЦ.  
      проверка области использования ключа. Проверка заключается в проверке значения поля регистрационного свидетельства «использование ключа» (KeyUsage). Если поле «использование ключа» содержит значения «Цифровая подпись» и «Неотрекаемость», то это регистрационное свидетельство используется для ЭЦП. А если поле «использование ключа» содержит значения «Цифровая подпись» и «Шифрование ключей», то это регистрационное свидетельство используется для аутентификации;  
      проверка номера политики регистрационного свидетельства и разрешенных способах его использования. Если политика проверяемого регистрационного свидетельства предусматривает ограничение его использования (только в одной системе), то данное регистрационное свидетельство и соответствующий закрытый ключ не использоваться в других системах;  
      проверка метки времени. Доказательством подписания документа в указанный момент времени является квитанция метки времени, полученная в НУЦ и содержащая время подписания документа. Данная проверка производится для электронных документов долговременного хранения и формируется в момент подписания документа. Метка времени является доказательством наличия ЭЦП в указанный в квитанции момент времени;  
      проверка полномочий лица подписавшего документ. Механизмы проверки полномочий возлагаются на информационную систему. Проверку полномочий также можно проверить, в случае наличии информации об этом в регистрационном свидетельстве.  
      39. Проверка подтверждения принадлежности и действительности открытого ключа ЭЦП в электронном документе производится с использованием СКЗИ НУЦ путем использования открытого ключа, который содержится в регистрационном свидетельстве подписывающей стороны. Техническая реализация проверки ЭЦП возлагается на владельца информационной системы.  
      40. В случае если ЭЦП или регистрационное свидетельство не соответствует требованиям хотя бы одного из критериев вышеописанных проверок, за исключением проверки метки времени, то ЭЦП или регистрационное свидетельство считается недействительным.  
      41. Техническая реализация проверки принадлежности и действительности открытого ключа ЭЦП и регистрационного свидетельства возлагается на информационную систему, путем использования высокоуровневых функций разработки с применением СКЗИ НУЦ.

Приложение 1           
к Правилам выдачи, хранения,  
отзыва регистрационных       
свидетельств и подтверждения    
принадлежности и действительности  
открытого ключа электронной    
цифровой подписи национальным   
удостоверяющим центром      
Республики Казахстан

Форма

**Заявление**  
**на выдачу регистрационных свидетельств НУЦ**  
**(от физического лица)**

Уникальный номер 

Идентификационные данные физического лица на имя которого выдаются  
регистрационные свидетельства:  
ИИН: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Фамилия: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Имя: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Отчество (при наличии): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Наименование области: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Город: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Адрес электронной  почты: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Телефон: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Срок действия регистрационных свидетельств: 1 год.  
С политикой соответствующих регистрационных свидетельств НУЦ РК  
ознакомлен, возражений не имею.  
Данные о средствах электронной цифровой подписи, используемых для  
создания соответствующего закрытого ключа электронной цифровой  
подписи, обозначение стандарта алгоритма электронной цифровой подписи  
и длины открытого ключа:  
СКЗИ НУЦ РК (ЭЦП - RSA 2048 Бит, аутентификация - RSA 2048 Бит, ЭЦП  
для sim-карты – ГОСТ 34.310-2004 512 Бит)  
Открытый ключ подписи: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Открытый ключ аутентификации: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Место для дополнительной информации: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
С пользовательским соглашением НУЦ ознакомлен и подтверждаю свое  
согласие на обработку моих персональных данных в целях получения  
регистрационных свидетельств и получения уведомлений на электронную  
почту.

Дата обращения в НУЦ «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20 \_\_г.  
Подпись физического лица (представителя физического лица) \_\_\_\_\_\_\_\_\_\_

Приложение 2           
к Правилам выдачи, хранения,  
отзыва регистрационных       
свидетельств и подтверждения    
принадлежности и действительности  
открытого ключа электронной    
цифровой подписи национальным   
удостоверяющим центром      
Республики Казахстан

Форма

**Заявление**  
**на выдачу регистрационных свидетельств НУЦ**  
**(от юридического лица и индивидуального предпринимателя,**  
**осуществляющего деятельность в виде совместного**  
**предпринимательства)**

Уникальный номер 

Идентификационные данные юридического лица:  
БИН: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Наименование организации или ИП: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Идентификационные данные сотрудника юридического лица на имя которого  
выдается регистрационные свидетельства:  
ИИН: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Фамилия: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Имя: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Отчество (при наличии): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Наименование области: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Город: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Адрес электронной почты: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Телефон: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Срок действия регистрационных свидетельств: 1 год.  
С политикой соответствующих регистрационных свидетельств НУЦ РК  
ознакомлен, возражений не имею.  
Данные о средствах электронной цифровой подписи, используемых для  
создания соответствующего закрытого ключа электронной цифровой  
подписи, обозначение стандарта алгоритма электронной цифровой подписи  
и длины открытого ключа:  
СКЗИ НУЦ (ЭЦП – ГОСТ 34.310-2004 512 Бит, Аутентификация - RSA 2048  
Бит)  
Открытый ключ подписи: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Открытый ключ аутентификации: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Место для дополнительной информации: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
С пользовательским соглашением НУЦ ознакомлен и подтверждаю свое  
согласие на обработку моих персональных данных в целях получения  
регистрационных свидетельств и получения уведомлений на электронную  
почту.  
Дата обращения в НУЦ «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20 \_\_г.

Подпись сотрудника юридического лица или ИП (представителя  
юридического лица или ИП) \_\_\_\_\_\_\_\_\_\_\_\_

Приложение 3           
к Правилам выдачи, хранения,  
отзыва регистрационных       
свидетельств и подтверждения    
принадлежности и действительности  
открытого ключа электронной    
цифровой подписи национальным   
удостоверяющим центром      
Республики Казахстан

Форма

**Доверенность**  
**на разовое получение или отзыв**  
**регистрационных свидетельств НУЦ от юридического лица**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,        «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_ г  
(наименование населенного пункта)  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,        БИН \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,  
(наименование юридического лица)

юридический адрес: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,  
в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,  
действующего на основании Устава (Положения), настоящей доверенностью  
уполномочивает:  
гражданина \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,  
           (фамилия, имя, отчество (при наличии), год и место  
            рождения, место жительства)  
ИИН \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
представить документы на \_\_\_\_\_\_\_\_\_\_\_\_\_ регистрационных свидетельств в  
                      (выдачу или отзыв)  
НУЦ для сотрудников юридического лица:  
1.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
           (фамилия, имя, отчество (при наличии))     (подпись)  
ИИН \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   
2.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
             (фамилия, имя, отчество (при наличии)) (подпись)  
ИИН \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
3.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
              (фамилия, имя, отчество (при наличии)) (подпись)  
ИИН \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
4.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
              (фамилия, имя, отчество (при наличии)) (подпись)  
ИИН \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
      Представитель наделяется правом расписываться в соответствующих  
документах НУЦ для исполнения поручений, определенных настоящей  
доверенностью.

      Руководитель \_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_  
                   (подпись) (имя, фамилия)

      МП (при наличии)

Приложение 4           
к Правилам выдачи, хранения,  
отзыва регистрационных       
свидетельств и подтверждения    
принадлежности и действительности  
открытого ключа электронной    
цифровой подписи национальным   
удостоверяющим центром      
Республики Казахстан

Форма

**Заявление**  
**на выдачу SSL регистрационного свидетельства НУЦ**  
**(от физического лица)**

Уникальный номер 

Идентификационные данные физического лица на имя которого выдается  
регистрационное свидетельство:  
ИИН: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Фамилия: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Имя: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Отчество (при наличии): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Наименование области: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Город: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Адрес электронной почты: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Телефон: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Доменное имя: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Список дополнительных доменных имен: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Запрос PKCS#10 в формате Base64:

*запрос в формате Base64*

Срок действия регистрационного свидетельства: 1 год.  
С политикой соответствующих регистрационных свидетельств НУЦ РК  
ознакомлен, возражений не имею.  
С пользовательским соглашением НУЦ ознакомлен и подтверждаю свое  
согласие на обработку моих персональных данных в целях получения  
регистрационных свидетельств и получения уведомлений на электронную  
почту.

Дата обращения в НУЦ «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_ г.

Подпись физического лица (представителя физического лица) \_\_\_\_\_\_\_\_\_\_\_

Приложение 5           
к Правилам выдачи, хранения,  
отзыва регистрационных       
свидетельств и подтверждения    
принадлежности и действительности  
открытого ключа электронной    
цифровой подписи национальным   
удостоверяющим центром      
Республики Казахстан

Форма

**Заявление**  
**на выдачу SSL регистрационного свидетельства НУЦ**  
**(от юридического лица)**

Уникальный номер 

Идентификационные данные юридического лица:  
БИН: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Наименование организации: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Идентификационные данные сотрудника юридического лица на имя которого  
выдается регистрационное свидетельство:  
ИИН: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Фамилия: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Имя: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Отчество (при наличии): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Наименование области: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Город: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Адрес электронной почты: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Телефон:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Доменное имя: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Список дополнительных доменных имен: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Запрос PKCS#10 в формате Base64:

*запрос в формате Base64*

Срок действия регистрационного свидетельства: 1 год.  
С политикой соответствующих регистрационных свидетельств НУЦ РК  
ознакомлен, возражений не имею.  
С пользовательским соглашением НУЦ ознакомлен и подтверждаю свое  
согласие на обработку моих персональных данных в целях получения  
регистрационных свидетельств и получения уведомлений на электронную  
почту.

