

**АКЦИОНЕРНОЕ ОБЩЕСТВО  
«НАЦИОНАЛЬНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ»**

Утверждаю  
Управляющий директор по  
информационной безопасности  
акционерного общества  
«Национальное информационное  
технологии»

\_\_\_\_\_ К. Тилеубеков  
«    » \_\_\_\_\_ 2024 года

**ПОЛИТИКА ПРИМЕНЕНИЯ РЕГИСТРАЦИОННЫХ СВИДЕТЕЛЬСТВ  
НАЦИОНАЛЬНОГО УДОСТОВЕРЯЮЩЕГО ЦЕНТРА РЕСПУБЛИКИ  
КАЗАХСТАН  
(CERTIFICATE POLICY)  
Версия 5.0**

**Астана, 2024 г.**

## КОНТРОЛИ ВЕРСИЙ

№	Статус	Дата	Автор	Описание изменений
5.0	Действующая	26.07.2024	Стрыгина А.Г.	Актуализация информации
4.0	Утратившая силу	10.07.2024	Стрыгина А.Г.	Актуализация информации
3.0	Утратившая силу	07.11.2016	Досанов Г.К.	Политика приведена в соответствие с требованиями международного стандарта Web Trust
2.0	Утратившая силу	13.09.2016	Досанов Г.К.	Политика приведена в соответствие с требованиями международного стандарта Web Trust
1.0	Утратившая силу	22.05.2015	Сейфулина А.О.	-

## Содержание

Понятия и аббревиатуры .....	5
<b>1. Введение .....</b>	<b>7</b>
1.1. Обзор .....	7
1.2. Наименование и идентификация документа .....	7
1.3. Участники НУЦ РК .....	8
1.3.1. НУЦ РК .....	8
1.3.2. Центры регистрации .....	8
1.4. Использование регистрационного свидетельства владельца РС НУЦ РК .....	8
1.4.1. Разрешённые способы использования регистрационных свидетельств владельцев РС НУЦ РК .....	8
1.4.2. Запрещённые способы использования регистрационных свидетельств владельцев РС НУЦ РК .....	8
1.5. Управление Политикой .....	8
1.5.1. Организация, администрирующая документ .....	8
1.5.2. Контактное лицо .....	9
1.5.3. Лицо, определяющее соответствие УЦ требованиям политики .....	9
1.5.4. Процедура квалифицирования регламента .....	9
<b>2. Ответственность в отношении публикации и хранения .....</b>	<b>9</b>
2.1. Хранилище и доступность публичной информации .....	9
2.2. Публикация информации о регистрационных свидетельствах .....	10
2.3. Период публикации информации .....	10
2.4. Контроль доступа к публичной информации .....	10
<b>3. Идентификация и аутентификация .....</b>	<b>Ошибка! Закладка не определена.</b>
3.1. Присваивание имён .....	10
3.2. Проверка (идентификация) услугополучателей при выдаче регистрационного свидетельства владельца РС НУЦ РК .....	10
3.3. Проверка (Идентификация) услугополучателя при повторном получении регистрационного свидетельства владельца РС НУЦ РК .....	11
3.4. Проверка (Идентификация) владельца РС НУЦ РК при отзыве регистрационных свидетельств .....	11
<b>4. Операционные требования к жизненному циклу регистрационного свидетельства владельца РС НУЦ РК .....</b>	<b>11</b>
4.1. Порядок подачи заявления на выдачу регистрационных свидетельств НУЦ РК .....	11
4.2. Обработка заявления на выдачу регистрационного свидетельства владельца РС НУЦ РК .....	11
4.3. Выдача регистрационных свидетельств владельцам РС НУЦ РК .....	11
4.4. Принятие регистрационного свидетельства владельца РС НУЦ РК .....	11
4.5. Использование ключевой пары и регистрационного свидетельства владельца РС НУЦ РК .....	11
4.6. Обновление регистрационного свидетельства владельца РС НУЦ РК .....	12
4.7. Переподчинение регистрационного свидетельства .....	12
4.8. Изменение регистрационных свидетельств .....	12
4.9. Отзыв регистрационного свидетельства владельца РС НУЦ РК .....	12
4.10. Службы проверки статуса регистрационного свидетельства владельцев РС НУЦ РК .....	12
4.11. Окончание подписки .....	12
4.12. Депонирование и восстановление ключевой пары .....	12
<b>5. Управленческие, операционные и физические контроли .....</b>	<b>12</b>
5.1. Контроль физической безопасности активов НУЦ РК .....	12
5.2. Ответственность и контроль деятельности НУЦ РК .....	12
5.3. Обеспечение безопасности работников НУЦ РК .....	13
5.4. Документирование событий (журналирование) в ИС НУЦ РК .....	13
5.5. Архив записей .....	13
5.6. Выпуск ключей НУЦ РК .....	13
5.7. Компрометация и аварийное восстановление ключей НУЦ РК .....	13
5.8. Прекращение деятельности НУЦ РК .....	13
<b>6. Контроль технической безопасности НУЦ РК .....</b>	<b>14</b>
6.1. Выпуск и установка ключевых пар НУЦ РК и владельцев РС НУЦ РК .....	14
6.2. Контроль защиты закрытых ключей НУЦ РК и владельцев РС НУЦ РК, а также управления жизненным циклом криптографического аппаратного обеспечения НУЦ РК .....	14
6.3. Другие аспекты управления ключевой парой НУЦ РК .....	14
6.4. Контроль компьютерной безопасности .....	14
6.5. Контроль жизненного цикла безопасности .....	14
<b>7. ПРОФИЛИ РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА владельцев РС НУЦ РК УЦ И СОРС .....</b>	<b>14</b>
7.1. Контроли безопасности сетей .....	14



<b>7.2. Профиль OSCP .....</b>	<b>15</b>
<b>8. Структура регистрационного свидетельства НУЦ РК .....</b>	<b>15</b>
8.1. Структура переподчиненного регистрационного свидетельства НУЦ РК и СОПС .....	15
8.1.1. Структура переподчиненного регистрационного свидетельства Национального удостоверяющего центра Республики Казахстан (на алгоритме RSA) .....	15
8.1.2. Структура переподчиненного регистрационного свидетельства Национального удостоверяющего центра Республики Казахстан (на алгоритме ГОСТ) .....	16
8.1.3. Информация о списке отозванных регистрационных свидетельств RSA Национального удостоверяющего центра Республики Казахстан .....	17
8.1.4. Информация о списке отозванных регистрационных свидетельств GOST Национального удостоверяющего центра Республики Казахстан .....	18
8.1.5. Информация о списке отозванных регистрационных свидетельств RSA (Delta CRL) Национального удостоверяющего центра Республики Казахстан .....	18
8.1.6. Информация о списке отозванных регистрационных свидетельств GOST (Delta CRL) Национального удостоверяющего центра Республики Казахстан .....	19
8.1.7. Структура регистрационного свидетельства OSCP GOST Национального удостоверяющего центра Республики Казахстан .....	19
8.1.8. Структура регистрационного свидетельства TSP GOST Национального удостоверяющего центра Республики Казахстан .....	20
8.2. Структура регистрационного свидетельства владельца PC НУЦ РК .....	22
8.2.1. Структура регистрационного свидетельства пользователя (физическое лицо) Национального удостоверяющего центра Республики Казахстан (для подписи) на алгоритме RSA .....	22
8.2.2. Структура регистрационного свидетельства пользователя (физическое лицо) Национального удостоверяющего центра Республики Казахстан (для подписи) .....	24
8.2.3. Структура регистрационного свидетельства пользователя (юридическое лицо или совместное предпринимательство) Национального удостоверяющего центра Республики Казахстан (для подписи) .....	26
8.2.4. Структура регистрационного свидетельства пользователя (ИС Казначейство -Клиент) Национального удостоверяющего центра Республики Казахстан (для подписи) .....	29
8.2.5. Структура регистрационного свидетельства SSL физического лица Национального удостоверяющего центра Республики Казахстан .....	31
8.2.6. Структура регистрационного свидетельства SSL юридического лица Национального удостоверяющего центра Республики Казахстан .....	33
8.2.7. Структура регистрационного свидетельства пользователя (физическое лицо) Национального удостоверяющего центра Республики Казахстан, предназначенного для использования информационной системой (для подписи) .....	35
8.2.8. Структура регистрационного свидетельства пользователя (юридическое лицо) Национального удостоверяющего центра Республики Казахстан, предназначенного для использования информационной системой (для подписи) .....	37
<b>9. Испытания на соответствие требованиям информационной безопасности .....</b>	<b>39</b>
9.1. Периодичность и основания проведения испытаний .....	39
<b>10. Правовая деятельность .....</b>	<b>39</b>
10.1. Оплата услуг .....	39
10.2. Конфиденциальность персональных данных владельцев PC НУЦ РК .....	39
10.3. Права на интеллектуальную собственность .....	40
10.4. Срок действия и порядок прекращения действия .....	40
10.5. Индивидуальные уведомления и взаимодействие с участниками .....	40



## ПОНЯТИЯ И АББРЕВИАТУРЫ

В настоящем документе используются следующие понятия:

Термин	Определение
Политика	Политика применения регистрационных свидетельств Национального удостоверяющего центра Республики Казахстан
Регистрационное свидетельство	Электронный документ, выдаваемый удостоверяющим центром для подтверждения соответствия электронной цифровой подписи
Внутренняя контрольная среда	Совокупность контролей процессов НУЦ РК
Журнал работ НУЦ РК	Файл с записями о событиях ИС НУЦ РК в хронологическом порядке
Интернет-ресурс НУЦ РК	Интернет-ресурс НУЦ РК <a href="http://www.pki.gov.kz">www.pki.gov.kz</a> - интернет-ресурс национального удостоверяющего центра Республики Казахстан, посредством которого акционерным обществом «Национальные информационные технологии» осуществляется прием заявлений, и выдача результатов на выпуск регистрационных свидетельств
Ключевая пара	Набор, состоящий из двух ключей: закрытого (секретного) ключа и открытого ключа
Открытый ключ ЭЦП	Последовательность электронных цифровых символов, доступная любому лицу и предназначенная для подтверждения подлинности электронной цифровой подписи в электронном документе
Государственная корпорация	Государственная корпорация «Правительство для граждан» юридическое лицо, созданное по решению Правительства Республики Казахстан для оказания государственных услуг в соответствии с законодательством Республики Казахстан, организации работы по приему заявлений на оказание государственных услуг и выдаче их результатов услугополучателю по принципу «одного окна», обеспечения оказания государственных услуг в электронной форме
МИД РК	Министерство иностранных дел Республики Казахстан

