

**АКЦИОНЕРНОЕ ОБЩЕСТВО
«НАЦИОНАЛЬНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ»**

Утверждаю
Управляющий директор по
информационной безопасности
_____ А. Даутбаев
« » _____ 2026
года



**ПОЛИТИКА ПРИМЕНЕНИЯ СЕРТИФИКАТОВ
УДОСТОВЕРЯЮЩЕГО ЦЕНТРА ГОСУДАРСТВЕННЫХ ОРГАНОВ
РЕСПУБЛИКИ КАЗАХСТАН
(CERTIFICATE POLICY)
Версия 7.0**

Астана 2026 г.

КОНТРОЛЬ ВЕРСИЙ

№	Статус	Дата	Автор	Описание изменений
7.0	Действующая	11.09.2026	Мұстафа А.Н.	Приведение в соответствие с Цифровым Кодексом Республики Казахстан
6.0	Утратившая силу	26.07.2024	Мұстафа А.Н.	Актуализация информации
5.0	Утратившая силу	10.07.2024	Мұстафа А.Н.	Актуализация информации
4.0	Утратившая силу	27.10.2022	Мұстафа А.Н.	Актуализация информации
3.0	Утратившая силу	02.07.2020	Калдыбеков А.Е.	Актуализация информации
2.0	Утратившая силу	24.09.2018	Калдыбеков А.Е.	Актуализация информации
1.0	Утратившая силу	07.08.2015	Калдыбеков А.Е.	Актуализация информации

СОДЕРЖАНИЕ

1.	ВВЕДЕНИЕ	7
2.	ОТВЕТСТВЕННОСТЬ В ОТНОШЕНИИ ПУБЛИКАЦИИ И ХРАНЕНИЯ.....	10
3.	ПРИСВАИВАНИЕ ИМЕН	11
4.	ОПЕРАЦИОННЫЕ ТРЕБОВАНИЯ К ЖИЗНЕННОМУ ЦИКЛУ СЕРТИФИКАТА ПОЛЬЗОВАТЕЛЯ УЦ ГО РК	11
5.	ОТЗЫВ И ХРАНЕНИЕ СЕРТИФИКАТОВ УЦ ГО РК	14
6.	ИСПОЛЬЗОВАНИЕ КЛЮЧЕВОЙ ПАРЫ УЦ ГО РК	15
7.	КЛЮЧЕВАЯ ПАРА УЦ ГО РК	16
8.	ПРАВОВЫЕ И БИЗНЕС-ВОПРОСЫ	17
9.	ГАРАНТИИ СТОРОН	17
10.	СРОК ДЕЙСТВИЯ И ПОРЯДОК ПРЕКРАЩЕНИЯ ДЕЙСТВИЯ ПОЛИТИКИ.....	18

ПОНЯТИЯ И АББРЕВИАТУРЫ

В настоящем документе используются следующие понятия:

Термин	Определение
Политика	Политика применения сертификатов Удостоверяющего центра государственных органов Республики Казахстан
Сертификат	сертификат открытого ключа электронной цифровой подписи (далее – сертификат) цифровая запись, удостоверенная электронной цифровой подписью удостоверяющего центра, которая служит для подтверждения соответствия электронной цифровой подписи требованиям, установленным Кодексом
Средства ЭЦП	совокупность программных и технических средств, используемых для создания и проверки подлинности ЭЦП
Сайт УЦ ГО РК	Информационный ресурс УЦ ГО РК https://ucgo.gov.kz/ в сети интернет и ЕТС ГО
Согласие на сбор и обработку персональных данных	разрешение, предоставленное субъектом персональных данных либо его законным представителем собственнику и (или) оператору на сбор и обработку персональных данных, то есть сведений, относящихся к определенному или определяемому на их основании субъекту персональных данных, зафиксированных на электронном, бумажном и (или) ином материальном носителе
Закрытый ключ ЭЦП	цифровые данные, предназначенные для создания электронной цифровой подписи с использованием средств электронной цифровой подписи;
Открытый ключ ЭЦП	цифровые данные, предназначенные для подтверждения подлинности электронной цифровой подписи

Владелец сертификата	физическое или юридическое лицо, на имя которого выдан сертификат открытого ключа электронной цифровой подписи, правомерно владеющее закрытым ключом, соответствующим открытому ключу, указанному в сертификате открытого ключа электронной цифровой подписи
Оператор	сотрудники структурного подразделения АО «НИТ»
Содержание полей сертификата (DN-имя)	имя сертификата – отличительное имя, применяемое для идентификации владельца сертификата или удостоверяющего центра;
защищенный носитель ключевой информации Type-C	защищенный носитель ключевой информации, оснащенный интерфейсом подключения USB Type-C
единая транспортная среда государственных органов (ЕТС ГО)	сеть телекоммуникаций, входящая в инфраструктуру «цифрового правительства» и предназначенная для обеспечения взаимодействия локальных (за исключением локальных сетей, имеющих доступ к Интернету), ведомственных и корпоративных сетей телекоммуникаций государственных органов, их подведомственных организаций и органов местного самоуправления, а также иных субъектов цифровой среды, определенных уполномоченным органом, с соблюдением требуемого уровня кибербезопасности