Дата обращения в НУЦ «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_ г.

Подпись сотрудника юридического лица (представителя юридического  
лица) \_\_\_\_\_\_\_\_\_\_\_\_

Приложение 6           
к Правилам выдачи, хранения,  
отзыва регистрационных       
свидетельств и подтверждения    
принадлежности и действительности  
открытого ключа электронной    
цифровой подписи национальным   
удостоверяющим центром      
Республики Казахстан

Форма

**Заявление**  
**на выдачу регистрационных свидетельств НУЦ**  
**(от юридического лица для пользователей**  
**ИС «Казначейство-Клиент»)**

Уникальный номер 

Идентификационные данные юридического лица:  
БИН: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Наименование организации: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Идентификационные данные сотрудника юридического лица на имя которого  
выдается регистрационное свидетельство:  
ИИН: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Фамилия: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Имя: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Отчество (при наличии): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
код ГУ/СКС: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Роль: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Наименование области: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Город: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Адрес электронной почты: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Телефон: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Срок действия регистрационного свидетельства: 1 год.  
С политикой соответствующих регистрационных свидетельств НУЦ РК  
ознакомлен, возражений не имею.  
Данные о средствах электронной цифровой подписи, используемых для  
создания соответствующего закрытого ключа электронной цифровой  
подписи, обозначение стандарта алгоритма электронной цифровой подписи  
и длины открытого ключа:  
СКЗИ НУЦ (ЭЦП – ГОСТ 34.310-2004 512 Бит, Аутентификация - RSA 2048  
Бит)  
Открытый ключ подписи: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Открытый ключ аутентификации: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Место для дополнительной информации: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
С пользовательским соглашением НУЦ ознакомлен и подтверждаю свое  
согласие на обработку моих персональных данных в целях получения  
регистрационных свидетельств и получения уведомлений на электронную  
почту.

Дата обращения в НУЦ «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_ г.

Подпись сотрудника юридического лица (представителя юридического  
лица) \_\_\_\_\_\_\_\_\_\_\_\_\_

Приложение 7           
к Правилам выдачи, хранения,  
отзыва регистрационных       
свидетельств и подтверждения    
принадлежности и действительности  
открытого ключа электронной    
цифровой подписи национальным   
удостоверяющим центром      
Республики Казахстан

**Структуры регистрационных свидетельств**

Структура переподчиненного регистрационного свидетельства НУЦ  
(на алгоритме RSA)

|  |  |  |  |
| --- | --- | --- | --- |
| Поле | Описание | OID, критичность | Содержание |
| Базовые поля регистрационного свидетельства в формате Х.509 v3 | | | |
| Version | Версия стандарта Х.509 | – | V3 |
| SerialNumber | Серийный номер регистрационного свидетельства | – | Положительное, целое число  (не более 20 байт) |
| Signature Algorithm | Алгоритм подписи | 1.2.840.113549.1.1.11 | sha256WithRSAEncryption |
| Issuer | Данные Издателя регистрационного свидетельства | CN=2.5.4.3  O=2.5.4.10  C=2.5.4.6 | CN = НЕГІЗГІ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (RSA)  O = РМК «МЕМЛЕКЕТТІК ТЕХНИКАЛЫҚ ҚЫЗМЕТ»  С = KZ |
| Validity from | Время начала срока действия | UTC TIME | Действителен с:  YYMMDDHHMMSSZ UTC |
| Validity to | Время окончания срока действия | UTC TIME | Действителен по: YYMMDDHHMMSSZ UTC |
| Subject | Данные Владельца регистрационного  свидетельства | C=2.5.4.6  L= 2.5.4.7  S=2.5.4.8  O=2.5.4.10  CN =2.5.4.3 | C = KZ (обязательное поле)  L = АСТАНА (обязательное поле)  S = АСТАНА (обязательное поле)  O = РМК «МЕМЛЕКЕТТІК ТЕХНИКАЛЫҚ ҚЫЗМЕТ» (обязательное поле)  CN = ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (RSA) (обязательное поле) |
| PublicKey | Открытый ключ | 1.2.840.113549.1.1.1 | Значение |
| Дополнительные поля регистрационного свидетельства в формате Х.509 v3 | | | |
| Subject Key Identifier | Идентификатор ключа субъекта | 2.5.29.14 | Значение идентификатор ключа субъекта в шестнадцатеричном формате |
| Authority Key Identifier | Идентификатор ключа центра сертификации | 2.5.29.35 | Значение идентификатора ключа центра сертификации в шестнадцатеричном формате |
| Basic Constraints | Основные ограничения | 2.5.29.19, critical | Тип субъекта = Центр сертификации  Ограничение на длину пути = Отсутствует |
| Key Usage | Использование ключа | 2.5.29.15, critical | Подписание регистрационного свидетельства, Автономное подписание списка отзыва (CRL), Подписание списка отзыва (CRL) (06) |
| Ceritifcate Policy | Политика регистрационного свидетельства | 2.5.29.32 | [1]Политика регистрационного свидетельства:  Идентификатор политики= 1.2.398.3.3.1.1  [1,1]Сведения квалификатора политики:  Идентификатор квалификатора политики = CPS  Квалификатор:  http://pki.gov.kz/cps |
| Ceritifcate Authority Information Access | Доступ к информации о центрах сертификации | 1.3.6.1.5.5.7.1.1 | [1]Доступ к сведениям центра сертификации  Метод доступа = Поставщик центра сертификации (1.3.6.1.5.5.7.48.2)  Дополнительное имя:  URL=http://root.gov.kz/cert/root\_rsa.cer |
| Crl Distribution Points | Точки распространения списков отзыва | 2.5.29.31 | [1]Точка распределения списка отзыва (CRL)  Имя точки распространения:  Полное имя:  URL=http://crl.root.gov.kz/rsa.crl  URL=http://crl1.root.gov.kz/rsa.crl |
| Digital Signature | Цифровая подпись центра сертификации (2048 бит) | 1.2.840.113549.1.1.11 | Значение |

      Структура переподчиненного регистрационного свидетельства НУЦ  
                          (на алгоритме ГОСТ)

|  |  |  |  |
| --- | --- | --- | --- |
| Поле | Описание | OID, критичность | **Содержание** |
| Базовые поля регистрационного свидетельства в формате Х.509 v3 | | | |
| Version | Версия стандарта X.509 | – | V3 |
| Serial Number | Серийный номер регистрационного свидетельства | – | Положительное, целое число  (не более 20 байт) |
| Signature Algorithm | Алгоритм подписи | 1.2.398.3.10.1.1.1.2 | ГОСТ 34.310-2004 |
| Issuer | Данные Издателя регистрационного свидетельства | CN=2.5.4.3  O=2.5.4.10  C=2.5.4.6 | CN = НЕГІЗГІ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (GOST)  O = РМК «МЕМЛЕКЕТТІК ТЕХНИКАЛЫҚ ҚЫЗМЕТ»  С = KZ |
| Validity from | Время начала срока действия | UTC TIME | Действителен с: YYMMDDHHMMSSZ UTC |
| Validity to | Время окончания срока действия | UTC TIME | Действителен по: YYMMDDHHMMSSZ UTC |
| Subject | Данные владельца регистрационного  свидетельства | C=2.5.4.6  L=2.5.4.7  S=2.5.4.8  O=2.5.4.10  CN =2.5.4.3 | C = KZ (обязательное поле)  L = АСТАНА (обязательное поле)  S = АСТАНА (обязательное поле)  O = РМК «МЕМЛЕКЕТТІК ТЕХНИКАЛЫҚ ҚЫЗМЕТ» (обязательное поле)  CN = ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (GOST) (обязательное поле) |
| Public Key | Открытый ключ (512 бит) | 1.2.398.3.10.1.1.1.1  с параметрами  1.2.398.3.10.1.1.1.1.1  1.2.398.3.10.1.3.1.1.0 | Значение |
| Дополнительные поля регистрационного свидетельства в формате Х.509 v3 | | | |
| Subject Key Identifier | Идентификатор ключа субъекта | 2.5.29.14 | Значение идентификатор ключа субъекта в шестнадцатеричном формате |
| Authority Key Identifier | Идентификатор ключа центра сертификации | 2.5.29.35 | Значение идентификатора ключа центра сертификации в шестнадцатеричном формате |
| Basic Constraints | Основные ограничения | 2.5.29.19, critical | Тип субъекта = центр сертификации  Ограничение на длину пути = Отсутствует |
| Key Usage | Использование ключа | 2.5.29.15, critical | Подписание регистрационных свидетельств, Автономное подписание списка отзыва (CRL), Подписание списка отзыва (CRL) (06) |
| Ceritifcate Policy | Политика регистрационного свидетельства | 2.5.29.32 | [1]Политика регистрационного свидетельства:  Идентификатор политики=1.2.398.3.3.1.1  [1,1]Сведения квалификатора политики:  Идентификатор квалификатора политики = CPS  Квалификатор:  http://pki.gov.kz/cps |
| Ceritifcate Authority Information Access | Доступ к информации о центрах сертификации | 1.3.6.1.5.5.7.1.1 | [1]Доступ к сведениям центра сертификации  Метод доступа = Поставщик центра сертификации (1.3.6.1.5.5.7.48.2)  Дополнительное имя:  URL=http://root.gov.kz/cert/root\_gost.cer |
| Crl Distribution Points | Точки распространения списков отзыва | 2.5.29.31 | [1]Точка распределения списка отзыва (CRL)  Имя точки распространения:  Полное имя:  URL=http://crl.root.gov.kz/gost.crl  URL=http://crl1.root.gov.kz/gost.crl |
| Digital Signature | Цифровая подпись центра сертификации (512 бит) | 1.2.398.3.10.1.1.1.2 | Значение |