В настоящей Политике используются следующие аббревиатуры:

Аббревиатура	Определение
RFC	(Request for Comments) Документ из серии пронумерованных информационных документов Интернета, содержащих технические спецификации и стандарты, широко применяемые во всемирной сети
TSP	(Time Stamp Protocol – протокол штампа времени) Криптографический протокол, позволяющий создавать доказательство факта существования электронного документа на определённый момент времени
OCSP	(Online Certificate Status Protocol) Онлайн проверка регистрационного свидетельства на аннулирование, основанная на протоколе On-line Certificate Status Protocol
WebTrust	Международный стандарт «Принципы и критерии услуг в области доверия для удостоверяющих центров», версия 2.0 («Trust Service Principles and Criteria for Certification Authorities Version 2.0»)
ИОК	Инфраструктура открытых ключей - комплекс
КУЦ РК	Корневой удостоверяющий центр Республики Казахстан - удостоверяющий центр, осуществляющий подтверждение принадлежности и действительности открытых ключей электронной цифровой подписи удостоверяющих центров

НУЦ РК	Национальный удостоверяющий центр Республики Казахстан) -удостоверяющий центр, предоставляющий средства электронной цифровой подписи и регистрационные свидетельства физическим или юридическим лицам для формирования электронных документов в государственных и негосударственных информационных системах
АО НИТ	Акционерное общество «Национальные информационные технологии»
РК	Республика Казахстан
СОРС	Список отозванных регистрационных свидетельств - часть регистра регистрационных свидетельств, содержащая сведения о регистрационных свидетельствах, действие которых прекращено, их серийные номера, дату и причину отзыва (аннулирования)
УЦ	Удостоверяющий Центр
ЭЦП	Электронная цифровая подпись - набор электронных цифровых символов, созданный средствами электронной цифровой подписи и подтверждающий достоверность электронного документа, его принадлежность и неизменность содержания.
ИС	Информационная система
Владелец РС	Владелец регистрационного свидетельства НУЦ РК; Физическое или юридическое лицо, на имя которого выдано регистрационное свидетельство, правомерно владеющее закрытым ключом, соответствующим открытому ключу, указанному в регистрационном свидетельстве
ЕТС ГО	Единая транспортная среда государственных органов - сеть телекоммуникаций, входящая в информационно-коммуникационную инфраструктуру «электронного правительства» и предназначенная для обеспечения взаимодействия локальных (за исключением локальных сетей, имеющих доступ к Интернету), ведомственных и корпоративных сетей телекоммуникации государственных органов, их подведомственных организаций и органов местного самоуправления, а так же иных субъектов информатизации определенных уполномоченным органом с соблюдением требуемого уровня информационной безопасности
Участники	Информационные системы и другие заинтересованные лица использующие сервисы НУЦ РК



## 1 ВВЕДЕНИЕ

Настоящий документ описывает Политику применения регистрационных свидетельств национального удостоверяющего центра Республики Казахстан (далее – Политика). Политика определяет деятельность НУЦ РК в отношении услуг, связанных с жизненным циклом регистрационных свидетельств НУЦ РК и применима ко всем владельцам РС и участникам НУЦ РК.

Национальный удостоверяющий центр Республики Казахстан создан в целях предоставления регистрационных свидетельств физическим и юридическим лицам. Национальный удостоверяющий центр Республики Казахстан осуществляет деятельность в соответствии со следующими законодательными и нормативно-правовыми актами Республики Казахстан, внутренними и публичными документами:

- 1) Закон Республики Казахстан «Об информатизации»;
- 2) Закон Республики Казахстан «Об электронном документе и электронной цифровой подписи»;
- 3) Закон Республики Казахстан от «О персональных данных и их защите»;
- 4) 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»;
- 5) Приказ Министра по инвестициям и развитию Республики Казахстан от 9 декабря 2015 года № 1187 «Об утверждении Правил проверки подлинности электронной цифровой подписи»;
- 6) Приказ Министра по инвестициям и развитию Республики Казахстан от 9 декабря 2015 года № 1184 «Об утверждении Типового положения удостоверяющего центра»;
- 7) СТ РК 1073-2007. Средства криптографической защиты информации. Общие требования;
- 8) Правила применения регистрационных свидетельств НУЦ РК (Certificate practice statement).

Настоящая Политика соответствует требованиям следующих стандартов, актуальных на момент публикации Политики:

- 9) базовые требования к выпуску и управлению публичными регистрационными свидетельствами, версия 1.1.9 (Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, version 1.1.9);

рекомендации руководства по разработке политик применения регистрационных свидетельств и инструкций по применению регистрационных свидетельств инфраструктуры открытых ключей в соответствии со стандартом X.509 «Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework» (далее — «RFC 3647»).

### 1.1. Обзор

Настоящая Политика применима ко всем владельцам РС и участникам НУЦ РК.

Настоящая Политика состоит из 10 разделов. Политика является высокоуровневым документом, принадлежащим НУЦ РК, более детальная информация изложена в Правилах применения регистрационных свидетельств национального удостоверяющего центра Республики Казахстан.

### 1.2. Наименование и идентификация документа

Наименование документа	настоящего	Политика применения регистрационных свидетельств Национального удостоверяющего центра Республики Казахстан
Версия документа		5.0
Введен в действие		
Ссылка на актуальную версию документа		

### 1.3. Участники НУЦ РК

#### 1.3.1. НУЦ РК

НУЦ РК является удостоверяющим центром, который выдает регистрационные свидетельства. НУЦ РК осуществляет деятельность, которая непосредственно связана с ИОК, а именно:

- 1) получение и обработка запросов на выдачу и отзыв регистрационных свидетельств;
- 2) выдача и отзыв регистрационных свидетельств владельцев РС НУЦ РК;
- 3) публикация и поддержка СОРС и промежуточных списков (далее – дельта СОРС);
- 4) обработка запросов на сервис OCSP;
- 5) постановка штампа метки времени TSP.

#### 1.3.2. ЦЕНТРЫ РЕГИСТРАЦИИ

В НУЦ РК функцию центров регистрации выполняют филиалы Государственной корпорации и структурное подразделение АО «НИТ». Взаимодействие Государственной корпорации и АО «НИТ» осуществляется на основе Регламента взаимодействия АО «НИТ» и Государственной корпорации по оказанию государственной услуги «Выдача и отзыв регистрационного свидетельства НУЦ РК».

Более подробная информация изложена в Правилах применения регистрационных свидетельств национального удостоверяющего центра Республика Казахстан.

### 1.4. Использование регистрационного свидетельства владельца РС НУЦ РК

#### 1.4.1. РАЗРЕШЕННЫЕ СПОСОБЫ ИСПОЛЬЗОВАНИЯ РЕГИСТРАЦИОННЫХ СВИДЕТЕЛЬСТВ ВЛАДЕЛЬЦЕВ РС НУЦ РК

Регистрационные свидетельства пользователей применимы для следующих целей:

- 1) проверка электронной цифровой подписи;
- 2) аутентификация пользователей в государственных и негосударственных ИС;
- 3) защита канала передачи информации между пользователем и интернет-ресурсом (SSL);
- 4) шифрование почтовых сообщений;
- 5) защиты VPN каналов.

#### 1.4.2. ЗАПРЕЩЕННЫЕ СПОСОБЫ ИСПОЛЬЗОВАНИЯ РЕГИСТРАЦИОННЫХ СВИДЕТЕЛЬСТВ ВЛАДЕЛЬЦЕВ РС НУЦ РК

Способы использования регистрационных свидетельств владельцев РС НУЦ РК не должны противоречить действующему законодательству Республики Казахстан, а также требованиям настоящей Политики.

Более подробная информация изложена в Правилах применения регистрационных свидетельств национального удостоверяющего центра Республика Казахстан.

### 1.5. Управление Политикой

#### 1.5.1. ОРГАНИЗАЦИЯ, АДМИНИСТРИРУЮЩАЯ ДОКУМЕНТ

Наименование организации	Акционерное общество «Национальные информационные технологии»
Физический адрес	Республика Казахстан, 010000, г. Астана пр. Мәңгілік Ел 55/15 блок 2.3
Юридический адрес	Республика Казахстан, 010000, г. Астана пр. Мәңгілік Ел 55/15 блок 2.3
Адрес электронной почты	info@pki.gov.kz
Телефон приемной	+7(7172) 701999
Телефон канцелярии	+7 (7172) 701665 (вн. 3395)
Телефон технической поддержки	1414



## 1.5.2. КОНТАКТНОЕ ЛИЦО

Наименование подразделения	Управление инфраструктуры открытых ключей
Наименование должности	Начальник Управления инфраструктуры открытых ключей
Адрес электронной почты	info@pki.gov.kz

## 1.5.3. ЛИЦО, ОПРЕДЕЛЯЮЩЕЕ СООТВЕТСТВИЕ УЦ ТРЕБОВАНИЯМ ПОЛИТИКИ

Управляющий директор по информационной безопасности АО «НИТ» Тилеубеков К. Г., email – info@pki.gov.kz.

Управляющий директор по информационной безопасности АО «НИТ» ответственен за подтверждение соответствия настоящей Политике Правилам применения регистрационных свидетельств НУЦ РК.

Управляющий директор по информационной безопасности АО «НИТ» ответственен за определение общих требований к инфраструктуре открытых ключей к настоящей Политике.

## 1.5.4. ПРОЦЕДУРА КВАЛИФИЦИРОВАНИЯ РЕГЛАМЕНТА

Изменения или дополнения в настоящую Политику вносятся после их проверки на соответствие Правилам применения регистрационных свидетельств НУЦ РК. Предложения по изменениям или дополнениям в Политику вносятся ответственными работниками НУЦ РК и утверждаются приказом Председателем Правления АО «НИТ» или уполномоченным лицом по доверенности.

Утвержденная измененная или дополненная Политика публикуется на Интернет-ресурсе НУЦ РК <https://pki.gov.kz/cps/> в виде отдельного документа, содержащего полный текст Политики, или уведомления о внесении изменений и самих изменений с указанием последовательного увеличивающегося номера версии Политики. Все устаревшие версии Политики также остаются опубликованными на Интернет-ресурсе НУЦ РК. Все устаревшие версии Политики снабжаются пометкой с указанием диапазона дат, действительной силы версии Политики и ссылкой на действующую версию Политики.