В настоящей Политике используются следующие аббревиатуры:

Аббревиатура	Определение
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-сервис удостоверяющего центра,

	предоставляющий OCSP-квитанцию, содержащую сведения об отзыве сертификата открытого ключа электронной цифровой подписи либо об отсутствии такого отзыва на момент выдачи OCSP-квитанции в соответствии с RFC 6960
ИОК	(Инфраструктура Открытых Ключей) Комплекс цифровых систем, организационных и технических мероприятий, направленный на управление сертификатами в соответствии с Цифровым Кодексом Республики Казахстан
КУЦ РК	(Корневой Удостоверяющий Центр Республики Казахстан) удостоверяющий центр, осуществляющий подтверждение принадлежности и действительности открытых ключей электронной цифровой подписи удостоверяющих центров
УЦ ГО РК	(Удостоверяющий центр государственных органов Республики Казахстан) удостоверяющий центр, предоставляющий средства электронной цифровой подписи и сертификаты открытых ключей электронной цифровой подписи должностным лицам государственных органов для формирования и проверки электронной цифровой подписи в электронных документах в государственных и негосударственных цифровых системах
АО «НИТ»	Акционерное общество «Национальные информационные технологии»
СОС	сертификат открытого ключа электронной цифровой подписи, выданный удостоверяющим центром государственных органов, действие которого прекращено в порядке, установленном Правилами выдачи, хранения, отзыва сертификатов открытого ключа электронной цифровой подписи, подтверждения принадлежности и действительности открытого ключа электронной цифровой подписи удостоверяющим центром государственных органов Республики Казахстан
УЦ	Удостоверяющий Центр
ЭЦП	(Электронная Цифровая Подпись) цифровая запись (набор цифровых данных), созданная с использованием закрытого ключа электронной цифровой подписи и средств электронной цифровой подписи, подтверждающая

	достоверность электронного документа, его принадлежность и неизменность содержания
ЦС	Цифровая система

1. ВВЕДЕНИЕ

Настоящая Политика применения сертификатов пользователей Удостоверяющего центра государственных органов Республики Казахстан (далее – Политика) определяет деятельность Удостоверяющего центра государственных органов Республики Казахстан (далее – УЦ ГО РК) в отношении услуг, связанных с жизненным циклом сертификата открытого ключа электронной цифровой подписи (далее – сертификат) УЦ ГО РК и пользователями УЦ ГО РК. Настоящая Политика обязательна для исполнения всеми участниками ИОК УЦ ГО РК, которые используют сертификаты УЦ ГО РК.

УЦ ГО РК создан в целях обслуживания государственных и местных исполнительных органов, должностных лиц государственных и местных исполнительных органов в цифровых системах государственных органов Республики Казахстан.

УЦ ГО РК осуществляет деятельность в соответствии со следующими законодательными, нормативными актами Республики Казахстан и стандартом:

- Цифровой Кодекс Республики Казахстан;
- Закон Республики Казахстан «О персональных данных и их защите»;
- Правила выдачи, хранения, отзыва сертификатов открытого ключа электронной цифровой подписи и подтверждения принадлежности и действительности открытого ключа электронной цифровой подписи удостоверяющим центром государственных органов Республики Казахстан;
- Правила формирования и проверки подлинности электронной цифровой подписи;
- приказ Министра по инвестициям и развитию Республики Казахстан «Об утверждении Типового положения удостоверяющего центра»;
- СТ РК 1073-2007. Средства криптографической защиты информации. Общие технические требования либо СТ РК 1073-2025 Средства криптографической защиты информации. Требования к информационной безопасности и процессам жизненного цикла

1.1 Обзор

Настоящая Политика применима ко всем участникам УЦ ГО РК.

Настоящая Политика состоит из 10 разделов. Политика является высокоуровневым документом, принадлежащим УЦ ГО РК.

1.1.1 Наименование и идентификация документа

Наименование настоящего документа	Политика применения сертификатов Удостоверяющего центра государственных органов Республики Казахстан
Версия документа	7.0
Введен в действие	11.09.2026
Ссылка на актуальную версию документа	https://ucgo.gov.kz/files/docs/ru/pprs_ru.pdf

1.2 Участники ИОК УЦ ГО РК

1.2.1 УЦ ГО РК

УЦ ГО РК является удостоверяющим центром, который выдаёт сертификаты.