    Структура регистрационного свидетельства для физических лиц НУЦ  
                              (для подписи)

|  |  |  |  |
| --- | --- | --- | --- |
| Поле | Описание | OID, критичность | Содержание |
| Базовые поля регистрационного свидетельства в формате Х.509 | | | |
| Version | Версия стандарта X.509 | – | V3 |
| Serial Number | Серийный номер регистрационного свидетельства | – | Положительное, целое число  (не более 20 байт) |
| Signature Algorithm | Алгоритм подписи | 1.2.840.113549.1.1.11 | sha256WithRSAEncryption |
| Issuer | Данные издателя регистрационного свидетельства | C=2.5.4.6  L=2.5.4.7  S=2.5.4.8  O=2.5.4.10  CN =2.5.4.3 | C = KZ (обязательное поле)  L = АСТАНА (обязательное поле)  S = АСТАНА (обязательное поле)  O = РМК «МЕМЛЕКЕТТІК ТЕХНИКАЛЫҚ ҚЫЗМЕТ» (обязательное поле)  CN = ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (RSA) (обязательное поле) |
| Validity from | Время начала срока действия | UTC TIME | Действителен с: YYMMDDHHMMSSZ UTC |
| Validity to | Время окончания срока действия | UTC TIME | Действителен по: YYMMDDHHMMSSZ UTC |
| Subject | Данные Владельца регистрационного  свидетельства | Е =1.2.840.113549.1.9.1  SERIALNUMBER = 2.5.4.5  SN=2.5.4.5  G=2.5.4.42  CN =2.5.4.3  L=2.5.4.7  S=2.5.4.8  C=2.5.4.6 | E = Адрес электронной почты (необязательное поле)  SERIALNUMBER = IIN012345678910 (обязательное поле)  SN = Фамилия (необязательное поле)  G = Отчество (необязательное поле)  CN = Фамилия Имя (обязательное поле)  L = Город (обязательное поле)  S = Область (обязательное поле)  C = KZ (обязательное поле) |
| PublicKey | Значение открытого ключа (2048 бит) | 1.2.840.113549.1.1.1 | Значение |
| Дополнительные поля регистрационного свидетельства в формате Х.509 | | | |
| Subject Key Identifier | Идентификатор ключа субъекта | 2.5.29.14 | Значение идентификатор ключа субъекта в шестнадцатеричном формате |
| Authority Key Identifier | Идентификатор ключа центра сертификации | 2.5.29.35 | Значение идентификатора ключа центра сертификации в шестнадцатеричном формате |
| Key Usage | Использование ключа | 2.5.29.15, critical | Цифровая подпись, Неотрекаемость |
| Extended Key Usage | Расширенное использование ключа | 2.5.29.37 | Защищенная электронная почта -1.3.6.1.5.5.7.3.4  Физическое лицо - 1.2.398.3.3.4.1.1 |
| Ceritifcate Policy | Политика регистрационного свидетельства | 2.5.29.32 | [1]Политика регистрационного свидетельства:  Идентификатор политики=1.2.398.3.3.2.3  [1,1]Сведения квалификатора политики:  Идентификатор квалификатора политики = CPS  Квалификатор: http://pki.gov.kz/cps  [1,2]Сведения квалификатора политики:  Идентификатор квалификатора политики = Текст уведомления  Квалификатор: http://pki.gov.kz/cps |
| Ceritifcate Authority Information Access | Доступ к информации о центрах сертификации | 1.3.6.1.5.5.7.1.1 | [1]Доступ к сведениям центра сертификации  Метод доступа = Поставщик центра сертификации (1.3.6.1.5.5.7.48.2)  Дополнительное имя:  URL=http://pki.gov.kz/cert/pki\_rsa.cer  [2]Доступ к сведениям центра сертификации Метод доступа = Протокол определения состояния регистрационного свидетельства через сеть (1.3.6.1.5.5.7.48.1)  Дополнительное имя: URL=http://ocsp.pki.gov.kz/ocsp/ |
| Crl Distribution Points | Точки распространения списков отзыва | 2.5.29.31 | [1]Точка распределения списка отзыва (CRL)  Имя точки распространения:  Полное имя:  URL= http://crl.pki.gov.kz/rsa.crl  URL= http://crl1.pki.gov.kz/rsa.crl |
| Freshest Crl Distribution Points | Новейший CRL | 2.5.29.46 | [1]Новейший CRL  Имя точки распространения:  Полное имя:  URL= http://crl.pki.gov.kz/d\_rsa.crl  URL= http://crl1.pki.gov.kz/d\_rsa.crl |
| Digital Signature | Цифровая подпись Центра сертификации (4096 бит) | 1.2.840.113549.1.1.11 | sha256WithRSAEncryption |

   Структура регистрационного свидетельства для физических лиц НУЦ  
                          (для аутентификации)

|  |  |  |  |
| --- | --- | --- | --- |
| Поле | Описание | OID, критичность | Содержание |
| Базовые поля регистрационного свидетельства в формате Х.509 | | | |
| Version | Версия стандарта X.509 | – | V3 |
| Serial Number | Серийный номер регистрационного свидетельства | – | Положительное, целое число  (не более 20 байт) |
| Signature Algorithm | Алгоритм подписи | 1.2.840.113549.1.1.11 | sha256WithRSAEncryption |
| Issuer | Данные издателя регистрационного свидетельства | C=2.5.4.6  L=2.5.4.7  S=2.5.4.8  O=2.5.4.10  CN =2.5.4.3 | C = KZ (обязательное поле)  L = АСТАНА (обязательное поле)  S = АСТАНА (обязательное поле)  O = РМК «МЕМЛЕКЕТТІК ТЕХНИКАЛЫҚ ҚЫЗМЕТ» (обязательное поле)  CN = ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (RSA) (обязательное поле) |
| Validity from | Время начала срока действия | UTC TIME | Действителен с: YYMMDDHHMMSSZ UTC |
| Validity to | Время окончания срока действия | UTC TIME | Действителен по: YYMMDDHHMMSSZ UTC |
| Subject | Данные Владельца регистрационного  свидетельства | Е =1.2.840.113549.1.9.1  SERIALNUMBER = 2.5.4.5  SN=2.5.4.5  G=2.5.4.42  CN =2.5.4.3  L=2.5.4.7  S=2.5.4.8  C=2.5.4.6 | E = адрес электронной почты физического лица (необязательное поле)  SERIALNUMBER = IIN012345678910 (обязательное поле)  SN = Фамилия (необязательное поле)  G = Отчество (необязательное поле)  CN = Фамилия Имя (обязательное поле)  L = Город (обязательное поле)  S = Область (обязательное поле)  C = KZ (обязательное поле) |
| PublicKey | Значение открытого ключа (2048 бит) | 1.2.840.113549.1.1.1 | Значение |
| Дополнительные поля регистрационного свидетельства в формате Х.509 | | | |
| Subject Key Identifier | Идентификатор ключа субъекта | 2.5.29.14 | Значение идентификатор ключа субъекта в шестнадцатеричном формате |
| Authority Key Identifier | Идентификатор ключа центра сертификации | 2.5.29.35 | Значение идентификатора ключа центра сертификации в шестнадцатеричном формате |
| Key Usage | Использование ключа | 2.5.29.15, critical | Цифровая подпись, Шифрование ключей |
| Extended Key Usage | Расширенное использование ключа | 2.5.29.37 | Проверка подлинности клиента -1.3.6.1.5.5.7.3.2  Физическое лицо- 1.2.398.3.3.4.1.1 |
| Ceritifcate Policy | Политика регистрационного свидетельства | 2.5.29.32 | [1]Политика регистрационного свидетельства:  Идентификатор политики=1.2.398.3.3.2.4  [1,1]Сведения квалификатора политики:  Идентификатор квалификатора политики = CPS  Квалификатор: http://pki.gov.kz/cps  [1,2]Сведения квалификатора политики:  Идентификатор квалификатора политики = Текст уведомления  Квалификатор: http://pki.gov.kz/cps |
| Ceritifcate Authority Information Access | Доступ к информации о центрах сертификации | 1.3.6.1.5.5.7.1.1 | [1]Доступ к сведениям центра сертификации  Метод доступа = Поставщик центра сертификации (1.3.6.1.5.5.7.48.2)  Дополнительное имя:  URL=http://pki.gov.kz/cert/pki\_rsa.cer  [2]Доступ к сведениям центра сертификации Метод доступа = Протокол определения состояния регистрационного свидетельства через сеть (1.3.6.1.5.5.7.48.1)  Дополнительное имя: URL=http://ocsp.pki.gov.kz/ocsp/ |
| Crl Distribution Points | Точки распространения списков отзыва | 2.5.29.31 | [1]Точка распределения списка отзыва (CRL)  Имя точки распространения:  Полное имя:  URL=http://crl.pki.gov.kz/rsa.crl  URL=http://crl1.pki.gov.kz/rsa.crl |
| Freshest Crl Distribution Points | Новейший CRL | 2.5.29.46 | [1]Новейший CRL  Имя точки распространения:  Полное имя:  URL=http://crl.pki.gov.kz/d\_rsa.crl  URL=http://crl1.pki.gov.kz/d\_rsa.crl |
| Digital Signature | Цифровая подпись Центра сертификации (4096 бит) | 1.2.840.113549.1.1.11 | sha256WithRSAEncryption |