## 2. ОТВЕТСТВЕННОСТЬ В ОТНОШЕНИИ ПУБЛИКАЦИИ И ХРАНЕНИЯ

### 2.1. Хранилище и доступность публичной информации

НУЦ РК обеспечивает публичную доступность 24 часа в сутки, 7 дней в неделю следующих материалов на Интернет-ресурсе НУЦ РК:

- 6) Переподчиненное регистрационное свидетельство НУЦ РК по алгоритму RSA;
- 7) Переподчиненное регистрационное свидетельство НУЦ РК по алгоритму ГОСТ;
- 8) Корневое регистрационное свидетельство КУЦ РК по алгоритму RSA;
- 9) Корневое регистрационное свидетельство КУЦ РК по алгоритму ГОСТ;
- 10) Правила применения регистрационных свидетельств НУЦ РК;
- 11) Настоящую Политику;
- 12) Согласие на сбор и обработку данных;
- 13) СОПС;
- 14) Дельта СОПС;
- 15) Службы OCSP;
- 16) Служба TSP.

## **2.2. Публикация информации о регистрационных свидетельствах**

СОРС НУЦ РК предоставляется в электронной форме и формате, определенном рекомендациями RFC 5280 и настоящей Политики. НУЦ РК публикует следующие виды СОРС:

1. СОРС для регистрационных свидетельств на алгоритме RSA;
2. СОРС для регистрационных свидетельств на алгоритме ГОСТ.

НУЦ РК также предоставляет службу анонимной проверки статуса регистрационного свидетельства владельца РС НУЦ РК посредством службы OCSP через интернет и ЕТС ГО. НУЦ РК предоставляет службу анонимной поставки «Штампа времени» владельцам РС НУЦ РК посредством службы TSP.

Более подробная информация изложена в Правилах применения регистрационных свидетельств национального удостоверяющего центра Республика Казахстан.

## **2.3. Период публикации информации**

Базовый СОРС публикуется раз в сутки. Срок действия базового СОРС составляет 25 часов.

Более подробная информация изложена в Правилах применения регистрационных свидетельств национального удостоверяющего центра Республика Казахстан.

## **2.4. Контроль доступа к публичной информации**

В НУЦ РК реализованы меры информационной и физической безопасности с целью предотвращения несанкционированного внесения, изменения или удаления информации, содержащейся в СОРС формируемого ИС НУЦ РК.

Для исключения высокой загруженности Интернет канала, информационным системам выполняющих проверку регистрационных свидетельств на основе базового СОРС необходимо предусмотреть исключение случаев скачивания базового СОРС (rsa.crl и gost.crl) больше 1-2 раз в сутки, а также выполнять скачивание дельта СОРС (d\_rsa.crl и d\_gost.crl) не более 1 раза в час. Либо выполнять проверку действия регистрационного свидетельства посредством использования службы OCSP (<http://ocsp.pki.gov.kz>).

В случае выявления случаев частого скачивания СОРС, НУЦ РК имеет право произвести временное блокирование, либо установку лимита по количеству скачиваний для данных IP адресов информационных систем.

# **3. ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ**

## **3.1. Присваивание имен**

Регистрационное свидетельство владельца РС НУЦ РК содержат отличительные имена в DN-имени в формате рекомендуемым стандартом X.501 «Information technology - Open Systems Interconnection - The Directory: Models» из серии рекомендуемых стандартов ITU-T X.500

Более подробная информация изложена в Правилах применения регистрационных свидетельств национального удостоверяющего центра Республика Казахстан.

## **3.2. Проверка (идентификация) услугополучателей при выдаче регистрационного свидетельства владельца РС НУЦ РК**

Подтверждение принадлежности и действительности открытого ключа ЭЦП ЦР осуществляется на основании заявления на выдачу регистрационных свидетельств НУЦ РК.

Более подробная информация изложена в Правилах применения регистрационных свидетельств национального удостоверяющего центра Республика Казахстан.



### **3.3. Проверка (Идентификация) услугополучателя при повторном получении регистрационного свидетельства владельца РС НУЦ РК**

НУЦ РК не предоставляет возможности повторного получения регистрационных свидетельств владельца РС НУЦ РК, идентичных выпущенным ранее регистрационным свидетельствам НУЦ РК при утрате или их повреждении.

Более подробная информация изложена в Правилах применения регистрационных свидетельств национального удостоверяющего центра Республика Казахстан.

### **3.4. Проверка (Идентификация) владельца РС НУЦ РК при отзыве регистрационных свидетельств**

Отзыв регистрационного свидетельства осуществляется на основании заявления. Заявление должно соответствовать требованиям законодательства Республики Казахстан.

Более подробная информация изложена в Правилах применения регистрационных свидетельств национального удостоверяющего центра Республика Казахстан.

## **4. ОПЕРАЦИОННЫЕ ТРЕБОВАНИЯ К ЖИЗНЕННОМУ ЦИКЛУ РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА ВЛАДЕЛЬЦА РС НУЦ РК**

### **4.1. Порядок подачи заявление на выдачу регистрационных свидетельств НУЦ РК**

Заявление на выдачу регистрационного свидетельства владельца РС НУЦ РК имеют право подавать:

- 1) физические лица;
- 2) юридические лица.

### **4.2. Обработка заявления на выдачу регистрационного свидетельства владельца РС НУЦ РК**

Более подробная информация изложена в Правилах применения регистрационных свидетельств национального удостоверяющего центра Республика Казахстан.

### **4.3. Выдача регистрационных свидетельств владельцев РС НУЦ РК**

Регистрационное свидетельство владельца РС НУЦ РК выдается НУЦ РК на основании заявления, оформленного через ИС НУЦ РК.

Более подробная информация изложена в Правилах применения регистрационных свидетельств национального удостоверяющего центра Республика Казахстан.

### **4.4. Принятие регистрационного свидетельства владельца РС НУЦ РК**

НУЦ РК направляет уведомление владельцу РС НУЦ РК посредством электронной почты на адрес, указанный при подаче заявления на выдачу регистрационных свидетельств НУЦ РК.

НУЦ РК не уведомляет доверяющие стороны о выпуске регистрационных свидетельств владельцев РС НУЦ РК.

Более подробная информация изложена в Правилах применения регистрационных свидетельств национального удостоверяющего центра Республика Казахстан.

### **4.5. Использование ключевой пары и регистрационного свидетельства владельца РС НУЦ РК**

Более подробная информация изложена в Правилах применения регистрационных свидетельств национального удостоверяющего центра Республика Казахстан.

#### **4.6. Обновление регистрационного свидетельства владельца РС НУЦ РК**

НУЦ РК не осуществляет обновление данных, увеличение срока действия, внесение изменений и дополнений в структуре регистрационных свидетельств владельца РС НУЦ РК.

Более подробная информация изложена в Правилах применения регистрационных свидетельств национального удостоверяющего центра Республика Казахстан.

#### **4.7. Переподчинение регистрационного свидетельства**

Более подробная информация изложена в Правилах применения регистрационных свидетельств национального удостоверяющего центра Республика Казахстан.

#### **4.8. Изменение регистрационных свидетельств**

Более подробная информация изложена в Правилах применения регистрационных свидетельств национального удостоверяющего центра Республика Казахстан.

#### **4.9. Отзыв регистрационного свидетельства владельца РС НУЦ РК**

Более подробная информация изложена в Правилах применения регистрационных свидетельств национального удостоверяющего центра Республика Казахстан.

#### **4.10. Службы проверки статуса регистрационного свидетельства владельцев РС НУЦ РК**

Более подробная информация изложена в Правилах применения регистрационных свидетельств национального удостоверяющего центра Республика Казахстан.

#### **4.11. Окончание подписки**

Более подробная информация изложена в Правилах применения регистрационных свидетельств национального удостоверяющего центра Республика Казахстан.

#### **4.12. Депонирование и восстановление ключевой пары**

НУЦ РК не допускает депонирование и восстановление ключевых пар владельцев РС и НУЦ РК.

### **5. УПРАВЛЕНЧЕСКИЕ, ОПЕРАЦИОННЫЕ И ФИЗИЧЕСКИЕ КОНТРОЛИ**

#### **5.1. Контроль физической безопасности активов НУЦ РК**

НУЦ РК обеспечивает физическую безопасность систем НУЦ РК в соответствии с действующим законодательством Республики Казахстан. Детальные политики и процедуры мер обеспечения физической безопасности содержат конфиденциальную информацию НУЦ РК и поэтому не публикуются.

Более подробная информация изложена в Правилах применения регистрационных свидетельств национального удостоверяющего центра Республика Казахстан.

#### **5.2. Ответственность и контроль деятельности НУЦ РК**

АО «НИТ» обеспечивает необходимое количество подразделений и работников для функционирования системы внутреннего контроля. В случае вакантности штатной единицы, необходимой для осуществления контроля, АО «НИТ» принимает альтернативные меры контроля исходя из оценки рисков.



Более подробная информация об оказании консультационных услуг для операторов центров регистрации Государственной корпорации и повышения квалификаций работников АО «НИТ» изложена в Правилах применения регистрационных свидетельств Национального удостоверяющего центра Республика Казахстан (Certificate Practice Statement).

### **5.3. Обеспечение безопасности работников НУЦ РК**

АО «НИТ» обеспечивает безопасность работников АО «НИТ» в соответствии с:

- 1) внутренними политиками НУЦ РК по организации физической безопасности;
- 2) внутренними политиками организаций, обеспечивающими размещение систем и работников НУЦ РК;
- 3) законодательством Республики Казахстан.

Более подробная информация изложена в Правилах применения регистрационных свидетельств национального удостоверяющего центра Республика Казахстан.

### **5.4. Документирование событий (журналирование) в ИС НУЦ РК**

НУЦ РК осуществляет ведение и хранение журналов для следующих типов событий:

- 1) события управления жизненным циклом ключевых пар НУЦ РК, в том числе генерация;
  - 2) события управления жизненным циклом регистрационных свидетельств НУЦ РК;
  - 3) события, связанные с обеспечением физической и информационной безопасности НУЦ РК
- НУЦ РК не допускает записи в явном виде ключей и паролей.

### **5.5. Архив записей**

НУЦ РК обеспечивает архивное хранение информации в соответствии с требованиями действующего законодательства Республики Казахстан.

Более подробная информация изложена в Правилах применения регистрационных свидетельств национального удостоверяющего центра Республика Казахстан.

### **5.6. Выпуск ключей НУЦ РК**

НУЦ РК осуществляет выпуск ключевых пар и регистрационных свидетельств НУЦ РК до истечения срока действия переподчиненного регистрационного свидетельства НУЦ РК или в случае компрометации ключевых пар.

Более подробная информация изложена в Правилах применения регистрационных свидетельств национального удостоверяющего центра Республика Казахстан.