УЦ ГО РК осуществляет деятельность, которая непосредственно связана с ИОК, а именно:

- получение и обработка запросов на выдачу и отзыв сертификатов;
- выдача и отзыв сертификатов пользователей УЦ ГО РК;
- публикация и поддержка СОС;
- обработка запросов на сервис OCSP;
- постановка штампа метки времени TSP.

1.2.2 Оператор УЦ ГО РК

В ИОК УЦ ГО РК функции операторов выполняют сотрудники структурного подразделения АО «НИТ».

Оператор УЦ ГО РК осуществляет:

- согласование и/или подтверждение запроса на выпуск/отзыв сертификатов (в случае «онлайн» выпуска);
- выпуск сертификатов (в случае «офлайн» выпуска);
- публикация сведений об отозванных сертификатах, их серийные номера и причину отзыва в СОС на интернет-ресурсе по адресу ucgo.gov.kz и в сети ЕТС ГО.

1.2.3 Владелец сертификата УЦ ГО РК

Владелец УЦ ГО РК – государственный служащий, на имя которого выдан сертификат открытого ключа электронной цифровой подписи, правомерно владеющее закрытым ключом, соответствующим открытому

ключу, указанному в сертификате открытого ключа электронной цифровой подписи.

1.2.4 Другие участники

1. ЦС и его пользователи, интегрируемые с ЦС УЦ ГО РК.
2. Владелец, представитель владельца сертификата на получение или отзыв сертификатов УЦ ГО РК.

1.3 Использование сертификатов пользователя УЦ ГО РК

Сертификаты пользователей УЦ ГО РК применяются для следующих целей:

- 1) подписание электронных документов средствами ЭЦП;
- 2) проверка ЭЦП.

Способы использования сертификатов пользователей УЦ ГО РК не должны противоречить действующему законодательству Республики Казахстан, а также требованиям настоящей Политики.

Владельцам сертификатов УЦ ГО РК и ЦС запрещается использование сертификатов УЦ ГО РК в случаях:

- 1) окончания срока действия сертификата УЦ ГО РК;
- 2) отзыва сертификата пользователя УЦ ГО РК;
- 3) подозрения на компрометацию закрытого ключа владельца сертификата УЦ ГО РК;
- 4) обнаруженной компрометации закрытого ключа пользователя УЦ ГО РК;
- 5) не относящихся к разрешенным способам использования сертификатов пользователей УЦ ГО РК.

1.4 Управление Политикой

1.4.1. Организация администрирующая документ

Наименование организации	Акционерное общество «Национальные информационные технологии»
Физический адрес	Республика Казахстан, 010000, г. Астана, Дом министерств, подъезд 16В
Юридический адрес	Республика Казахстан, 010000, г. Астана, ул. Мәңгілік ел 55/15
Адрес электронной почты	support@ucgo.gov.kz
Телефон канцелярии	+7 (7172) 70 49 37

1.4.2. Контактное лицо

Наименование подразделения	Управление инфраструктуры открытых ключей
Наименование должности	Начальник Управления инфраструктуры открытых ключей
Адрес электронной почты	support@ucgo.gov.kz
Контактный телефон	+7(7172) 70 16 65 вн 3108

Утверждённые изменения или дополнения в Политике публикуются на сайте УЦ ГО РК (https://ucgo.gov.kz/files/docs/ru/pprs_ru.pdf) в виде отдельного документа, содержащего полный текст Политики, или уведомление о внесении изменений и самих изменений с указанием последовательного увеличивающегося номера версии Политики.

2. ОТВЕТСТВЕННОСТЬ В ОТНОШЕНИИ ПУБЛИКАЦИИ И ХРАНЕНИЯ

УЦ ГО РК обеспечивает публичную доступность 24 часа в сутки, 7 дней в неделю следующих материалов на сайте УЦ ГО РК, за исключением объективных причин, ложных срабатываний и производственной необходимости (профилактические работы и т.д.):

1) корневой сертификат УЦ ГО РК по алгоритму ГОСТ 34.310-2004 доступен по адресу https://ucgo.gov.kz/ru/root_cert_ru-2/;

2) настоящую Политику;

3) Регламент УЦ ГО РК;

4) СОС, который доступен для загрузки с сайта <https://ucgo.gov.kz/crl/ucgo.crl>;

5) службы OCSP, доступные по адресу <http://ucgo.gov.kz:62265> и <http://ucgo.gov.kz:62266>;

6) служба TSP, доступная по адресу <http://ucgo.gov.kz:62275> и <http://ucgo.gov.kz:62276>;

7) согласие на сбор и обработку персональных данных.