    Структура регистрационного свидетельства для юридических лиц НУЦ  
                             (для подписи)

|  |  |  |  |
| --- | --- | --- | --- |
| Поле | Описание | OID, критичность | Содержание |
| Базовые поля регистрационного свидетельства в формате Х.509 | | | |
| Version | Версия стандарта X.509 | – | V3 |
| Serial Number | Серийный номер регистрационного свидетельства | – | Положительное, целое число  (не более 20 байт) |
| Signature Algorithm | Алгоритм подписи | 1.2.398.3.10.1.1.1.2 | ГОСТ 34.310-2004 |
| Issuer | Данные издателя регистрационного свидетельства | C=2.5.4.6  L=2.5.4.7  S=2.5.4.8  O=2.5.4.10  CN =2.5.4.3 | C = KZ (обязательное поле)  L = АСТАНА (обязательное поле)  S = АСТАНА (обязательное поле)  O = РМК «МЕМЛЕКЕТТІК ТЕХНИКАЛЫҚ ҚЫЗМЕТ» (обязательное поле)  CN = ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (GOST) (обязательное поле) |
| Validity from | Время начала срока действия | UTC TIME | Действителен с: YYMMDDHHMMSSZ UTC |
| Validity to | Время окончания срока действия | UTC TIME | Действителен по: YYMMDDHHMMSSZ UTC |
| Subject | Данные Владельца регистрационного  свидетельства | Е =1.2.840.113549.1.9.1  SERIALNUMBER = 2.5.4.5  SN=2.5.4.4  G=2.5.4.42  CN =2.5.4.3  OU=2.5.4.11  O=2.5.4.10  L=2.5.4.7  S=2.5.4.8  C=2.5.4.6 | E = адрес электронной почты (необязательное поле)  SERIALNUMBER = IIN012345678910 (обязательное поле)  SN = Фамилия (необязательное поле)  G = Отчество (необязательное поле)  CN = Фамилия Имя (обязательное поле)  OU = BIN012345678910 (обязательное поле)  O = Наименование организации (обязательное поле)  L = Город (обязательное поле)  S = Область (обязательное поле)  C = KZ (обязательное поле) |
| Public Key | Значение открытого ключа (512 бит) | 1.2.398.3.10.1.1.1.1  с параметрами  1.2.398.3.10.1.1.1.1.1  1.2.398.3.10.1.3.1.1.0 | ГОСТ 34.310-2004 |
| Дополнительные поля регистрационного свидетельства в формате Х.509 | | | |
| Subject Key Identifier | Идентификатор ключа субъекта | 2.5.29.14 | Значение идентификатор ключа субъекта в шестнадцатеричном формате |
| Authority Key Identifier | Идентификатор ключа центра сертификации | 2.5.29.35 | Значение идентификатора ключа центра сертификации в шестнадцатеричном формате |
| Key Usage | Использование ключа | 2.5.29.15, critical | Цифровая подпись, Неотрекаемость |
| Extended Key Usage | Расширенное использование ключа | 2.5.29.37 | Защищенная электронная почта -1.3.6.1.5.5.7.3.4  Юридическое лицо - 1.2.398.3.3.4.1.2  Неизвестное использование ключа (OID), где в качестве OID определено множество  доступных идентификаторов.  Доступные идентификаторы:  1.2.398.3.3.4.1.2.1 – Первый руководитель юридического лица, имеющий право подписи  1.2.398.3.3.4.1.2.2 – Лицо, наделенное правом подписи  1.2.398.3.3.4.1.2.3 - Лицо, наделенное правом подписи финансовых документов  1.2.398.3.3.4.1.2.4 – Сотрудник отдела кадров, наделенный правом подтверждать заявки на выпуск регистрационных свидетельств поданные от сотрудников юридического лица  1.2.398.3.3.4.1.2.5 – Сотрудник организации |
| Ceritifcate Policy | Политика регистрационного свидетельства | 2.5.29.32 | [1]Политика регистрационного свидетельства:  Идентификатор политики=1.2.398.3.3.2.1  [1,1]Сведения квалификатора политики:  Идентификатор квалификатора политики=CPS  Квалификатор:  http://pki.gov.kz/cps  [1,2]Сведения квалификатора политики:  Идентификатор квалификатора политики=Текст уведомления  Квалификатор: http://pki.gov.kz/cps |
| Certificate Authority Information Access | Доступ к информации о центрах сертификации | 1.3.6.1.5.5.7.1.1 | [1]Доступ к сведениям центра сертификации  Метод доступа=Поставщик центра сертификации (1.3.6.1.5.5.7.48.2)  Дополнительное имя: URL=http://pki.gov.kz/cert/pki\_gost.cer  [2]Доступ к сведениям центра сертификации Метод доступа=Протокол определения состояния регистрационного свидетельства через сеть (1.3.6.1.5.5.7.48.1)  Дополнительное имя: URL= URL=http://ocsp.pki.gov.kz/ocsp/ |
| Crl Distribution Points | Точки распространения списков отзыва | 2.5.29.31 | [1]Точка распределения списка отзыва (CRL)  Имя точки распространения:  Полное имя:  URL= http://crl.pki.gov.kz/gost.crl  URL=http://crl1.pki.gov.kz/gost.crl |
| Freshest Crl Distribution Points | Новейший CRL | 2.5.29.46 | [1]Новейший CRL  Имя точки распространения:  Полное имя:  URL=http://crl.pki.gov.kz/d\_gost.crl  URL=http://crl1.pki.gov.kz/d\_gost.crl |
| Digital Signature | Цифровая подпись Центра сертификации (512 бит) | 1.2.398.3.10.1.1.1.2 | ГОСТ 34.310-2004 |

    Структура регистрационного свидетельства для юридических лиц НУЦ  
                              (для аутентификации)

|  |  |  |  |
| --- | --- | --- | --- |
| Поле | Описание | OID, критичность | Содержание |
| Базовые поля регистрационного свидетельства в формате Х.509 | | | |
| Version | Версия стандарта X.509 | – | V3 |
| Serial Number | Серийный номер регистрационного свидетельства | – | Положительное, целое число  (не более 20 байт) |
| Signature Algorithm | Алгоритм подписи | 1.2.840.113549.1.1.11 | sha256WithRSAEncryption |
| Issuer | Данные издателя регистрационного свидетельства | C=2.5.4.6  L=2.5.4.7  S=2.5.4.8  O=2.5.4.10  CN =2.5.4.3 | C = KZ (обязательное поле)  L = АСТАНА (обязательное поле)  S = АСТАНА (обязательное поле)  O = РМК «МЕМЛЕКЕТТІК ТЕХНИКАЛЫҚ ҚЫЗМЕТ» (обязательное поле)  CN = ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (RSA) (обязательное поле) |
| Validity from | Время начала срока действия | UTC TIME | Действителен с: YYMMDDHHMMSSZ UTC |
| Validity to | Время окончания срока действия | UTC TIME | Действителен по: YYMMDDHHMMSSZ UTC |
| Subject | Данные Владельца регистрационного  свидетельства | Е =1.2.840.113549.1.9.1  SERIALNUMBER =2.5.4.5  SN=2.5.4.5  G=2.5.4.42  CN =2.5.4.3  OU=2.5.4.11  О=2.5.4.10  L=2.5.4.7  S=2.5.4.8  C=2.5.4.6 | E = Адрес электронный почты (необязательное поле)  SERIALNUMBER = IIN012345678910 (обязательное поле)  SN = Фамилия (необязательное поле)  G = Отчество (необязательное поле)  CN = Фамилия Имя (обязательное поле)  OU = BIN012345678910 (обязательное поле)  O = Наименование организации (обязательное поле)  L = Город (обязательное поле)  S = Область (обязательное поле)  C = KZ (обязательное поле) |
| Public Key | Значение открытого ключа (2048 бит) | 1.2.840.113549.1.1.1 | Значение |
| Дополнительные поля регистрационного свидетельства в формате Х.509 | | | |
| Subject Key Identifier | Идентификатор ключа субъекта | 2.5.29.14 | Значение идентификатор ключа субъекта в шестнадцатеричном формате |
| Authority Key Identifier | Идентификатор ключа центра сертификации | 2.5.29.35 | Значение идентификатора ключа центра сертификации в шестнадцатеричном формате |
| Key Usage | Использование ключа | 2.5.29.15, critical | Цифровая подпись, Шифрование ключей |
| Extended Key Usage | Расширенное использование ключа | 2.5.29.37 | Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)  Юридическое лицо (1.2.398.3.3.4.1.2)  Неизвестное использование ключа (OID), где в качестве OID определено множесто  доступных идентификаторов.  Доступные идентификаторы:  1.2.398.3.3.4.1.2.1 – Первый руководитель юридического лица, имеющий право подписи  1.2.398.3.3.4.1.2.2 – Лицо, наделенное правом подписи  1.2.398.3.3.4.1.2.3 - Лицо, наделенное правом подписи финансовых документов  1.2.398.3.3.4.1.2.4 – Сотрудник отдела кадров, наделенный правом подтверждать заявки на выпуск регистрационных свидетельств поданные от сотрудников юридического лица  1.2.398.3.3.4.1.2.5 – Сотрудник организации |
| Ceritifcate Policy | Политика регистрационного свидетельства | 2.5.29.32 | [1]Политика регистрационного свидетельства:  Идентификатор политики=1.2.398.3.3.2.2  [1,1]Сведения квалификатора политики:  Идентификатор квалификатора политики = CPS  Квалификатор: http://pki.gov.kz/cps  [1,2]Сведения квалификатора политики:  Идентификатор квалификатора политики = Текст уведомления  Квалификатор: http://pki.gov.kz/cps |
| Ceritifcate Authority Information Access | Доступ к информации о центрах сертификации | 1.3.6.1.5.5.7.1.1 | [1]Доступ к сведениям центра сертификации  Метод доступа = Поставщик центра сертификации (1.3.6.1.5.5.7.48.2)  Дополнительное имя:  URL=http://pki.gov.kz/cert/pki\_rsa.cer  [2]Доступ к сведениям центра сертификации Метод доступа = Протокол определения состояния регистрационного свидетельства через сеть (1.3.6.1.5.5.7.48.1)  Дополнительное имя: URL=http://ocsp.pki.gov.kz/ocsp/ |
| Crl Distribution Points | Точки распространения списков отзыва | 2.5.29.31 | [1]Точка распределения списка отзыва (CRL)  Имя точки распространения:  Полное имя:  URL=http://crl.pki.gov.kz/rsa.crl  URL=http://crl1.pki.gov.kz/rsa.crl |
| Freshest Crl Distribution Points | Новейший CRL | 2.5.29.46 | [1]Новейший CRL  Имя точки распространения:  Полное имя:  URL=http://crl.pki.gov.kz/d\_rsa.crl  URL=http://crl1.pki.gov.kz/d\_rsa.crl |
| Digital Signature | Цифровая подпись ЦС (4096 бит) | 1.2.840.113549.1.1.11 | sha256WithRSAEncryption |