### **5.7. Компрометация и аварийное восстановление ключей НУЦ РК**

По фактам происшествий в НУЦ РК, а также при обнаружении факта компрометации или подозрению на компрометацию закрытых ключей НУЦ РК проводятся процедуры в соответствии с требованиями законодательства Республики Казахстан.

Более подробная информация изложена в Правилах применения регистрационных свидетельств национального удостоверяющего центра Республика Казахстан.

### **5.8. Прекращение деятельности НУЦ РК**

В случае необходимости прекращения деятельности НУЦ РК, НУЦ РК предпринимает все меры, необходимые для заблаговременного уведомления об этом владельцев РС и участников НУЦ РК.

Более подробная информация изложена в Правилах применения регистрационных свидетельств национального удостоверяющего центра Республика Казахстан.

## **6. КОНТРОЛЬ ТЕХНИЧЕСКОЙ БЕЗОПАСНОСТИ НУЦ РК**

### **6.1. Выпуск и установка ключевых пар НУЦ РК и владельцев РС НУЦ РК**

НУЦ РК генерирует все ключевые пары, используемые в НУЦ РК. Генерация ключевых пар осуществляется при помощи СКЗИ, сертифицированных на соответствие действующему стандарту Республики Казахстан СТ РК 1073-2007 по второму уровню.

Генерация ключевых пар самого НУЦ РК осуществляется исключительно в соответствии с утвержденным внутренним регламентом, при участии компетентных ответственных работников и при наблюдении сторонних организаций. Церемония генерации ключевых пар НУЦ РК активируется соответствующим протоколом за подписью всех участников процедуры комиссии. Протоколы хранятся и архивируются в соответствии с требованиями действующего законодательства Республики Казахстан и правил применения РС.

Более подробная информация изложена в Правилах применения регистрационных свидетельств национального удостоверяющего центра Республика Казахстан.

### **6.2. Контроль защиты закрытых ключей НУЦ РК и владельцев РС НУЦ РК, а также управления жизненным циклом криптографического аппаратного обеспечения НУЦ РК.**

НУЦ РК поддерживает внутреннюю контрольную среду с целью защиты закрытых ключей НУЦ РК и безопасного управления жизненным циклом криптографического аппаратного обеспечения НУЦ РК.

Более подробная информация изложена в Правилах применения регистрационных свидетельств национального удостоверяющего центра Республика Казахстан.

### **6.3. Другие аспекты управления ключевой парой НУЦ РК**

Более подробная информация изложена в Правилах применения регистрационных свидетельств национального удостоверяющего центра Республика Казахстан.

### **6.4. Контроль компьютерной безопасности**

НУЦ РК использует сертифицированные средства обеспечения компьютерной безопасности, что свидетельствует об успешной оценке высокого уровня безопасности.

НУЦ РК осуществляет периодические оценки уязвимостей в инфраструктуре с оценкой рисков и последующей обработкой рисков.

### **6.5. Контроль жизненного цикла безопасности**

НУЦ РК разрабатывает собственное программное обеспечение. НУЦ РК использует внутренние контроли для определения требований к обновлениям системы и тестированию.

Система внутреннего контроля НУЦ РК предусматривает разделение среды разработки и продуктивной среды, а также разделение полномочий работников в конфликтных ролях разработчиков и администраторов систем.

## **7. ПРОФИЛИ РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА ВЛАДЕЛЬЦЕВ РС НУЦ РК УЦ И СОРС**

### **7.1. Контроли безопасности сетей**

НУЦ РК обеспечивает организационно-технические меры от несанкционированного доступа и атак на свои сети. Политики и процедуры в мероприятиях по контролю безопасности сетей документированы и утверждены, однако не публикуются, поскольку содержат конфиденциальную информацию НУЦ РК.



## 7.2. Профиль OCSP

Версия службы OCSP, используемая НУЦ РК для проверки статуса регистрационного свидетельства, соответствует рекомендациям RFC 6960.

Расширения, обрабатываемые сервисом OCSP, а также их критичность, соответствует рекомендациям RFC 6960.

## 8. СТРУКТУРА РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА НУЦ РК

### 8.1. Структура переподчиненного регистрационного свидетельства НУЦ РК и СОРС

#### 8.1.1. СТРУКТУРА ПЕРЕПОДЧИНЕННОГО РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА НАЦИОНАЛЬНОГО УДОСТОВЕРЯЮЩЕГО ЦЕНТРА РЕСПУБЛИКИ КАЗАХСТАН (НА АЛГОРИТМЕ RSA)

Поле	Описание	OID, критичность	Содержание
Базовые поля регистрационного свидетельства в формате X.509 v3			
Version	Версия Стандарта X.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 C=2.5.4.6	CN = НЕГІЗГІ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (RSA) (обязательное поле); C = KZ (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	C=2.5.4.6 CN =2.5.4.3	C = KZ (обязательное поле) CN = ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (RSA) 2022 (обязательное поле)
PublicKey	Значение открытого ключа (4096 бит)	1.2.840.113549.1.1.1	Значение
Дополнительные поля регистрационного свидетельства в формате X.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)
Certificate Policy	Политика регистрационного свидетельства	2.5.29.32	[1]Политика регистрационного свидетельства:

			Идентификатор политики= 1.2.398.3.3.2 [1,1]Сведения квалifikатора политики: Идентификатор квалifikатора политики = CPS (1.3.6.1.5.5.7.2.1) Квалifikатор: 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://root.gov.kz/cert/* .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/* .crl
Digital Signature	Цифровая подпись центра сертификации (4096 бит)	1.2.840.113549.1.1.11	Значение

### 8.1.2. СТРУКТУРА ПЕРЕПОДЧИНЕННОГО РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА НАЦИОНАЛЬНОГО УДОСТОВЕРЯЮЩЕГО ЦЕНТРА РЕСПУБЛИКИ КАЗАХСТАН (НА АЛГОРИТМЕ ГОСТ)

Поле	Описание	OID, критичность	Содержание
Базовые поля регистрационного свидетельства в формате X.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	1.2.398.3.10.1.1.2.3.2	-
Issuer	Данные Издателя регистрационного свидетельства	CN=2.5.4.3 C=2.5.4.6	C = KZ (обязательное поле) CN = НЕГІЗГІ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (GOST) 2022 (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	C=2.5.4.6 CN =2.5.4.3	C = KZ (обязательное поле) CN = ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (GOST) 2022 (обязательное поле)
Public Key	Значение открытого ключа (1024 бит)	1.2.398.3.10.1.1.2.2	Значение
Key parameter sets	Параметр открытого ключа (СТРК ГОСТ Р 34.10-2015)		Значение Параметр открытого ключа - 1.2.398.3.10.1.1.2.2.1 Алгоритм хэширования 1.2.398.3.10.1.3.3
Дополнительные поля регистрационного свидетельства в формате X.509 v3			



Subject Identifier	Key	Идентификатор ключа субъекта	2.5.29.14	Значение идентификатор ключа субъекта в шестнадцатеричном формате
Authority Identifier	Key	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)
Certificate Policy		Политика регистрационного свидетельства	2.5.29.32	[1] Политика регистрационного свидетельства: Идентификатор политики=1.2.398.3.3.2 [1,1] Сведения квалификатора политики: Идентификатор квалификатора политики = CPS (1.3.6.1.5.5.7.2.1) Квалификатор: <a href="http://pki.gov.kz/cps">http://pki.gov.kz/cps</a>
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= <a href="http://root.gov.kz/cert/*.cer">http://root.gov.kz/cert/*.cer</a>
Crl Distribution Points		Точки распространения списков отзыва	2.5.29.31	[1] Точка распределения списка отзыва (CRL) Имя точки распространения: Полное имя: URL= <a href="http://crl.root.gov.kz/*.crl">http://crl.root.gov.kz/*.crl</a>
Digital Signature		Цифровая подпись центра сертификации (1024 бит)	1.2.398.3.10.1.1.2.3.2	Значение

### 8.1.3. ИНФОРМАЦИЯ О СПИСКЕ ОТОЗВАННЫХ РЕГИСТРАЦИОННЫХ СВИДЕТЕЛЬСТВ RSA НАЦИОНАЛЬНОГО УДОСТОВЕРЯЮЩЕГО ЦЕНТРА РЕСПУБЛИКИ КАЗАХСТАН

Поле	Описание	OID, критичность	Содержание
Базовые поля COPC в формате X.509			
Version	Версия Стандарта X.509	—	V2
Issuer	Данные издателя COPC	C=2.5.4.6 CN=2.5.4.3	C = KZ (обязательное поле); CN = ҰЛТТЫҚ ҚУӘЛАНДЫРУШЫ ОРТАЛЫҚ (RSA) 2022 (обязательное поле)
This Update	Время издания COPC	UTC TIME	Действителен с: YYMMDDHHMMSSZ UTC
Next Update	Следующее обновление COPC	UTC TIME	Действителен по: YYMMDDHHMMSSZ UTC
Signature Algorithm	Алгоритм подписи	1.2.840.113549.1.1.11	sha256WithRSAEncryption
Дополнительные поля COPC в формате X.509			

Number CRL	Порядковый номер CОРС	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 (4096 бит)	1.2.840.113549.1.1.11	Значение

#### 8.1.4. ИНФОРМАЦИЯ О СПИСКЕ ОТОЗВАННЫХ РЕГИСТРАЦИОННЫХ СВИДЕТЕЛЬСТВ GOST НАЦИОНАЛЬНОГО УДОСТОВЕРЯЮЩЕГО ЦЕНТРА РЕСПУБЛИКИ КАЗАХСТАН

Поле	Описание	OID, критичность	Содержание
Базовые поля CОРС в формате X.509			
Version	Версия Стандарта X.509	—	V2
Issuer	Данные Издателя CОРС	C=2.5.4.6 CN =2.5.4.3	C = KZ (обязательное поле); CN = ҰЛТТЫҚ КҰӘЛАНДЫРУШЫ ОРТАЛЫҚ (GOST) 2022 (обязательное поле)
This Update	Время издания CОРС	UTC TIME	Действителен с: YYMMDDHHMMSSZ UTC
Next Update	Следующее обновление CОРС	UTC TIME	Действителен по: YYMMDDHHMMSSZ UTC
Signature Algorithm	Алгоритм подписи	1.2.398.3.10.1.1.2.3.2	-
Дополнительные поля CОРС в формате X.509			
Number CRL	Порядковый номер CОРС	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 (1024 бит)	1.2.398.3.10.1.1.2.3.2	Значение