СОС УЦ ГО РК предоставляется в электронной форме и формате, определённым рекомендациями RFC 5280 и настоящей Политике. УЦ ГО РК публикует СОС для сертификатов на алгоритме ГОСТ 34.310-2004, доступный по адресу <https://ucgo.gov.kz/crl/ucgo.crl>.

СОС (CRL) УЦ ГО РК – это электронный документ (файл), содержащий сведения об отозванных сертификатах и подписанный ЭЦП УЦ ГО РК.

Цифровая система для проверки сертификата на отозванность имеет возможность загрузить (скачать) СОС с сайта <https://ucgo.gov.kz/crl/ucgo>. (открытый доступ) в сети интернет и ЕТС ГО crl.ucgo.gov.kz.

УЦ ГО РК также предоставляет службу проверки статуса сертификата

пользователя УЦ ГО РК посредством службы OSCP в Единой транспортной среде государственных органов (далее – ЕТС ГО).

УЦ ГО РК предоставляет службу поставки «Штампа времени» пользователям УЦ ГО РК посредством службы TSP в ЕТС ГО.

СОС публикуется 2 раза в неделю. Срок действия СОС составляет 7 дней.

В УЦ ГО РК реализованы меры кибербезопасности и физической безопасности с целью предотвращения несанкционированного внесения, изменения или удаления информации, содержащейся в СОС ЦС УЦ ГО РК.

СОС доступен для загрузки с сайта <https://ucgo.gov.kz/crl/ucgo.crl>.

3. ПРИСВАИВАНИЕ ИМЁН

Сертификат пользователя УЦ ГО РК содержит отличительные имена в DN-имени в формате рекомендуемым стандартом X.501 «Information technology – Open Systems Interconnection – The Directory: Models» («Информационные технологии – Открытые системы коммуникации») из серии рекомендуемых стандартов ITU-T X.500 в поле «Subject» (Субъект), указанные в Приложении 1 настоящей Политики.

УЦ ГО РК выдаёт сертификаты пользователей УЦ ГО РК, которые содержат персональные данные в DN-имени, позволяющие идентифицировать пользователя УЦ ГО РК.

Анонимность пользователей и использование псевдонимов пользователей не допускается.

УЦ ГО РК заполняет поле «Subject» (Субъект) персональными данными пользователя УЦ ГО РК, полученными из государственной базы данных физических лиц и государственной базы данных юридических лиц на основании предоставленных пользователем идентифицирующих данных.

Каждому уникальному пользователю УЦ ГО РК должно соответствовать уникальное имя в поле «Subject» (Субъект) сертификата пользователя УЦ ГО РК, указанных в Приложении 1 настоящей Политики.

4. ОПЕРАЦИОННЫЕ ТРЕБОВАНИЯ К ЖИЗНЕННОМУ ЦИКЛУ СЕРТИФИКАТА ПОЛЬЗОВАТЕЛЯ УЦ ГО РК

Для получения сертификата УЦ ГО РК заявитель предоставляет в УЦ ГО РК в режиме онлайн, почтовой или специальной почтовой связью, а также нарочно письмо на получение сертификатов.

Выдача сертификата УЦ ГО РК осуществляется в течении трех рабочих дней.

Сертификат выдается в форме электронного документа, записанного на защищенный носитель ключевой информации, со структурой сертификата для пользователей УЦ ГО РК.

Выдача сертификата нарочно регистрируется в специальном журнале учета выдачи сертификатов пользователей УЦ ГО РК.

4.1 Порядок выпуска переподчиненного сертификата удостоверяющего центра государственных органов Республики Казахстан

Для генерации сертификата используется криптографический модуль (HSM), соответствующий уровню 3 стандарта СТ РК 1073-2007 «Средства криптографической защиты информации». HSM выполняет генерацию ключа, используя ключ алгоритма: СТ РК ГОСТ 34.310-2004.

Ключ УЦ ГО РК генерируются в физической защищенной среде. Криптографическое оборудование должно быть физический отдельно от остальных систем, не относящихся к УЦ ГО РК. Доступ должен контролироваться не менее чем тремя уровнями защиты.

Генерация ключа УЦ ГО РК осуществляется Администратором ЦС УЦ ГО.

При выпуске переподчиненного сертификата назначаются участники процедуры (работники ЦС УЦ ГО РК, владелец ЦС)

Администратор ЦС осуществляет следующее:

- генерация ключа и сертификата УЦ ГО РК;
- создание «секрет» ключа;

Передача «секрета» производится лично на носителе ключевой информации и подтверждается актом приема-передачи на хранение, который согласовывается со всеми участниками процедуры.

По окончании мероприятия составляется протокол процедуры, который согласовывается со всеми ее участниками.