      Структура регистрационного свидетельства для участников  
     информационной системы «Казначейство-клиент» (для подписи)

|  |  |  |  |
| --- | --- | --- | --- |
| Поле | Описание | OID, Критичность | Содержание |
| Базовые поля регистрационного свидетельства в формате Х.509 | | | |
| Version | Версия стандарта X.509 | – | V3 |
| Serial Number | Серийный номер регистрационного свидетельства | – | Положительное, целое число  (не более 20 байт) |
| Signature Algorithm | Алгоритм подписи | 1.2.398.3.10.1.1.1.2 | ГОСТ 34.310-2004 |
| Issuer | Данные издателя регистрационного свидетельства | C=2.5.4.6  L=2.5.4.7  S=2.5.4.8  O=2.5.4.10  CN =2.5.4.3 | C = KZ (обязательное поле)  L = АСТАНА (обязательное поле)  S = АСТАНА (обязательное поле)  O = РМК «МЕМЛЕКЕТТІК ТЕХНИКАЛЫҚ ҚЫЗМЕТ» (обязательное поле)  CN = ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (GOST) (обязательное поле) |
| Validity from | Время начала срока действия | UTC TIME | Действителен с: YYMMDDHHMMSSZ UTC |
| Validity to | Время окончания срока действия | UTC TIME | Действителен по: YYMMDDHHMMSSZ UTC |
| Subject | Данные Владельца регистрационного  свидетельства | Е =1.2.840.113549.1.9.1  SERIALNUMBER =2.5.4.5  SN=2.5.4.5  G=2.5.4.42  CN =2.5.4.3  BUSINESSCATEGORY = 2.5.4.15  DC=0.9.2342.19200300.100.1.25  OU=2.5.4.11  O=2.5.4.10  L=2.5.4.7  S=2.5.4.8  C=2.5.4.6 | E = адрес электронной почты (необязательное поле)  SERIALNUMBER = IIN012345678910 (обязательное поле)  SN = Фамилия (необязательное поле)  G = Отчество (необязательное поле)  CN = Фамилия Имя (обязательное поле)  BUSINESSCATEGORY = KS01234 (обязательное поле)  DC = ROLE01 (обязательное поле)  OU = BIN012345678910 (обязательное поле)  O = Наименование организации (обязательное поле)  L = Город (обязательное поле)  S = Область (обязательное поле)  C = KZ (обязательное поле) |
| PublicKey | Значение открытого ключа (512 бит) | 1.2.398.3.10.1.1.1.1  с параметрами  1.2.398.3.10.1.1.1.1.1  1.2.398.3.10.1.3.1.1.0 | ГОСТ 34.310-2004 |
| Дополнительные поля регистрационного свидетельства в формате Х.509 | | | |
| Subject Key Identifier | Идентификатор ключа субъекта | 2.5.29.14 | Значение идентификатор ключа субъекта в шестнадцатеричном формате |
| Authority Key Identifier | Идентификатор ключа центра сертификации | 2.5.29.35 | Значение идентификатора ключа центра сертификации в шестнадцатеричном формате |
| Key Usage | Использование ключа | 2.5.29.15, critical | Цифровая подпись, Неотрекаемость |
| Extended Key Usage | Расширенное использование ключа | 2.5.29.37 | Неизвестное использование ключа (OID),.где в качестве OID определено множесто доступных идентификаторов.  Доступные идентификаторы:  Юридическое лицо -1.2.398.3.3.4.1.2;  Информационная система К2 -1.2.398.5.19.1.2.2.1 |
| Ceritifcate Policy | Политика регистрационного свидетельства | 2.5.29.32 | [1]Политика регистрационного свидетельства:  Идентификатор политики=1.2.398.5.19.1.2.2.1.2  [1,1]Сведения квалификатора политики:  Идентификатор квалификатора политики = CPS  Квалификатор:  http://pki.gov.kz/cps |
| Certificate Authority Information Access | Доступ к информации о центрах сертификации | 1.3.6.1.5.5.7.1.1 | [1]Доступ к сведениям центра сертификации  Метод доступа = Поставщик центра сертификации (1.3.6.1.5.5.7.48.2)  Дополнительное имя:  URL = http://pki.gov.kz/cert/pki\_gost.cer  [2]Доступ к сведениям центра сертификации Метод доступа = Протокол определения состояния регистрационного свидетельства через сеть (1.3.6.1.5.5.7.48.1)  Дополнительное имя:  URL=http://ocsp.pki.gov.kz/ocsp/ |
| Crl Distribution Points | Точки распространения списков отзыва | 2.5.29.31 | [1]Точка распределения списка отзыва (CRL)  Имя точки распространения:  Полное имя:  URL=http://crl.pki.gov.kz/gost.crl  URL=http://crl1.pki.gov.kz/gost.crl |
| Freshest Crl Distribution Points | Новейший CRL | 2.5.29.46 | [1]Новейший CRL  Имя точки распространения:  Полное имя:  URL=http://crl.pki.gov.kz/d\_gost.crl  URL=http://crl1.pki.gov.kz/d\_gost.crl |
| Digital Signature | Цифровая подпись Центра сертификации (512 бит) | 1.2.398.3.10.1.1.1.2 | ГОСТ 34.310-2004 |

             Структура регистрационного свидетельства  
    для участников информационной системы «Казначейство-клиент»  
                      (для аутентификации)

|  |  |  |  |
| --- | --- | --- | --- |
| Поле | Описание | OID, критичность | Содержание |
| Базовые поля регистрационного свидетельства в формате Х.509 | | | |
| Version | Версия стандарта X.509 | – | V3 |
| Serial Number | Серийный номер регистрационного свидетельства | – | Положительное, целое число  (не более 20 байт) |
| Signature Algorithm | Алгоритм подписи | 1.2.840.113549.1.1.11 | sha256WithRSAEncryption |
| Issuer | Данные издателя регистрационного свидетельства | C=2.5.4.6  L=2.5.4.7  S=2.5.4.8  O=2.5.4.10  CN =2.5.4.3 | C = KZ (обязательное поле)  L = АСТАНА (обязательное поле)  S = АСТАНА (обязательное поле)  O = РМК «МЕМЛЕКЕТТІК ТЕХНИКАЛЫҚ ҚЫЗМЕТ» (обязательное поле)  CN = ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (RSA) (обязательное поле) |
| Validity from | Время начала срока действия | UTC TIME | Действителен с: YYMMDDHHMMSSZ UTC |
| Validity to | Время окончания срока действия | UTC TIME | Действителен по: YYMMDDHHMMSSZ UTC |
| Subject | Данные Владельца регистрационного  свидетельства | Е =1.2.840.113549.1.9.1  SERIALNUMBER =2.5.4.5  SN=2.5.4.5  G=2.5.4.42  CN =2.5.4.3  BUSINESSCATEGORY= 2.5.4.15  DC=0.9.2342.19200300.100.1.25  OU=2.5.4.11  O=2.5.4.10  L=2.5.4.7  S=2.5.4.8  C=2.5.4.6 | E = адрес электронной почты (необязательное поле)  SERIALNUMBER = IIN012345678910 (обязательное поле)  SN = Фамилия (необязательное поле)  G = Отчество (необязательное поле)  CN = Фамилия Имя (обязательное поле)  BUSINESSCATEGORY= KS01234 (обязательное поле)  DC = ROLE01 (обязательное поле)  OU = BIN012345678910 (обязательное поле)  O = Наименование организации (обязательное поле)  L = Город (обязательное поле)  S = Область (обязательное поле)  C = KZ (обязательное поле) |
| Public Key | Значение открытого ключа (2048 бит) | 1.2.840.113549.1.1.1 | Значение |
| Дополнительные поля регистрационного свидетельства в формате Х.509 | | | |
| Subject Key Identifier | Идентификатор ключа субъекта | 2.5.29.14 | Значение идентификатор ключа субъекта в шестнадцатеричном формате |
| Authority Key Identifier | Идентификатор ключа центра сертификации | 2.5.29.35 | Значение идентификатора ключа центра сертификации в шестнадцатеричном формате |
| Key Usage | Использование ключа | 2.5.29.15, critical | Цифровая подпись, Шифрование ключей |
| Extended Key Usage | Расширенное использование ключа | 2.5.29.37 | Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)  Неизвестное использование ключа (OID), где в качестве OID определено множесто доступных идентификаторов.  Доступные идентификаторы:  1.2.398.3.3.4.1.2 – Юридическое лицо;  1.2.398.5.19.1.2.2.1 – Информационная система К2 |
| Ceritifcate Policy | Политика регистрационного свидетельства | 2.5.29.32 | [1]Политика регистрационного свидетельства:  Идентификатор политики=1.2.398.5.19.1.2.2.1.3  [1,1]Сведения квалификатора политики:  Идентификатор квалификатора политики = CPS  Квалификатор:  http://pki.gov.kz/cps |
| Authority Info Access | Доступ к информации о центрах сертификации | 1.3.6.1.5.5.7.1.1 | [1]Доступ к сведениям центра сертификации  Метод доступа = Поставщик центра сертификации (1.3.6.1.5.5.7.48.2)  Дополнительное имя:  URL=http://pki.gov.kz/cert/pki\_rsa.cer  [2]Доступ к сведениям центра сертификации Метод доступа = Протокол определения состояния регистрационного свидетельства через сеть (1.3.6.1.5.5.7.48.1)  Дополнительное имя: URL=http://ocsp.pki.gov.kz/ocsp/ |
| Crl Distribution Points | Точки распространения списков отзыва | 2.5.29.31 | [1]Точка распределения списка отзыва (CRL)  Имя точки распространения:  Полное имя:  URL=http://crl.pki.gov.kz/rsa.crl  URL=http://crl1.pki.gov/kz/rsa.crl |
| Freshest Crl Distribution Points | Новейший CRL | 2.5.29.46 | [1]Новейший CRL  Имя точки распространения:  Полное имя:  URL=http://crl.pki.gov.kz/crl/d\_rsa.crl  URL=http://crl1.pki.gov.kz/crl/d\_rsa.crl |
| Digital Signature | Цифровая подпись Центра сертификации (4096 бит) | 1.2.840.113549.1.1.11 | sha256WithRSAEncryption |