#### 8.1.5. ИНФОРМАЦИЯ О СПИСКЕ ОТОЗВАННЫХ РЕГИСТРАЦИОННЫХ СВИДЕТЕЛЬСТВ RSA (DELTA CRL) НАЦИОНАЛЬНОГО УДОСТОВЕРЯЮЩЕГО ЦЕНТРА РЕСПУБЛИКИ КАЗАХСТАН

Поле	Описание	OID, критичность	Содержание
Базовые поля CОРС в формате X.509			
Version	Версия Стандарта X.509	—	V2
Issuer	Данные Издателя CОРС	C=2.5.4.6 CN =2.5.4.3	C = KZ (обязательное поле); CN = ҰЛТТЫҚ КҰӘЛАНДЫРУШЫ ОРТАЛЫҚ (RSA) 2022 (обязательное поле)
This Update	Время издания CОРС	UTC TIME	Действителен с: YYMMDDHHMMSSZ UTC
Next Update	Следующее обновление CОРС	UTC TIME	Действителен по: YYMMDDHHMMSSZ UTC



Signature Algorithm	Алгоритм подписи	1.2.840.113549.1.1.11	sha256WithRSAEncryption
Дополнительные поля COPS в формате X.509			
Number CRL	Порядковый номер COPS	2.5.29.20	Последовательно увеличивающийся номер
Authority Identifier	Идентификатор ключа центра сертификации	2.5.29.35	Значение идентификатора ключа центра сертификации в шестнадцатеричном формате
Freshest CRL	Идентификатор разностного COPS	2.5.29.46, critical	
Digital Signature	Цифровая подпись ЦС (4096 бит)	1.2.840.113549.1.1.11	Значение

#### 8.1.6. ИНФОРМАЦИЯ О СПИСКЕ ОТОЗВАННЫХ РЕГИСТРАЦИОННЫХ СВИДЕТЕЛЬСТВ GOST (DELTA CRL) НАЦИОНАЛЬНОГО УДОСТОВЕРЯЮЩЕГО ЦЕНТРА РЕСПУБЛИКИ КАЗАХСТАН

Поле	Описание	OID, критичность	Содержание
Базовые поля COPS в формате X.509			
Version	Версия Стандарта X.509	—	V2
Issuer	Данные Издателя COPS	C=2.5.4.6 CN=2.5.4.3	C = KZ (обязательное поле); CN = ҰЛТТЫҚ КҰӘЛАНДЫРУШЫ ОРТАЛЫҚ (GOST) 2022 (обязательное поле)
This Update	Время издания COPS	UTC TIME	Действителен с: YYMMDDHHMMSSZ UTC
Next Update	Следующее обновление COPS	UTC TIME	Действителен по: YYMMDDHHMMSSZ UTC
Signature Algorithm	Алгоритм подписи	1.2.398.3.10.1.1.2.3.2	-
Дополнительные поля COPS в формате X.509			
Number CRL	Порядковый номер COPS	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 COPS	2.5.29.46, critical	—
Digital Signature	Цифровая подпись центра сертификации (1024 бит)	1.2.398.3.10.1.1.2.3.2	Значение

#### 8.1.7. СТРУКТУРА РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА OSCP GOST НАЦИОНАЛЬНОГО УДОСТОВЕРЯЮЩЕГО ЦЕНТРА РЕСПУБЛИКИ КАЗАХСТАН

Поле	Описание	OID, критичность	Содержание
Базовые поля регистрационного свидетельства в формате X.509			
Version	Версия Стандарта X.509	—	V3

Serial Number	Серийный номер регистрационного свидетельства	-	Положительное, целое число (не более 20 байт)
Signature Algorithm	Алгоритм подписи	1.2.398.3.10.1.1.2.3.2	-
Issuer	Данные издателя регистрационного свидетельства	C=2.5.4.6 CN=2.5.4.3	C = KZ (обязательное поле); CN = ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (GOST) 2022 (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 O=2.5.4.10 C=2.5.4.6	O=ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (обязательное поле); C=KZ (обязательное поле). CN=OCSPP RESPONDER (обязательное поле);
Public Key	Значение открытого ключа (1024 бит)	1.2.398.3.10.1.1.2.2	Значение
Key parameter sets	Параметр открытого ключа (СТРК ГОСТ Р 34.10-2015)		Значение Параметр открытого ключа - 1.2.398.3.10.1.1.2.2.1 Алгоритм хэширования - 1.2.398.3.10.1.3.3
Дополнительные поля регистрационного свидетельства в формате X.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)
OCSPP No Revocation Checking	Проверка безотзывности OCSPP	1.3.6.1.5.5.7.48.1.5	NULL
Key Usage	Использование ключа	2.5.29.15, critical	Цифровая подпись;
Digital Signature	Цифровая подпись центра сертификации (1024 бит)	1.2.398.3.10.1.1.2.3.2	Значение

#### 8.1.8. СТРУКТУРА РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА TSP GOST НАЦИОНАЛЬНОГО УДОСТОВЕРЯЮЩЕГО ЦЕНТРА РЕСПУБЛИКИ КАЗАХСТАН

Поле	Описание	OID, критичность	Содержание
Базовые поля регистрационного свидетельства в формате X.509			
Version	Версия Стандарта X.509	-	V3
Serial Number	Серийный номер регистрационного свидетельства	-	Положительное, целое число (не более 20 байт)



Signature Algorithm	Алгоритм подписи	1.2.398.3.10.1.1.2.3.2	-
Issuer	Данные издателя регистрационного свидетельства	C=2.5.4.6 CN=2.5.4.3	C = KZ (обязательное поле); CN = ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (GOST) 2022 (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 O=2.5.4.10 C=2.5.4.6	O=ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (обязательное поле). C=KZ (обязательное поле); CN=TIME-STAMPING AUTHORITY (обязательное поле);
Public Key	Значение открытого ключа (1024 бит)	1.2.398.3.10.1.1.2.2	Значение
Key parameter sets	Параметр открытого ключа (СТРК ГОСТ Р 34.10-2015)		Значение Параметр открытого ключа - 1.2.398.3.10.1.1.2.2.1; Алгоритм хэширования 1.2.398.3.10.1.3.3
Дополнительные поля регистрационного свидетельства в формате X.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, critical	Установка отметки времени (1.3.6.1.5.5.7.3.8)
Certificate Policy	Политика регистрационного свидетельства	2.5.29.32	[1]Политика регистрационного свидетельства: Идентификатор политики=1.2.398.3.3.2.6 [1,1]Сведения квалификатора политики: Идентификатор квалификатора политики= CPS Квалификатор: <a href="http://pki.gov.kz/cps">http://pki.gov.kz/cps</a>
Certificate Authority Information Access	Доступ к информации центрах сертификации	1.3.6.1.5.5.7.1.1	[1]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= <a href="http://ocsp.pki.gov.kz">http://ocsp.pki.gov.kz</a> [2]Доступ к сведениям центра сертификации Метод доступа = Поставщик центра сертификации (1.3.6.1.5.5.7.48.2) Дополнительное имя: URL= <a href="http://pki.gov.kz/cert/*.cer">http://pki.gov.kz/cert/*.cer</a>
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/*.crl
Freshest Distribution Points	Новейший CRL	2.5.29.46	[1]Новейший CRL Имя точки распространения: Полное имя: URL=http://crl.pki.gov.kz/*.crl
Key Usage	Использование ключа	2.5.29.15, critical	Цифровая подпись;
Digital Signature	Цифровая подпись центра сертификации (1024 бит)	1.2.398.3.10.1.1.2.3.2	Значение

## 8.2. Структура регистрационного свидетельства владельца РС НУЦ РК

### 8.2.1. СТРУКТУРА РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА ПОЛЬЗОВАТЕЛЯ (ФИЗИЧЕСКОЕ ЛИЦО) НАЦИОНАЛЬНОГО УДОСТОВЕРЯЮЩЕГО ЦЕНТРА РЕСПУБЛИКИ КАЗАХСТАН (ДЛЯ ПОДПИСИ) НА АЛГОРИТМЕ RSA

Поле	Описание	OID, критичность	Содержание
Базовые поля регистрационного свидетельства в формате X.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	-
Issuer	Данные издателя регистрационного свидетельства	C=2.5.4.6 CN =2.5.4.3	C = KZ (обязательное поле) CN = ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (RSA) 2022 (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	SERIALNUMBER = 2.5.4.5 SN=2.5.4.4 G=2.5.4.42 CN =2.5.4.3 C=2.5.4.6	SERIALNUMBER = IIN012345678910 (обязательное поле); SN = ФАМИЛИЯ (необязательное поле); G = ОТЧЕСТВО (необязательное поле); CN = ФАМИЛИЯ ИМЯ (обязательное поле); C = KZ (обязательное поле)
PublicKey	Значение открытого ключа (2048 бит)	1.2.840.113549.1.1.1	Значение
Key parameter sets	Набор ключевых параметров		null
Дополнительные поля регистрационного свидетельства в формате X.509			
Subject Key Identifier	Идентификатор ключа субъекта	2.5.29.14	Значение идентификатор ключа субъекта в шестнадцатеричном формате



Authority 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; Согласование ключа
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; Биометрическая идентификация - Значение (необязательное поле)
Certificate Policy	Политика регистрационного свидетельства	2.5.29.32	[1]Политика регистрационного свидетельства: Идентификатор политики=1.2.398.3.3.2 [1,1]Сведения квалификатора политики: Идентификатор квалификатора политики = CPS (1.3.6.1.5.5.7.2.1) Квалификатор: <a href="http://pki.gov.kz/cps">http://pki.gov.kz/cps</a>
Certificate Authority Information Access	Доступ информации центрах сертификации	1.3.6.1.5.5.7.1.1	[1]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= <a href="http://ocsp.pki.gov.kz">http://ocsp.pki.gov.kz</a> [2]Доступ к сведениям центра сертификации Метод доступа = Поставщик центра сертификации (1.3.6.1.5.5.7.48.2) Дополнительное имя: URL= <a href="http://pki.gov.kz/cert/* .cer">http://pki.gov.kz/cert/* .cer</a>
Crl Distribution Points	Точки распространения списков отзыва	2.5.29.31	[1]Точка распределения списка отзыва (CRL) Имя точки распространения: Полное имя: URL= <a href="http://crl.pki.gov.kz/* .crl">http://crl.pki.gov.kz/* .crl</a>
Freshest Crl Distribution Points	Новейший CRL	2.5.29.46	[1]Новейший CRL Имя точки распространения: Полное имя: URL= <a href="http://crl.pki.gov.kz/* .crl">http://crl.pki.gov.kz/* .crl</a>
Subject Alternative Name	Дополнительное имя субъекта		Имя RFC822=адрес электронной почты (необязательное поле)
Key Storage	Хранилище ключей	1.2.398.3.3.5	Доступные хранилища ключей (один из параметров): Защищенный носитель - 1.2.398.3.3.5.2: Удостоверение личности - 1.2.398.3.3.5.2.1.