Администратор ЦС публикует переподчиненный сертификат УЦ ГО РК на интернет-ресурсе <https://ucgo.gov.kz>, а также в БД.

4.2 Порядок выпуска сертификата служб OCSP и TSP удостоверяющего центра государственных органов Республики Казахстан

Для проверки статуса и подлинности сертификатов УЦ ГО РК необходимы сертификаты служб УЦ ГО РК (OCSP и TSP) в УЦ, которые выпускает Администратор ЦС каждые 3 года.

Администратор ЦС осуществляет следующее:

- выпуск сертификата (OCSP и TSP) УЦ ГО РК;
- публикация сертификата служб OCSP и TSP в БД ЦС УЦ ГО РК.
- формирование протокола выпуска сертификата служб OCSP и TSP.

По окончании мероприятия сертификат (OCSP и TSP) УЦ ГО РК передается заявителю на электронном носителе информации (заявитель расписывается в журнале учета выдачи сертификатов пользователей УЦ ГО РК), при необходимости производится установка сертификата (OCSP и TSP) на серверах заявителя.

4.3 Порядок выдачи сертификата открытого ключа электронной цифровой подписи

Для получения сертификата заявитель подает заявление одним из следующих способов:

- 1) в режиме онлайн – при подаче заявления заявителем (осуществляется при наличии у заявителя защищенного носителя ключевой информации);
- 2) посредством личного кабинета уполномоченного сотрудника;
- 3) в режиме офлайн – для сотрудника архива и VPN устройства.

4.4 Порядок выдачи сертификата в режиме онлайн

При подаче заявки на выдачу сертификата сотрудник государственного органа или местного государственного органа (далее – сотрудник ГО/МИО) подключает к рабочей станции защищенный носитель ключевой информации заявителя;

Сотрудник ГО/МИО подает онлайн заявку в сервисе подачи заявки online УЦ ГО РК на выдачу сертификата в УЦ ГО РК посредством ЕТС ГО.

Сотрудник ГО/МИО направляет оператору УЦ ГО РК письмо с заявлением на выдачу сертификата УЦ ГО РК посредством СЭД, почтовой связи или нарочно

Сотрудник оператора УЦ ГО РК после получения письма осуществляет проверку полноты и достоверности представленных сведений и при их соответствии подтверждает запрос на выдачу сертификата. В случае несоответствия представленных данных сотрудник оператора УЦ ГО РК отказывает в выдаче сертификата на основании подпункта 4.7 настоящей Политики.

Заявитель после подтверждения заявки сотрудником оператора, устанавливает сертификат на защищенный носитель ключевой информации заявителя.

4.5 Порядок выдачи сертификата в режиме офлайн

Порядок выдачи сертификата пользователя УЦ ГО РК

Выдача сертификатов УЦ ГО РК заявителю осуществляется по шаблонам:

- 1) сотрудник ГО/МИО;
- 2) сотрудник архива;
- 3) VPN устройство.

4.6 Порядок выдачи сертификата почтовой или специальной почтовой связью

Ответом на заявку по выпуску сертификата пользователя УЦ ГО РК заявителя является:

1) для режима онлайн и личного кабинета уполномоченного сотрудника – выпуск сертификата пользователя УЦ ГО РК;

2) для режима офлайн – передача заявителю носителя ключевой информации нарочно, почтовой или специальной почтовой связью;

Защищенный носитель ключевой информации передается заявителю почтовой или специальной почтовой связью с регистрацией в специальном журнале учета выданных сертификатов.

4.7 Порядок отказа в выдаче сертификата УЦ ГО РК

УЦ ГО РК отказывает в выдаче сертификата в следующих случаях:

1) неполноты представленных документов;

2) представления недостоверных сведений;

3) вступления в законную силу судебного акта;

4) недостижения лицом шестнадцатилетнего возраста.

При рассмотрении заявления УЦ ГО РК осуществляет проверку достоверности представленных сведений, включая сопоставление данных заявителя и данных, указываемых в сертификате. Несоответствие указанных данных рассматривается как представление недостоверных сведений, за исключением случаев, связанных с территориальной или подведомственной принадлежностью организации.

Выдача сертификата осуществляется при отсутствии у владельца сертификата действующего сертификата, за исключением случаев, предусмотренных внутренними процессами УЦ ГО РК, включая:

осуществление служебной деятельности в двух государственных органах (при наличии подтверждающих документов);

использование двух защищенных носителей ключевой информации, один из которых оснащён интерфейсом USB Type-C.

Ответ об отказе в выдаче сертификата предоставляется заявителю путем отклонения заявления в сервисе подачи онлайн-заявок с указанием причины отказа либо направлением мотивированного отказа через СЭД.