  Структура регистрационного свидетельства SSL для физических лиц НУЦ

|  |  |  |  |
| --- | --- | --- | --- |
| Поле | Описание | OID, критичность | Содержание |
| Базовые поля регистрационного свидетельства в формате Х.509 | | | |
| Version | Версия стандарта X.509 | – | V3 |
| Serial Number | Серийный номер регистрационного свидетельства | – | Положительное, целое число  (не более 20 байт) |
| Signature Algorithm | Алгоритм подписи | 1.2.840.113549.1.1.11 | sha256WithRSAEncryption |
| Issuer | Данные Издателя регистрационного свидетельства | C=2.5.4.6  L=2.5.4.7  S=2.5.4.8  O=2.5.4.10  CN =2.5.4.3 | C = KZ (обязательное поле)  L = АСТАНА (обязательное поле)  S = АСТАНА (обязательное поле)  O = РМК «МЕМЛЕКЕТТІК ТЕХНИКАЛЫҚ ҚЫЗМЕТ» (обязательное поле)  CN = ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (RSA) (обязательное поле) |
| Validity from | Время начала срока действия | UTC TIME | Действителен с: YYMMDDHHMMSSZ UTC |
| Validity to | Время окончания срока действия | UTC TIME | Действителен по: YYMMDDHHMMSSZ UTC |
| Subject | Данные Владельца регистрационного  свидетельства | Е =1.2.840.113549.1.9.1  SERIALNUMBER = 2.5.4.5  CN =2.5.4.3  L=2.5.4.7  S=2.5.4.8  C=2.5.4.6 | E = Адрес электронной почты (необязательное поле)  SERIALNUMBER = IIN012345678910 (обязательное поле)  CN = Доменное имя (обязательное поле)  L = Город (обязательное поле)  S = Область (обязательное поле)  C = KZ (обязательное поле) |
| Public Key | Значение открытого ключа (2048 бит) | 1.2.840.113549.1.1.1 | Значение |
| Дополнительные поля регистрационного свидетельства в формате Х.509 | | | |
| Subject Key Identifier | Идентификатор ключа субъекта | 2.5.29.14 | Значение идентификатор ключа субъекта в шестнадцатеричном формате |
| Authority Key Identifier | Идентификатор ключа центра сертификации | 2.5.29.35 | Значение идентификатора ключа центра сертификации в шестнадцатеричном формате |
| Extended Key Usage | Расширенное использование ключа | 2.5.29.37 | Проверка подлинности сервера  (1.3.6.1.5.5.7.3.1)  Физическое лицо - 1.2.398.3.3.4.1.1 |
| Key Usage | Использование ключа | 2.5.29.15, critical | Цифровая подпись, Шифрование ключей |
| Subject Alternative  Name | Дополнительное имя субъекта |  | DNS-имя=Доменное имя-1  DNS-имя= Доменное имя-2  DNS-имя= N  (обязательное поле) |
| Authority Info Access | Доступ к информации о центрах сертификации | 1.3.6.1.5.5.7.1.1 | [1]Доступ к сведениям центра сертификации  Метод доступа = Поставщик центра сертификации (1.3.6.1.5.5.7.48.2)  Дополнительное имя:  URL = http://pki.gov.kz/cert/pki\_rsa.cer  [2]Доступ к сведениям центра сертификации Метод доступа = Протокол определения состояния регистрационного свидетельства через сеть (1.3.6.1.5.5.7.48.1)  Дополнительное имя: URL=http://ocsp.pki.gov.kz/ocsp/ |
| Ceritifcate Policy | Политика регистрационного свидетельства | 2.5.29.32 | 1]Политика сертификата:  Идентификатор политики= 1.2.398.3.3.2.5  [1,1]Сведения квалификатора политики:  Идентификатор квалификатора политики=CPS  Квалификатор:  http://pki.gov.kz/cps |
| Crl Distribution Points | Точки распространения списков отзыва | 2.5.29.31 | [1]Точка распределения списка отзыва (CRL)  Имя точки распространения:  Полное имя:  URL=http://crl.pki.gov.kz/rsa.crl  URL=http://crl1.pki.gov.kz/rsa.crl |
| Freshest Crl Distribution Points | Новейший CRL | 2.5.29.46 | [1]Новейший CRL  Имя точки распространения:  Полное имя:  URL=http://crl.pki.gov.kz/d\_rsa.crlURL=http://crl1.pki.gov.kz/d\_rsa.crl |
| Digital Signature | Цифровая подпись ЦС (4096 бит) | 1.2.840.113549.1.1.1.1 | Значение |

            Структура регистрационного свидетельства SSL для  
                           юридических лиц НУЦ

|  |  |  |  |
| --- | --- | --- | --- |
| Поле | Описание | OID, критичность | Содержание |
| Базовые поля регистрационного свидетельства в формате Х.509 | | | |
| Version | Версия стандарта X.509 | – | V3 |
| Serial Number | Серийный номер регистрационного свидетельства | – | Положительное, целое число  (не более 20 байт) |
| Signature Algorithm | Алгоритм подписи | 1.2.840.113549.1.1.11 | sha256WithRSAEncryption |
| Issuer | Данные издателя регистрационного свидетельства | C=2.5.4.6  L=2.5.4.7  S=2.5.4.8  O=2.5.4.10  CN =2.5.4.3 | C = KZ (обязательное поле)  L = АСТАНА (обязательное поле)  S = АСТАНА (обязательное поле)  O = РМК «МЕМЛЕКЕТТІК ТЕХНИКАЛЫҚ ҚЫЗМЕТ» (обязательное поле)  CN = ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (RSA) (обязательное поле) |
| Validity from | Время начала срока действия | UTC TIME | Действителен с: YYMMDDHHMMSSZ UTC |
| Validity to | Время окончания срока действия | UTC TIME | Действителен по: YYMMDDHHMMSSZ UTC |
| Subject | Данные Владельца регистрационного  свидетельства | Е =1.2.840.113549.1.9.1  SERIALNUMBER =2.5.4.5  SN=2.5.4.4  CN =2.5.4.3  OU=2.5.4.11  О=2.5.4.10  L=2.5.4.7  S=2.5.4.8  C=2.5.4.6 | E = Адрес электронный почты (необязательное поле)  SERIALNUMBER = IIN012345678910 (обязательное поле)  CN = Доменное имя (обязательное поле)  OU = BIN012345678910 (обязательное поле)  O = Наименование организации (обязательное поле)  L = Город (обязательное поле)  S = Область (обязательное поле)  C = KZ (обязательное поле) |
| Public Key | Значение открытого ключа (2048 бит) | 1.2.840.113549.1.1.1 | Значение |
| Дополнительные поля регистрационного свидетельства в формате Х.509 | | | |
| Subject Key Identifier | Идентификатор ключа субъекта | 2.5.29.14 | Значение идентификатор ключа субъекта в шестнадцатеричном формате |
| Authority Key Identifier | Идентификатор ключа центра сертификации | 2.5.29.35 | Значение идентификатора ключа центра сертификации в шестнадцатеричном формате |
| Extended Key Usage | Расширенное использование ключа | 2.5.29.37 | Проверка подлинности сервера  (1.3.6.1.5.5.7.3.1)  Юридическое лицо - 1.2.398.3.3.4.1.2 |
| Key Usage | Использование ключа | 2.5.29.15, critical | Цифровая подпись, Шифрование ключей |
| Subject Alternative Name | Дополнительное имя субъекта |  | DNS-имя=Доменное имя-1  DNS-имя= Доменное имя-2  DNS-имя= N  (обязательное поле) |
| Authority Info Access | Доступ к информации о центрах сертификации | 1.3.6.1.5.5.7.1.1 | [1]Доступ к сведениям центра сертификации  Метод доступа = Поставщик центра сертификации (1.3.6.1.5.5.7.48.2)  Дополнительное имя:  URL = http://pki.gov.kz/cert/pki\_rsa.cer  [2]Доступ к сведениям центра сертификации Метод доступа = Протокол определения состояния регистрационного свидетельства через сеть (1.3.6.1.5.5.7.48.1)  Дополнительное имя: URL=http://ocsp.pki.gov.kz/ocsp/ |
| Ceritifcate Policy | Политика регистрационного свидетельства | 2.5.29.32 | 1]Политика сертификата:  Идентификатор политики= 1.2.398.3.3.2.5  [1,1]Сведения квалификатора политики:  Идентификатор квалификатора политики=CPS  Квалификатор:  http://pki.gov.kz/cps |
| Crl Distribution Points | Точки распространения списков отзыва | 2.5.29.31 | [1]Точка распределения списка отзыва (CRL)  Имя точки распространения:  Полное имя:  URL=http://crl.pki.gov.kz/rsa.crl  URL=http://crl1.pki.gov.kz/rsa.crl |
| Freshest Crl Distribution Points | Новейший CRL | 2.5.29.46 | [1]Новейший CRL  Имя точки распространения:  Полное имя:  URL=http://crl.pki.gov.kz/d\_rsa.crl  URL=http://crl1.pki.gov.kz/d\_rsa.crl |
| Digital Signature | Цифровая подпись ЦС (4096 бит) | 1.2.840.113549.1.1.1.1 | Значение |