Digital Signature	Цифровая подпись Центра сертификации (4096 бит)	1.2.840.113549.1.1.11	Значение
-------------------	----------------------------------------------------------	-----------------------	----------

**8.2.2. СТРУКТУРА РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА ПОЛЬЗОВАТЕЛЯ (ФИЗИЧЕСКОЕ ЛИЦО) НАЦИОНАЛЬНОГО УДОСТОВЕРЯЮЩЕГО ЦЕНТРА РЕСПУБЛИКИ КАЗАХСТАН (ДЛЯ ПОДПИСИ)**

Поле	Описание	OID, критичность	Содержание
Базовые поля регистрационного свидетельства в формате X.509			
Version	Версия Стандарта X.509	–	V3
Serial Number	Серийный регистрационного свидетельства номер	–	Положительное, целое число (не более 20 байт)
Signature Algorithm	Алгоритм подписи	1.2.398.3.10.1.1.2.3.2	-
Issuer	Данные издателя регистрационного свидетельства	C=2.5.4.6 CN=2.5.4.3	C = KZ (обязательное поле); CN = ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (GOST) 2022 (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	SERIALNUMBER = 2.5.4.5 SN=2.5.4.4 G=2.5.4.42 CN=2.5.4.3 C=2.5.4.6	G = ОТЧЕСТВО (необязательное поле); C = KZ (обязательное поле) SERIALNUMBER = IIN012345678910 (обязательное поле); SN = ФАМИЛИЯ (необязательное поле); CN = ФАМИЛИЯ ИМЯ (обязательное поле);
Public Key	Значение открытого ключа (1024 бит)	1.2.398.3.10.1.1.2.2	Значение
Key parameter sets	Параметр открытого ключа (СТРК ГОСТ Р 34.10-2015)		Значение Параметр открытого ключа - 1.2.398.3.10.1.1.2.2.1 Алгоритм хэширования 1.2.398.3.10.1.3.3
Дополнительные поля регистрационного свидетельства в формате X.509			
Subject Key Identifier	Идентификатор ключа субъекта	2.5.29.14	Значение идентификатора ключа субъекта в шестнадцатеричном формате
Authority Key Identifier	Идентификатор ключа центра сертификации	2.5.29.35	Значение идентификатора ключа центра сертификации в



Subject Name	Alternative	Дополнительное имя субъекта	имя	Имя RFC822=адрес электронной почты (необязательное поле)
Key Storage		Хранилище ключей	1.2.398.3.3.5	Доступные хранилища ключей (один из параметров): Файловое хранилище - 1.2.398.3.3.5.1; PKCS12 - 1.2.398.3.3.5.1.1; Защищенный носитель - 1.2.398.3.3.5.2; Казтокен - 1.2.398.3.3.5.2.2; eToken 5110 - 1.2.398.3.3.5.2.4; aKey - 1.2.398.3.3.5.2.6; Облачное хранилище (защищенный носитель) - 1.2.398.3.3.5.3; Certex Cloud - 1.2.398.3.3.5.3.1
Digital Signature		Цифровая подпись центра сертификации (1024 бит)	1.2.398.3.10.1.1.2.3.2	Значение

### 8.2.3. СТРУКТУРА РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА ПОЛЬЗОВАТЕЛЯ (ЮРИДИЧЕСКОЕ ЛИЦО ИЛИ СОВМЕСТНОЕ ПРЕДПРИНИМАТЕЛЬСТВО) НАЦИОНАЛЬНОГО УДОСТОВЕРЯЮЩЕГО ЦЕНТРА РЕСПУБЛИКИ КАЗАХСТАН (ДЛЯ ПОДПИСИ)

Поле	Описание	OID, критичность	Содержание
Базовые поля регистрационного свидетельства в формате X.509			
Version	Версия Стандарта X.509	-	V3
Serial Number	Серийный номер регистрационного свидетельства	-	Положительное, целое число (не более 20 байт)
Signature Algorithm	Алгоритм подписи	1.2.398.3.10.1.1.2.3.2	-
Issuer	Данные издателя регистрационного свидетельства	C=2.5.4.6 CN=2.5.4.3	C = KZ (обязательное поле); CN = ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (GOST) 2022 (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	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 C=2.5.4.6	G = ОТЧЕСТВО (необязательное поле); OU = BIN012345678910 (обязательное поле); O = НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ (обязательное поле); C = KZ (обязательное поле)

			шестнадцатеричном формате
Key Usage	Использование ключа	2.5.29.15, critical	Цифровая подпись; Неотрекаемость; Согласование ключа
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; Биометрическая идентификация - Значение (необязательное поле)
Certificate Policy	Политика регистрационного свидетельства	2.5.29.32	[1]Политика регистрационного свидетельства: Идентификатор политики=1.2.398.3.3.2 [1,1]Сведения квалификатора политики: Идентификатор квалификатора политики = CPS (1.3.6.1.5.5.7.2.1) Квалификатор: <a href="http://pki.gov.kz/cps">http://pki.gov.kz/cps</a>
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 = Протокол определения состояния регистрационного свидетельства через сеть (1.3.6.1.5.5.7.48.1) Дополнительное имя: URL= <a href="http://ocsp.pki.gov.kz">http://ocsp.pki.gov.kz</a> [2]Доступ к сведениям центра сертификации Метод доступа = Поставщик центра сертификации (1.3.6.1.5.5.7.48.2) Дополнительное имя: URL= <a href="http://pki.gov.kz/cert/*.*cer">http://pki.gov.kz/cert/*.*cer</a>
Crl Distribution Points	Точки распространения списков отзыва	2.5.29.31	[1]Точка распределения списка отзыва (CRL) Имя точки распространения: Полное имя: URL= <a href="http://crl.pki.gov.kz/*.*crl">http://crl.pki.gov.kz/*.*crl</a>
Freshest Crl Distribution Points	Новейший CRL	2.5.29.46	[1]Новейший CRL Имя точки распространения: Полное имя: URL= <a href="http://crl.pki.gov.kz/*.*crl">http://crl.pki.gov.kz/*.*crl</a>



				SERIALNUMBER = IIN012345678910 (обязательное поле); SN = ФАМИЛИЯ (необязательное поле); CN = ФАМИЛИЯ ИМЯ (обязательное поле);
Public Key	Значение открытого ключа (1024 бит)	1.2.398.3.10.1.1.2.2		Значение
Key parameter sets	Параметр открытого ключа (СТРК ГОСТ Р 34.10-2015)			Значение Параметр открытого ключа 1.2.398.3.10.1.1.2.2.1 Алгоритм хэширования 1.2.398.3.10.1.3.3
Дополнительные поля регистрационного свидетельства в формате X.509				
Subject Key Identifier	Идентификатор субъекта	ключ	2.5.29.14	Значение идентификатор ключа субъекта в шестнадцатеричном формате
Authority Key Identifier	Идентификатор центра сертификации	ключ	2.5.29.35	Значение идентификатора ключа центра сертификации в шестнадцатеричном формате
Key Usage	Использование ключа		2.5.29.15, critical	Цифровая подпись; Неотрекаемость; Согласование ключа
Extended Key Usage	Расширенное использование ключа		2.5.29.37	Защищенная электронная почта -1.3.6.1.5.5.7.3.4; Юридическое лицо/совместное предпринимательство - 1.2.398.3.3.4.1.2; Биометрическая идентификация - Значение (необязательное поле). Доступные идентификаторы (один из параметров): 1.2.398.3.3.4.1.2.1 – Первый руководитель юридического лица/ совместное предпринимательство; 1.2.398.3.3.4.1.2.2 – Лицо, наделенное правом подписи; 1.2.398.3.3.4.1.2.5 – Сотрудник организации
Certificate Policy	Политика регистрационного свидетельства		2.5.29.32	[1]Политика регистрационного свидетельства: Идентификатор политики=1.2.398.3.3.2 [1,1]Сведения квалификатора политики: Идентификатор

				квалификатора политики= CPS (1.3.6.1.5.5.7.2.1) Квалификатор: <a href="http://pki.gov.kz/cps">http://pki.gov.kz/cps</a>
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 = Протокол определения состояния регистрационного свидетельства через сеть (1.3.6.1.5.5.7.48.1) Дополнительное имя: URL= <a href="http://ocsp.pki.gov.kz">http://ocsp.pki.gov.kz</a> [2] Доступ к сведениям центра сертификации Метод доступа = Поставщик центра сертификации (1.3.6.1.5.5.7.48.2) Дополнительное имя: URL= <a href="http://pki.gov.kz/cert/* .cer">http://pki.gov.kz/cert/* .cer</a>
Crl Distribution Points	Точки распространения списков отзыва	2.5.29.31		[1] Точка распределения списка отзыва (CRL) Имя точки распространения: Полное имя: URL= <a href="http://crl.pki.gov.kz/* .crl">http://crl.pki.gov.kz/* .crl</a>
Freshest Crl Distribution Points	Новейший CRL	2.5.29.46		[1] Новейший CRL Имя точки распространения: Полное имя: URL= <a href="http://crl.pki.gov.kz/* .crl">http://crl.pki.gov.kz/* .crl</a>
Subject Alternative Name	Дополнительное субъекта	имя		Имя RFC822=адрес электронной почты (необязательное поле)
Key Storage	Хранилище ключей	1.2.398.3.3.5		Доступные хранилища ключей (один из параметров): Файловое хранилище - 1.2.398.3.3.5.1: PKCS12 - 1.2.398.3.3.5.1.1. Защищенный носитель - 1.2.398.3.3.5.2: Казтокен - 1.2.398.3.3.5.2.2; eToken 5110 - 1.2.398.3.3.5.2.4; aKey - 1.2.398.3.3.5.2.6; Облачное хранилище (защищенный носитель) - 1.2.398.3.3.5.3:



				Certex Cloud 1.2.398.3.3.5.3.1
Digital Signature	Цифровая подпись центра сертификации (1024 бит)	1.2.398.3.10.1.1.2.3.2		Значение

#### 8.2.4. СТРУКТУРА РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА ПОЛЬЗОВАТЕЛЯ (ИС КАЗНАЧЕЙСТВО -КЛИЕНТ) НАЦИОНАЛЬНОГО УДОСТОВЕРЯЮЩЕГО ЦЕНТРА РЕСПУБЛИКИ КАЗАХСТАН (ДЛЯ ПОДПИСИ)