При получении нарочно носителя ключевой информации, содержащего сертификат пользователя УЦ ГО РК для сотрудника архива и VPN устройства, уполномоченный сотрудник заявителя расписывается в журнале учета выдачи сертификатов пользователей УЦ ГО РК.

5. ОТЗЫВ И ХРАНЕНИЕ СЕРТИФИКАТОВ УЦ ГО РК

УЦ ГО РК обеспечивает хранение копий выданных сертификатов в электронной форме.

Срок хранения отозванных сертификатов в регистре сертификатов

составляет пять лет.

По истечении срока, отозванные сертификаты поступают на архивное хранение в порядке, установленном действующим законодательством Республики Казахстан.

Оператор УЦ ГО РК отзывает сертификат по требованию владельца сертификата, при установлении факта представления недостоверных сведений либо неполного пакета документов при получении сертификата, в случае смерти владельца сертификата, изменения фамилии, имени или отчества (если оно указано в документе, удостоверяющем личность) владельца сертификата, смены руководителя, смены наименования, реорганизации или ликвидации юридического лица – владельца сертификата, а также на основании вступившего в законную силу решения суда на основании письма на отзыв сертификата.

УЦ ГО РК после получения письма на отзыв сертификата осуществляет его рассмотрение и обработку. В случае успешного рассмотрения заявления, ЦС УЦ ГО РК осуществляет отзыв сертификата, публикует информацию об отозванном сертификате в СОС. В случае несоответствия представленных сведений сотрудник оператора УЦ ГО РК отказывает в отзыве сертификата по основаниям, предусмотренным подпунктом 5.1 настоящей Политики.

5.1 Порядок отказа в отзыве сертификата УЦ ГО РК

УЦ ГО РК отказывает в отзыве сертификата в случае представления неполного пакета документов, представления недостоверных сведений, в том числе если заявитель не является владельцем сертификата, за исключением случаев, связанных с территориальной или подведомственной принадлежностью организации, а также при отсутствии действующего сертификата у владельца сертификата УЦ ГО РК. Уведомление об отказе в отзыве сертификата направляется заявителю путем отклонения заявления в сервис подачи онлайн-заявок с указанием причины отказа либо посредством направления мотивированного отказа через СЭД.

6. ИСПОЛЬЗОВАНИЕ КЛЮЧЕВОЙ ПАРЫ УЦ ГО РК

Пользователь УЦ ГО РК использует закрытый ключ после ознакомления и принятия им в полном объеме требований, указанных в:

- 1) действующем законодательстве Республики Казахстан;
- 2) согласии на сбор и обработку персональных данных;
- 3) настоящей Политике.

Пользователь УЦ ГО РК использует сертификаты пользователя УЦ ГО РК в соответствии с политикой применения, указанной в полях «keyUsage» (использование) согласно Приложению 1 настоящей Политики.

Использование пользователями сертификатов УЦ ГО РК означает принятие положений настоящей Политики и согласие на публикацию данных,

не рассматриваемых в качестве конфиденциальных.

Пользователь УЦ ГО РК обязан принимать меры для защиты принадлежащего ему закрытого ключа ЭЦП от неправомерного доступа и использования, а также хранить закрытые ключи в порядке, установленном действующим законодательством Республики Казахстан.

6.1 Использование открытых ключей и сертификатов пользователя УЦ ГО РК

Участники ИОК УЦ ГО РК, принимают обязательства, регламентированные в:

- 1) действующем законодательстве Республики Казахстан;
- 2) настоящей Политике.

6.2 Обновление сертификата пользователя УЦ ГО РК

УЦ ГО РК не осуществляет обновление данных, увеличение срока действия, внесение изменений и дополнений в структуру сертификатов пользователя УЦ ГО РК.

В случае изменения персональных данных пользователя УЦ ГО РК ранее выданный сертификат подлежит отзыву, после чего осуществляется выдача нового сертификата УЦ ГО РК.

7. КЛЮЧЕВАЯ ПАРА УЦ ГО РК

Ключевые пары пользователей УЦ ГО РК выпускаются в соответствии с алгоритмом СТ РК ГОСТ 34.310-2004 и имеющие длину:

- 1) закрытый ключ — 256 бит;
- 2) открытый ключ — 512 бит.

УЦ ГО РК допускает использование только криптографического аппаратного обеспечения, сертифицированного на соответствие действующим в Республике Казахстан стандартам, определяющим общие технические требования к средствам криптографической защиты информации на соответствие не ниже, чем третьему уровню безопасности по стандарту Республики Казахстан СТ РК 1073-2007.

Криптографическое аппаратное обеспечение УЦ ГО РК должно храниться и эксплуатироваться исключительно в предназначенных для этого защищённых объектах УЦ ГО РК.