                        Структура СОРС НУЦ на алгоритме RSA

|  |  |  |  |
| --- | --- | --- | --- |
| Поле | Описание | OID, критичность | Содержание |
| Базовые поля СОРС в формате Х.509 | | | |
| Version | Версия стандарта X.509 | – | V2 |
| Issuer | Данные издателя СОРС | C=2.5.4.6  L=2.5.4.7  S=2.5.4.8  O=2.5.4.10  CN =2.5.4.3 | C = KZ (обязательное поле)  L = АСТАНА (обязательное поле)  S = АСТАНА (обязательное поле)  O = РМК «МЕМЛЕКЕТТІК ТЕХНИКАЛЫҚ ҚЫЗМЕТ» (обязательное поле)  CN = ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (RSA) (обязательное поле) |
| This Update | Время издания СОРС | UTC TIME | Действителен с: YYMMDDHHMMSSZ UTC |
| Next Update | Следующее обновление СОРС | UTC TIME | Действителен по: YYMMDDHHMMSSZ UTC |
| Signature Algorithm | Алгоритм подписи | 1.2.840.113549.1.1.11 | sha256WithRSAEncryption |
| Дополнительные поля СОРС в формате Х.509 | | | |
| Number CRL | Порядковый номер СОРС | 2.5.29.20 | Последовательно увеличивающийся номер |
| Authority Key Identifier | Идентификатор ключа центра сертификации | 2.5.29.35 | Значение идентификатора ключа центра сертификации в шестнадцатеричном формате |
| Digital Signature | Цифровая подпись ЦС (4096 бит) | 1.2.840.113549.1.1.11 | sha256WithRSAEncryption |

                   Структура СОРС НУЦ на алгоритме ГОСТ

|  |  |  |  |
| --- | --- | --- | --- |
| Поле | Описание | OID, критичность | Содержание |
| Базовые поля СОРС в формате Х.509 | | | |
| Version | Версия стандарта X.509 | – | V2 |
| Issuer | Данные Издателя СОРС | C=2.5.4.6  L=2.5.4.7  S=2.5.4.8  O=2.5.4.10  CN =2.5.4.3 | C = KZ (обязательное поле)  L = АСТАНА (обязательное поле)  S = АСТАНА (обязательное поле)  O = РМК «МЕМЛЕКЕТТІК ТЕХНИКАЛЫҚ ҚЫЗМЕТ» (обязательное поле)  CN = ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (GOST) (обязательное поле) |
| This Update | Время издания СОРС | UTC TIME | Действителен с: YYMMDDHHMMSSZ UTC |
| Next Update | Следующее обновление СОРС | UTC TIME | Действителен по: YYMMDDHHMMSSZ UTC |
| Signature Algorithm | Алгоритм подписи | 1.2.398.3.10.1.1.1.2 | ГОСТ 34.310-2004 |
| Дополнительные поля СОРС в формате Х.509 | | | |
| Number CRL | Порядковый номер СОРС | 2.5.29.20 | Последовательно увеличивающийся номер |
| Authority Key Identifier | Идентификатор ключа центра сертификации | 2.5.29.35 | Значение идентификатора ключа центра сертификации в шестнадцатеричном формате |
| Digital Signature | Цифровая подпись Центра сертификации (512 бит) | 1.2.398.3.10.1.1.1.2 | ГОСТ 34.310-2004 |

        Структура дополнительного СОРС НУЦ на алгоритме RSA

|  |  |  |  |
| --- | --- | --- | --- |
| Поле | Описание | OID, критичность | Содержание |
| Базовые поля СОРС в формате Х.509 | | | |
| Version | Версия стандарта X.509 | – | V2 |
| Issuer | Данные Издателя СОРС | C=2.5.4.6  L=2.5.4.7  S=2.5.4.8  O=2.5.4.10  CN =2.5.4.3 | C = KZ (обязательное поле)  L = АСТАНА (обязательное поле)  S = АСТАНА (обязательное поле)  O = РМК «МЕМЛЕКЕТТІК ТЕХНИКАЛЫҚ ҚЫЗМЕТ» (обязательное поле)  CN = ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (RSA) (обязательное поле) |
| This Update | Время издания СОРС | UTC TIME | Действителен с: YYMMDDHHMMSSZ UTC |
| Next Update | Следующее обновление СОРС | UTC TIME | Действителен по: YYMMDDHHMMSSZ UTC |
| Signature Algorithm | Алгоритм подписи | 1.2.840.113549.1.1.11 | sha256WithRSAEncryption |
| Дополнительные поля СОРС в формате Х.509 | | | |
| Number CRL | Порядковый номер СОРС | 2.5.29.20 | Последовательно увеличивающийся номер |
| Authority Key Identifier | Идентификатор ключа центра сертификации | 2.5.29.35 | Значение идентификатора ключа центра сертификации в шестнадцатеричном формате |
| Freshest CRL | Идентификатор разностного СОРС | 2.5.29.46, critical | – |
| Digital Signature | Цифровая подпись ЦС (4096 бит) | 1.2.840.113549.1.1.11 | sha256WithRSAEncryption |

              Структура дополнительного СОРС НУЦ на ГОСТ

|  |  |  |  |
| --- | --- | --- | --- |
| Поле | Описание | OID, критичность | Содержание |
| Базовые поля СОРС в формате Х.509 | | | |
| Version | Версия стандарта X.509 | – | V2 |
| Issuer | Данные Издателя СОРС | C=2.5.4.6  L=2.5.4.7  S=2.5.4.8  O=2.5.4.10  CN =2.5.4.3 | C = KZ (обязательное поле)  L = АСТАНА (обязательное поле)  S = АСТАНА (обязательное поле)  O = РМК «МЕМЛЕКЕТТІК ТЕХНИКАЛЫҚ ҚЫЗМЕТ» (обязательное поле)  CN = ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (GOST) (обязательное поле) |
| This Update | Время издания СОРС | UTC TIME | Действителен с: YYMMDDHHMMSSZ UTC |
| Next Update | Следующее обновление СОРС | UTC TIME | Действителен по: YYMMDDHHMMSSZ UTC |
| Signature Algorithm | Алгоритм подписи | 1.2.398.3.10.1.1.1.2 | ГОСТ 34.310-2004 |
| Дополнительные поля СОРС в формате Х.509 | | | |
| Number CRL | Порядковый номер СОРС | 2.5.29.20 | Последовательно увеличивающийся номер |
| Authority Key Identifier | Идентификатор ключа центра сертификации | 2.5.29.35 | Значение идентификатора ключа центра сертификации в шестнадцатеричном формате |
| Freshest CRL | Идентификатор разностного СОРС | 2.5.29.46, critical | – |
| Digital Signature | Цифровая подпись Центра сертификации (512 бит) | 1.2.398.3.10.1.1.1.2 | ГОСТ 34.310-2004 |