Поле	Описание	OID, Критичность	Содержание
Базовые поля регистрационного свидетельства в формате X.509			
Version	Версия Стандарта X.509	-	V3
Serial Number	Серийный регистрационный номер свидетельства	-	Положительное, целое число (не более 20 байт)
Signature Algorithm	Алгоритм подписи	1.2.398.3.10.1.1.2.3.2	-
Issuer	Данные издателя регистрационного свидетельства	C=2.5.4.6 CN=2.5.4.3	C = KZ (обязательное поле); CN = ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (GOST) 2022 (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	SERIALNUMBER=2.5.4.5 SN=2.5.4.4 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 C=2.5.4.6	G = ОТЧЕСТВО (необязательное поле); OU = BIN012345678910 (обязательное поле); O = НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ (обязательное поле); C = KZ (обязательное поле) SERIALNUMBER = PIN012345678910 (обязательное поле); SN = ФАМИЛИЯ (необязательное поле); CN = ФАМИЛИЯ ИМЯ (обязательное поле); BUSINESSCATEGORY = KS01234 (обязательное поле); DC = ROLE01 (обязательное поле);
Public Key	Значение открытого ключа (1024 бит)	3.10.1.1.2.2	1.2.398. Значение
Key parameter sets	Параметр открытого ключа (СТРК ГОСТ Р 34.10-2015)		Значение Параметр открытого ключа 1.2.398.3.10.1.1.2.2.1

				Алгоритм хэширования 1.2.398.3.10.1.3.3
Дополнительные поля регистрационного свидетельства в формате X.509				
Subject Key Identifier	Идентификатор субъекта	ключа	2.5.29.14	Значение идентификатора ключа субъекта в шестнадцатеричном формате
Authority Key Identifier	Идентификатор центра сертификации	ключа	2.5.29.35	Значение идентификатора ключа центра сертификации в шестнадцатеричном формате
Key Usage	Использование ключа		2.5.29.15, critical	Цифровая подпись; Неотрекаемость; Согласование ключа
Extended Key Usage	Расширенное использование ключа		2.5.29.37	Защищенная электронная почта -1.3.6.1.5.5.7.3.4; Юридическое лицо/совместное предпринимательство - 1.2.398.3.3.4.1.2; Биометрическая идентификация - Значение (необязательное поле); Информационная система К2 -1.2.398.5.19.1.2.2.1
Certificate Policy	Политика регистрационного свидетельства		2.5.29.32	[1]Политика регистрационного свидетельства: Идентификатор политики=1.2.398.3.3.2 [1,1]Сведения квалификатора политики: Идентификатор квалификатора политики= CPS (1.3.6.1.5.5.7.2.1) Квалификатор: <a href="http://pki.gov.kz/cps">http://pki.gov.kz/cps</a>
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 = Протокол определения состояния регистрационного свидетельства через сеть (1.3.6.1.5.5.7.48.1) Дополнительное имя: URL= <a href="http://ocsp.pki.gov.kz">http://ocsp.pki.gov.kz</a> [2]Доступ к сведениям центра сертификации Метод доступа = Поставщик центра сертификации (1.3.6.1.5.5.7.48.2) Дополнительное имя: URL= <a href="http://pki.gov.kz/cert/*">http://pki.gov.kz/cert/*</a> .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/*.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
Subject Alternative Name	Дополнительное имя субъекта		Имя RFC822=адрес электронной почты (необязательное поле)
Key Storage	Хранилище ключей	1.2.398.3.3.5	Доступные хранилища ключей (один из параметров): Защищенный носитель - 1.2.398.3.3.5.2: Казтокен - 1.2.398.3.3.5.2.2; eToken 5110 - 1.2.398.3.3.5.2.4; aKey - 1.2.398.3.3.5.2.6; Облачное хранилище (защищенный носитель) - 1.2.398.3.3.5.3: Certex Cloud - 1.2.398.3.3.5.3.1
Digital Signature	Цифровая подпись центра сертификации (1024 бит)	1.2.398.3.10.1.1.2.3.2	Значение

#### 8.2.5. СТРУКТУРА РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА SSL ФИЗИЧЕСКОГО ЛИЦА НАЦИОНАЛЬНОГО УДОСТОВЕРЯЮЩЕГО ЦЕНТРА РЕСПУБЛИКИ КАЗАХСТАН

Поле	Описание	OID, критичность	Содержание
Базовые поля регистрационного свидетельства в формате X.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	-
Issuer	Данные Издателя регистрационного свидетельства	C=2.5.4.6 CN =2.5.4.3	C = KZ (обязательное поле); CN = ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (RSA) 2022 (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 регистрационного свидетельства	Владельца SERIALNUMBER = 2.5.4.5 CN = 2.5.4.3 C=2.5.4.6	SERIALNUMBER IIN012345678910 (обязательное поле); CN = ДОМЕННОЕ ИМЯ (обязательное поле); C = KZ (обязательное поле)
Public Key	Значение открытого ключа (2048 бит)	1.2.840.113549.1.1.1	Значение
Key parameter sets	Набор параметров	ключевых	
Дополнительные поля регистрационного свидетельства в формате X.509			
Subject Key Identifier	Идентификатор субъекта	ключа 2.5.29.14	Значение идентификатор ключа субъекта в шестнадцатеричном формате
Authority Key Identifier	Идентификатор центра сертификации	ключа 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); Проверка подлинности клиента - 1.3.6.1.5.5.7.3.2; Физическое лицо - 1.2.398.3.3.4.1.1; Биометрическая идентификация - Значение (необязательное поле)
Key Usage	Использование ключа	2.5.29.15, critical	Цифровая подпись, Шифрование ключей
Subject Name	Alternative Дополнительное субъекта	имя	DNS-имя=Доменное имя- 1; DNS-имя= Доменное имя- 2; DNS-имя= N(обязательное поле). Максимальное количество допустимых доменных имен = 10 доменных имен. Имя RFC822=адрес электронной почты (необязательное 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 = Протокол определения состояния регистрационного свидетельства через сеть (1.3.6.1.5.5.7.48.1) Дополнительное имя: URL=http://ocsp.pki.gov.kz [2]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/ *.cer
Certificate Policy	Политика регистрационного свидетельства	2.5.29.32	[1]Политика регистрационного свидетельства: Идентификатор политики=1.2.398.3.3.2 [1,1]Сведения квалификатора политики: Идентификатор квалификатора политики= CPS (1.3.6.1.5.5.7.2.1) 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/* .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
Key Storage	Хранилище ключей	1.2.398.3.3.5	Доступные хранилища ключей (один из параметров): Файловое хранилище - 1.2.398.3.3.5.1: PKCS12 - 1.2.398.3.3.5.1.1; JKS - 1.2.398.3.3.5.1.2.
Digital Signature	Цифровая подпись ЦС (4096 бит)	1.2.840.113549.1.1.1.1	Значение

#### 8.2.6. СТРУКТУРА РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА SSL ЮРИДИЧЕСКОГО ЛИЦА НАЦИОНАЛЬНОГО УДОСТОВЕРЯЮЩЕГО ЦЕНТРА РЕСПУБЛИКИ КАЗАХСТАН

Поле	Описание	OID, критичность	Содержание
Базовые поля регистрационного свидетельства в формате X.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	-
Issuer	Данные издателя регистрационного свидетельства	.4.6 CN =2.5.4.3	C = KZ (обязательное поле); C=2.5 CN = ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (RSA) 2022 (обязательное поле)
Validity from	Время начала действия срока	UTC TIME	Действителен с: YYMMDDHHMMSSZ UTC

Validity to	Время окончания срока действия	UTC TIME	Действителен по: YYMMDDHHMMSSZ UTC
Subject	Данные регистрационного свидетельства	Владельца SERIALNUMBER =2.5.4.5 SN=2.5.4.4 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 = IIN012345678910 (обязательное поле); CN = ДОМЕННОЕ ИМЯ (обязательное поле); OU = BIN012345678910 (обязательное поле); O = НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ (обязательное поле); L = ГОРОД РЕГИСТРАЦИИ ЮРИДИЧЕСКОГО ЛИЦА (обязательное поле); S = ОБЛАСТЬ РЕГИСТРАЦИИ ЮРИДИЧЕСКОГО ЛИЦА (обязательное поле); C = KZ (обязательное поле)
Public Key	Значение открытого ключа (2048 бит или 4096)	1.2.840.113549.1.1.1	Значение
Key parameter sets	Набор ключевых параметров		null
Дополнительные поля регистрационного свидетельства в формате X.509			
Subject Key Identifier	Идентификатор субъекта	ключа 2.5.29.14	Значение идентификатора ключа субъекта в шестнадцатеричном формате
Authority Key Identifier	Идентификатор центра сертификации	ключа 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); Проверка подлинности клиента -1.3.6.1.5.5.7.3.2; Юридическое лицо/совместное предпринимательство - 1.2.398.3.3.4.1.2; Биометрическая идентификация - Значение (необязательное поле)
Key Usage	Использование ключа	2.5.29.15, critical	Цифровая подпись, Шифрование ключей
Subject Alternative Name	Дополнительное имя субъекта	имя	DNS-имя=Доменное имя-1 ; DNS-имя= Доменное имя-2; DNS-имя= N (обязательное поле). Максимальное количество допустимых доменных имен = 10 доменных имен. Имя RFC822=адрес электронной почты (необязательное 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 = Протокол определения состояния



				регистрационного свидетельства через сеть (1.3.6.1.5.5.7.48.1) Дополнительное имя: URL= <a href="http://ocsp.pki.gov.kz">http://ocsp.pki.gov.kz</a> [2]Доступ к сведениям центра сертификации Метод доступа = Поставщик центра сертификации (1.3.6.1.5.5.7.48.2) Дополнительное имя: URL= <a href="http://pki.gov.kz/cert/*.cer">http://pki.gov.kz/cert/*.cer</a>
Certificate Policy	Политика регистрационного свидетельства	2.5.29.32		[1]Политика регистрационного свидетельства: Идентификатор политики=1.2.398.3.3.2 [1,1]Сведения квалификатора политики: Идентификатор квалификатора политики=CPS (1.3.6.1.5.5.7.2.1) Квалификатор: <a href="http://pki.gov.kz/cps">http://pki.gov.kz/cps</a>
Crl Distribution Points	Точки распространения списков отзыва	2.5.29.31		[1]Точка распределения списка отзыва (CRL) Имя точки распространения: Полное имя: URL= <a href="http://crl.pki.gov.kz/*.crl">http://crl.pki.gov.kz/*.crl</a>
Freshest Crl Distribution Points	Новейший CRL	2.5.29.46		[1]Новейший CRL Имя точки распространения: Полное имя: URL= <a href="http://crl.pki.gov.kz/*.crl">http://crl.pki.gov.kz/*.crl</a>
Key Storage	Хранилище ключей	1.2.398.3.3.5		Доступные хранилища ключей (один из параметров): Файловое хранилище - 1.2.398.3.3.5.1; PKCS12 - 1.2.398.3.3.5.1.1; JKS - 1.2.398.3.3.5.1.2.
Digital Signature	Цифровая подпись ЦС (4096 бит)	1.2.840.113549.1.1.1.1		Значение