Мероприятия по приёму, обслуживанию и выводу из эксплуатации криптографического аппаратного обеспечения УЦ ГО РК должны осуществляться в присутствии ответственных работников.

Криптографические модули, хранящие закрытые ключи УЦ ГО РК аппаратно, не допускают хранения ключевого материала в незашифрованном виде.

Все части закрытых ключей УЦ ГО РК, выведенные из эксплуатации, уничтожаются с гарантированной невозможностью восстановления. Процедура уничтожения закрытого ключа УЦ ГО РК осуществляется уполномоченными работниками в присутствии независимого наблюдателя.

8. ПРАВОВЫЕ И БИЗНЕС-ВОПРОСЫ

8.1 Иная финансовая ответственность

УЦ ГО РК в процессе своей деятельности обрабатывает, получает, использует и хранит конфиденциальную информацию, при этом УЦ ГО РК принимает все необходимые меры по ее защите в соответствии с действующим законодательством Республики Казахстан.

УЦ ГО РК несёт ответственность по защите обрабатываемой, получаемой, используемой и хранящейся конфиденциальной информации в соответствии с действующим законодательством Республики Казахстан.

8.2 Обеспечение конфиденциальности УЦ ГО РК персональных данных пользователей УЦ ГО РК

УЦ ГО РК обеспечивает защиту персональных данных пользователей УЦ ГО РК в соответствии с действующим законодательством Республики Казахстан.

В случае прекращения деятельности УЦ ГО РК обязан за тридцать дней до прекращения своей деятельности проинформировать об этом всех участников ИОК УЦ ГО РК и уполномоченный орган.

При прекращении деятельности УЦ ГО РК, выданные им сертификаты и соответствующие ключи электронной цифровой подписи, сведения о сертификатах пользователей УЦ ГО РК передаются в другие удостоверяющие центры по согласованию с пользователями УЦ ГО РК сертификата.

По истечении срока сертификаты пользователей УЦ ГО РК и соответствующие ключи ЭЦП, не переданные в другие удостоверяющие центры, прекращают свое действие и подлежат хранению в соответствии с законодательством Республики Казахстан.

9. ГАРАНТИИ СТОРОН

УЦ ГО РК гарантирует обеспечение сертификатами 100% пользователей, обратившихся в УЦ ГО РК, за исключением случаев указанных в подпунктах

4.6 и 5.1 настоящей Политики.

Владелец сертификата гарантирует использование сертификата УЦ ГО РК в соответствии с действующим законодательством Республики Казахстан и настоящей Политикой.

10. СРОК ДЕЙСТВИЯ И ПОРЯДОК ПРЕКРАЩЕНИЯ ДЕЙСТВИЯ ПОЛИТИКИ

Настоящая Политика вступает в силу с момента подписания и опубликования их на информационном сайте УЦ ГО РК (ucgo.gov.kz).

Настоящая Политика остается в силе до замены новой версией в течение функционирования УЦ ГО РК.

С момента прекращения действия настоящей Политики участники ИОК УЦ ГО РК остаются связанными условиями последней версии Политики по всем сертификатам до момента истечения периода действия каждого из сертификатов.

Приложение 1

к Политике применения
сертификатов удостоверяющего
центра государственных органов
Республики Казахстан

1. Структура сертификата Удостоверяющего центра государственных органов Республики Казахстан (на алгоритме ГОСТ 34.310-2004)

Поле	Описание	OID, критичность	Содержание
Базовые поля сертификата в формате X.509 V3			
Version	Версия Стандарта X.509	—	V3
Serial Number	Серийный номер сертификата	—	Положительное, целое число (не более 20 байт)
Signature Algorithm	Алгоритм подписи	1.2.398.3.10.1.1.1.2	T ГОСТ 34.310-2004
Issuer	Данные Издателя сертификата	CN=2.5.4.3 C=2.5.4.6	CN = НЕГІЗГІ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (GOST) (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 сертификата	C=2.5.4.6 CN = 2.5.4.3 O=2.5.4.10	CN = Удостоверяющий центр Государственных органов (обязательное поле) O = Республика Казахстан (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	Значение
Дополнительные поля сертификата 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	Подписывание сертификатов, Автономное подписание списка отзыва (CRL), Подписывание списка отзыва (CRL) (06)
Certificate Policy	Политика сертификата	2.5.29.32	[1] Политика сертификата: Идентификатор политики=1.2.398.3.2.1 [1,1] Сведения квалификатора политики: Идентификатор квалификатора политики = CPS Квалификатор: http://ucgo.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://crl1.root.gov.kz/gost.crl URL= http://crl.root.gov.kz/gost.crl Причина списка отзыва (CRL)=Сертификат заменен, Прекращение действия, Приостановка действия (0f)