   Структура регистрационного свидетельства OCSP НУЦ на алгоритме RSA

|  |  |  |  |
| --- | --- | --- | --- |
| Поле | Описание | OID, критичность | Содержание |
| Базовые поля регистрационного свидетельства в формате Х.509 | | | |
| Version | Версия стандарта X.509 | – | V3 |
| Serial Number | Серийный номер регистрационного свидетельства | – | Положительное, целое число  (не более 20 байт) |
| Signature Algorithm | Алгоритм подписи | 1.2.840.113549.1.1.11 | sha256WithRSAEncryption |
| Issuer | Данные издателя регистрационного свидетельства | C=2.5.4.6  L=2.5.4.7  S=2.5.4.8  O=2.5.4.10  CN =2.5.4.3 | C = KZ (обязательное поле)  L = АСТАНА (обязательное поле)  S = АСТАНА (обязательное поле)  O = РМК «МЕМЛЕКЕТТІК ТЕХНИКАЛЫҚ ҚЫЗМЕТ» (обязательное поле)  CN = ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (RSA) (обязательное поле) |
| Validity from | Время начала срока действия | UTC TIME | Действителен с: YYMMDDHHMMSSZ GMT |
| Validity to | Время окончания срока действия | UTC TIME | Действителен по: YYMMDDHHMMSSZ GMT |
| Subject | Данные Владельца регистрационного  свидетельства | CN =2.5.4.3  OU=2.5.4.11  O=2.5.4.10  L=2.5.4.7  S=2.5.4.8  C=2.5.4.6  SERIALNUMBER = 2.5.4.5 | CN = Наименование сервиса (обязательное поле)  OU = Подразделение (обязательное поле)  O = Наименование организации (обязательное поле)  L = Город (обязательное поле)  S = Область (обязательное поле)  C = KZ (обязательное поле)  SERIALNUMBER = IIN012345678910 (обязательное поле) |
| Public Key | Значение открытого ключа (2048 бит) | 1.2.840.113549.1.1.1 | Значение |
| Дополнительные поля регистрационного свидетельства в формате Х.509 | | | |
| Subject Key Identifier | Идентификатор ключа субъекта | 2.5.29.14 | Значение идентификатор ключа субъекта в шестнадцатеричном формате |
| Authority Key Identifier | Идентификатор ключа центра сертификации | 2.5.29.35 | Значение идентификатора ключа центра сертификации в шестнадцатеричном формате |
| Extended Key Usage | Расширенное использование ключа | 2.5.29.37 | Online Certificate Status Protocol (1.3.6.1.5.5.7.3.9) |
| Ceritifcate Authority Information Access | Доступ к информации о центрах сертификации | 1.3.6.1.5.5.7.1.1 | [1]Доступ к сведениям центра сертификации  Метод доступа = Поставщик центра сертификации (1.3.6.1.5.5.7.48.2)  Дополнительное имя:  URL=http://pki.gov.kz/cert/pki\_rsa.cer |
| Crl Distribution Points | Точки распространения списков отзыва | 2.5.29.31 | [1]Точка распределения списка отзыва (CRL)  Имя точки распространения:  Полное имя:  URL=http://crl.pki.gov.kz/rsa.crl  URL=http://crl1.pki.gov.kz/rsa.crl |
| Freshest Crl Distribution Points | Новейший CRL | 2.5.29.46 | [1]Новейший CRL  Имя точки распространения:  Полное имя:  URL=http://crl.pki.gov.kz/d\_rsa.crl  URL=http://crl1.pki.gov.kz/d\_rsa.crl |
| OCSP No Revocation Checking | Проверка безотзывности OCSP | 1.3.6.1.5.5.7.48.1.5 | Пустое значение |
| Digital Signature | Цифровая подпись Центра сертификации (4096 бит) | 1.2.840.113549.1.1.11 | sha256WithRSAEncryption |

Структура регистрационного свидетельства TSP НУЦ на алгоритме RSA

|  |  |  |  |
| --- | --- | --- | --- |
| Поле | Описание | OID, критичность | Содержание |
| Базовые поля регистрационного свидетельства в формате Х.509 | | | |
| Version | Версия стандарта X.509 | – | V3 |
| Serial Number | Серийный номер регистрационного свидетельства | – | Положительное, целое число (не более 20 байт) |
| Signature Algorithm | Алгоритм подписи | 1.2.840.113549.1.1.11 | sha256WithRSAEncryption |
| Issuer | Данные издателя регистрационного свидетельства | C=2.5.4.6  L=2.5.4.7  S=2.5.4.8  O=2.5.4.10  CN =2.5.4.3 | C = KZ (обязательное поле)  L = АСТАНА (обязательное поле)  S = АСТАНА (обязательное поле)  O = РМК «МЕМЛЕКЕТТІК ТЕХНИКАЛЫҚ ҚЫЗМЕТ» (обязательное поле)  CN = ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (RSA) (обязательное поле) |
| Validity from | Время начала срока действия | UTC TIME | Действителен с: YYMMDDHHMMSSZ GMT |
| Validity to | Время окончания срока действия | UTC TIME | Действителен по: YYMMDDHHMMSSZ GMT |
| Subject | Данные Владельца регистрационного свидетельства | CN =2.5.4.3  OU=2.5.4.11  O=2.5.4.10  L=2.5.4.7  S=2.5.4.8  C=2.5.4.6 SERIALNUMBER = 2.5.4.5 | CN = Наименование сервиса (обязательное поле)  OU = Подразделение (обязательное поле)  O = Наименование организации (обязательное поле)  L = Город (обязательное поле)  S = Область (обязательное поле)  C = KZ (обязательное поле)  SERIALNUMBER = IIN012345678910 (обязательное поле) |
| Public Key | Значение открытого ключа (2048 бит) | 1.2.840.113549.1.1.1 | Значение |
| Дополнительные поля регистрационного свидетельства в формате Х.509 | | | |
| Subject Key Identifier | Идентификатор ключа субъекта | 2.5.29.14 | Значение идентификатор ключа субъекта в шестнадцатеричном формате |
| Authority Key Identifier | Идентификатор ключа центра сертификации | 2.5.29.35 | Значение идентификатора ключа центра сертификации в шестнадцатеричном формате |
| Extended Key Usage | Расширенное использование ключа | 2.5.29.37 | Установка отметки времени (1.3.6.1.5.5.7.3.8) |
| Ceritifcate Authority Information Access | Доступ к информации о центрах сертификации | 1.3.6.1.5.5.7.1.1 | [1]Доступ к сведениям центра сертификации  Метод доступа = Поставщик центра сертификации (1.3.6.1.5.5.7.48.2)  Дополнительное имя:  URL=http://pki.gov.kz/cert/pki\_rsa.cer  [2]Доступ к сведениям центра сертификации Метод доступа = Протокол определения состояния регистрационного свидетельства через сеть (1.3.6.1.5.5.7.48.1)  Дополнительное имя: URL=http://ocsp.pki.gov.kz/ocsp/ |
| Crl Distribution Points | Точки распространения списков отзыва | 2.5.29.31 | [1]Точка распределения списка отзыва (CRL)  Имя точки распространения:  Полное имя:  URL=http://crl.pki.gov.kz/rsa.crl  URL=http://crl1.pki.gov.kz/rsa.crl |
| Freshest Crl Distribution Points | Новейший CRL | 2.5.29.46 | [1]Новейший CRL  Имя точки распространения:  Полное имя:  URL=http://crl.pki.gov.kz/d\_rsa.crl  URL=http://crl1.pki.gov.kz/d\_rsa.crl |
| Digital Signature | Цифровая подпись Центра сертификации (4096 бит) | 1.2.840.113549.1.1.11 | sha256WithRSAEncryption |

Приложение 8           
к Правилам выдачи, хранения,  
отзыва регистрационных       
свидетельств и подтверждения    
принадлежности и действительности  
открытого ключа электронной    
цифровой подписи национальным   
удостоверяющим центром      
Республики Казахстан

Форма

**Заявление**  
**на отзыв регистрационных свидетельств НУЦ от физического лица,**  
**физического лица - владельца доменного имени интернет-ресурса,**  
**физического лица-нерезидента**

Идентификационные данные физического лица:  
ИИН: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Фамилия: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Имя: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Отчество (при наличии): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Адрес электронной почты: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Телефон: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Идентификационные данные регистрационных свидетельств:  
Серийные номера:  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Дата выдачи: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
С пользовательским соглашением НУЦ ознакомлен и подтверждаю свое  
согласие на обработку моих персональных данных в целях отзыва  
регистрационных свидетельств и получения уведомлений на электронную  
почту.

Дата обращения в НУЦ «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_ г.

Подпись физического лица (представителя физического лица) \_\_\_\_\_\_\_\_\_\_\_

Приложение 9           
к Правилам выдачи, хранения,  
отзыва регистрационных       
свидетельств и подтверждения    
принадлежности и действительности  
открытого ключа электронной    
цифровой подписи национальным   
удостоверяющим центром      
Республики Казахстан

Форма

                                Заявление  
     на отзыв регистрационных свидетельств НУЦ от юридического лица,  
      индивидуального предпринимателя, осуществляющего деятельность  
           в виде совместного предпринимательства, юридического  
           лица - владельца доменного имени интернет-ресурса,  
         участника информационной системы «Казначейство-клиент»,  
                      юридического лица-нерезидента

Идентификационные данные юридического лица:  
БИН: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Наименование организации или ИП: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
ИИН: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Фамилия: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Имя: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Отчество (при наличии):\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_код  
ГУ/СКС (для пользователей информационной системы  
«Казначейство-Клиент»): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Роль (для пользователей информационной системы «Казначейство  
Клиент»): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Наименование области: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Город: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Телефон: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Идентификационные данные регистрационных свидетельств:  
Серийные номера: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
С пользовательским соглашением НУЦ ознакомлен и подтверждаю свое  
согласие на обработку моих персональных данных в целях отзыва  
регистрационных свидетельств и получения уведомлений на электронную  
почту.

Дата обращения в НУЦ «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_ г.

Руководитель\*                              \_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
                                           (подпись) (имя, фамилия)

МП (при наличии)

      \*В случае предоставления выписки из приказа об увольнении  
владельца регистрационного свидетельства НУЦ РК, заявление может быть  
подписано владельцем регистрационного свидетельства НУЦ. В данном  
случае нет необходимости в печати организации.

© 2012. РГП на ПХВ «Институт законодательства и правовой информации Республики Казахстан» Министерства юстиции Республики Казахстан