**8.2.7. СТРУКТУРА РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА ПОЛЬЗОВАТЕЛЯ (ФИЗИЧЕСКОЕ ЛИЦО) НАЦИОНАЛЬНОГО УДОСТОВЕРЯЮЩЕГО ЦЕНТРА РЕСПУБЛИКИ КАЗАХСТАН, ПРЕДНАЗНАЧЕННОГО ДЛЯ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННОЙ СИСТЕМОЙ (ДЛЯ ПОДПИСИ)**

Поле	Описание	OID, Критичность	Содержание
Базовые поля регистрационного свидетельства в формате X.509			
Version	Версия Стандарта X.509	-	V3
Serial Number	Серийный номер регистрационного свидетельства	-	Положительное, целое число (не более 20 байт)
Signature Algorithm	Алгоритм подписи	1.2.398.3.10.1.1.2.3.2	-

Issuer	Данные издателя регистрационного свидетельства	C=2.5.4.6 CN=2.5.4.3	C = KZ (обязательное поле); CN = ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (GOST) 2022 (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	SERIALNUMBER=2.5.4.5 CN=2.5.4.3 UID=0.9.2342.19200300.100.1.1 C=2.5.4.6	C = KZ (обязательное поле) SERIALNUMBER = IIN012345678910 (обязательное поле); CN = НАИМЕНОВАНИЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ (обязательное поле); UID = OID ИНФОРМАЦИОННОЙ СИСТЕМЫ, ВЫДАННЫЙ УПОЛНОМОЧЕННЫМ ОРГАНОМ (обязательное поле);
PublicKey	Значение открытого ключа (1024 бит)	1.2.398.3.10.1.1.2.2	Значение
Key parameter sets	Параметр открытого ключа (СТРК ГОСТ Р 34.10-2015)		Значение Параметр открытого ключа - 1.2.398.3.10.1.1.2.2.1 Алгоритм хэширования 1.2.398.3.10.1.3.3
Дополнительные поля регистрационного свидетельства в формате X.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, Шифрование ключей
Extended Key Usage	Расширенное использование ключа	2.5.29.37	Физическое лицо - 1.2.398.3.3.4.1.1; Информационная система физического лица- 1.2.398.3.3.4.1.1.1
Certificate Policy	Политика регистрационного свидетельства	2.5.29.32	[1]Политика регистрационного свидетельства: Идентификатор политики=1.2.398.3.3.2 [1,1]Сведения квалификатора политики: Идентификатор квалификатора политики= CPS (1.3.6.1.5.5.7.2.1) Квалификатор: <a href="http://pki.gov.kz/cps">http://pki.gov.kz/cps</a>
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 = Протокол определения состояния регистрационного свидетельства через сеть (1.3.6.1.5.5.7.48.1) Дополнительное имя: URL=http://ocsp.pki.gov.kz [2]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/* .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/* .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
Subject Alternative Name	Дополнительное имя субъекта		Имя RFC822=адрес электронной почты (необязательное поле)
Key Storage	Хранилище ключей	1.2.398.3.3.5	Доступные хранилища ключей (один из параметров): Файловое хранилище - 1.2.398.3.3.5.1: PKCS12 - 1.2.398.3.3.5.1.1. Защищенный носитель - 1.2.398.3.3.5.2: Казтокен - 1.2.398.3.3.5.2.2; eToken 5110 - 1.2.398.3.3.5.2.4; aKey - 1.2.398.3.3.5.2.6; Облачное хранилище (защищенный носитель) - 1.2.398.3.3.5.3: Certex Cloud - 1.2.398.3.3.5.3.1.
Digital Signature	Цифровая подпись центра сертификации (1024 бит)	1.2.398.3.10.1.1.2.3.2	Значение

**8.2.8. СТРУКТУРА РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА ПОЛЬЗОВАТЕЛЯ (ЮРИДИЧЕСКОЕ ЛИЦО) НАЦИОНАЛЬНОГО УДОСТОВЕРЯЮЩЕГО ЦЕНТРА РЕСПУБЛИКИ КАЗАХСТАН, ПРЕДНАЗНАЧЕННОГО ДЛЯ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННОЙ СИСТЕМОЙ (ДЛЯ ПОДПИСИ)**

Поле	Описание	OID, Критичность	Содержание
Базовые поля регистрационного свидетельства в формате X.509			
Version	Версия Стандарта X.509	-	V3
Serial Number	Серийный номер регистрационного свидетельства	-	Положительное, целое число (не более 20 байт)
Signature Algorithm	Алгоритм подписи	1.2.398.3.10.1.1.2.3.2	-

Issuer	Данные издателя регистрационного свидетельства	C=2.5.4.6 CN=2.5.4.3	C = KZ (обязательное поле); CN = ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (GOST) 2022 (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 Владелец регистрационного свидетельства	CN=2.5.4.3 UID=0.9.2342.19200300.100.1.1 OU=2.5.4.11 O=2.5.4.10 C=2.5.4.6	OU = BIN012345678910 (обязательное поле); O = НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ (обязательное поле); C = KZ (обязательное поле). CN = НАИМЕНОВАНИЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ (обязательное поле); UID = OID ИНФОРМАЦИОННОЙ СИСТЕМЫ, ВЫДАННЫЙ УПОЛНОМОЧЕННЫМ ОРГАНОМ (обязательное поле);
PublicKey	Значение открытого ключа (1024 бит)	1.2.398.3.10.1.1.2.2	Значение
Key parameter sets	Параметр открытого ключа (СТРК ГОСТ Р 34.10-2015)		Значение Параметр открытого ключа - 1.2.398.3.10.1.1.2.2.1 Алгоритм хэширования 1.2.398.3.10.1.3.3
Дополнительные поля регистрационного свидетельства в формате X.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, Шифрование ключей
Extended Key Usage	Расширенное использование ключа	2.5.29.37	Юридическое лицо/совместное предпринимательство 1.2.398.3.3.4.1.2; Информационная система юридического лица- 1.2.398.3.3.4.1.2.6
Certificate Policy	Политика регистрационного свидетельства	2.5.29.32	[1]Политика регистрационного свидетельства: Идентификатор политики=1.2.398.3.3.2 [1,1]Сведения квалификатора политики: Идентификатор квалификатора политики= CPS (1.3.6.1.5.5.7.2.1) Квалификатор: <a href="http://pki.gov.kz/cps">http://pki.gov.kz/cps</a>
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 = Протокол определения состояния регистрационного свидетельства через сеть (1.3.6.1.5.5.7.48.1)



			Дополнительное имя: URL=http://ocsp.pki.gov.kz [2]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/*.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/*.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
Subject Alternative Name	Дополнительное имя субъекта		Имя RFC822=адрес электронной почты (необязательное поле)
Key Storage	Хранилище ключей	1.2.398.3.3.5	Доступные хранилища ключей (один из параметров): Файловое хранилище - 1.2.398.3.3.5.1: PKCS12 - 1.2.398.3.3.5.1.1. Защищенный носитель - 1.2.398.3.3.5.2: Казтокен - 1.2.398.3.3.5.2.2; eToken 5110 - 1.2.398.3.3.5.2.4; aKey - 1.2.398.3.3.5.2.6; Облачное хранилище (защищенный носитель) - 1.2.398.3.3.5.3: Certex Cloud - 1.2.398.3.3.5.3.1.
Digital Signature	Цифровая подпись центра сертификации (1024 бит)	1.2.398.3.10.1.1.2.3.2	Значение

## 9. ИСПЫТАНИЯ НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В соответствии с Законом Республики Казахстан «Об информатизации» проводятся испытания объектов информатизации «электронного правительства» на соответствие требованиям информационной безопасности.

### 9.1. Периодичность и основания проведения испытаний

Срок действия акта испытаний ограничивается сроком промышленной эксплуатации объекта испытаний или до момента начала модернизации объекта испытаний.

## 10. ПРАВОВАЯ ДЕЯТЕЛЬНОСТЬ

### 10.1. Оплата услуг

НУЦ РК не взимает платы за предоставление государственной услуги «Выдача и отзыв регистрационных свидетельств НУЦ РК».

### 10.2. Конфиденциальность персональных данных владельцев РС НУЦ РК

НУЦ РК обеспечивает защиту персональных данных владельцев РС НУЦ РК в соответствии с действующим законодательством Республики Казахстан.

Более подробная информация изложена в Правилах применения регистрационных свидетельств национального удостоверяющего центра Республика Казахстан.

### **10.3. Права на интеллектуальную собственность**

НУЦ РК оставляет за собой права интеллектуальной собственности на регистрационные свидетельства, которые он выдаёт, и на информацию об их статусе. При этом НУЦ РК не запрещает копирование и распространение регистрационных свидетельств на неисключительной безвозмездной основе, при соблюдении условий полноты копирования и использования регистрационных свидетельств в соответствии с условиями заключенных пользовательских Соглашений. НУЦ РК также не запрещает использование информации о статусе регистрационных свидетельств для выполнения функций доверяющей стороны.

Участники ИС, обслуживаемых НУЦ РК, признают право интеллектуальной собственности НУЦ РК на настоящую Политику и другую документацию НУЦ РК, регламентирующую деятельность УЦ.

### **10.4. Срок действия и порядок прекращения действия**

Настоящая Политика вступает в силу незамедлительно с момента подписания и опубликования ее на интернет-ресурсе НУЦ РК.

### **10.5. Индивидуальные уведомления и взаимодействие с участниками**

НУЦ РК использует любые доступные методы официального уведомления участников НУЦ РК.



**Лист согласования правил применения регистрационных свидетельств  
национального удостоверяющего центра Республики Казахстан (Certificate Policy)**

№	ФИО	Должность	Подпись	Дата
1	Билеутасова Э.А.	Вед. инженер	Э.А. Билеутасова	
2	Саржанов А.Т.	Глав. инж.	А.Т. Саржанов	
3	Кандыбаев А.Е.	Кат. упр.	А.Е. Кандыбаев	
4				