Digital Signature	Цифровая подпись центра сертификации (512 бит)	1.2.398.3.10.1.1.1.2	Значение
-------------------	--	----------------------	----------

2. Структура сертификата для пользователей Удостоверяющего центра государственных органов (для подписи и цифровой аутентификации на алгоритме ГОСТ 34.310-2004)

Поле	Описание	OID, критичность	Содержание
Version	Версия		V3
Serial Number	Серийный номер		Значение целого числа в шестнадцатеричном представлении
Signature Algorithm	Алгоритм подписи	1.2.398.3.10.1.1.1.2	ГОСТ 34.310-2004 критично
Issuer	Издатель (Уникальное имя)	C=2.3.4.6 O=2.5.4.10 CN=2.5.4.3	CN = Удостоверяющий центр Государственных органов O = Республика Казахстан C = KZ
Valid From	Действителен с	UTC TIME	День/месяц/год часы/минуты/секунды
Valid To	Действителен до	UTC TIME	День/месяц/год часы/минуты/секунды
Subject	Субъект (Уникальное имя)	C=2.3.4.6 CN=2.5.4.3 G=2.5.4.42 SN=2.5.4.5 Phone=2.5.4.20 OU=2.5.4.11 E=1.2.840.113549.1.9.1 S=2.5.4.8 SURNAME=2.5.4.4	CN = ФАМИЛИЯ ИМЯ G = ОТЧЕСТВО (необязательное поле) SERIALNUMBER= PINXXXXXXXXXXXXX SURNAME = Фамилия (необязательное поле) Phone = +7XXXXXXXXXXXX (необязательное поле) E = ЭЛЕКТРОННАЯ ПОЧТА (необязательное поле) OU = BINXXXXXXXXXXXXX O= Организация S = ОБЛАСТЬ C = KZ
Public Key	Открытый ключ	1.2.398.3.10.1.1.1.1 с параметрами 1.2.398.3.10.1.1.1.1. 1	Значение

		1.2.398.3.10.1.1.1.1.2	
Key Usage	Использование ключей	2.5.29.15, critical	Цифровая подпись, Неотрекаемость, Шифрование ключей
Certificate Policy	Политика сертификата	2.5.29.32	[1] Политика сертификата: Идентификатор политики=1.2.398.3.2.1 [1,1] Сведения квалификатора политики: Идентификатор квалификатора политики=CPS Квалификатор: URL=http://ucgo.gov.kz/cps
Certificate Authority Information Access	Доступ к сведениям центра 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://ucgo.gov.kz/cert/*.cer [2] Доступ к сведениям центра сертификации Метод доступа = Протокол определения состояния сертификата через сеть (1.3.6.1.5.5.7.48.1) Дополнительное имя: URL=http://ocsp.ucgo.gov.kz
CRL Distribution Point	Точка распространения списков отзыва	2.5.29.31	[1] Точка распределения списка отзыва (CRL) Имя точки распространения: Полное имя: URL=http://crl.ucgo.gov.kz/crl/*.crl
Subject Key Identifier	Идентификатор ключа субъекта	2.5.29.14	Серийный номер сертификата
Authority Key Identifier	Идентификатор ключа центра сертификаций	2.5.29.35	Значение идентификатора ключа центра сертификации в шестнадцатеричном формате

1.2.398.3.10.1. 2	Бинарные данные	Данные в шестнадцатеричном представлении (опционально)
----------------------	--------------------	---

3. Структура сертификата для VPN устройств, полученных в Удостоверяющем центре государственных органов Республики Казахстан на алгоритме ГОСТ 34.310-2004

п	Ти	Описание	Значение	Обязательность/Критичность
Version	Версия		V3	Да/Не критично
Serial Number	Серийный номер		Значение целого числа в шестнадцатеричном представлении	Да/Не критично
Signature Algorithm	Алгоритм подписи		ГОСТ 34.310-2004	Да/Не критично
Issuer	Издатель (Уникальное имя)		CN = Удостоверяющий центр Государственных органов O = Республика Казахстан C = KZ	Да/Не критично
Valid From	Действителен с		День/месяц/год часы/минуты/секунды	Да/Не критично
Valid To	Действителен до		День/месяц/год часы/минуты/секунды	Да/Не критично
Subject	Субъект (Уникальное имя)		CN = НАИМЕНОВАНИЕ ОБЛАСТИ OU = VPN_XXXXXXXXXXXXX S = ОБЛАСТЬ C = KZ	Да/Не критично
Public Key	Открытый ключ		1.2.398.3.10.1.1.1.1 с параметрами 1.2.398.3.10.1.1.1.1.1 1.2.398.3.10.1.1.1.1.2	Да/Не критично
Key Usage	Использование ключей		Цифровая подпись, Неотрекаемость, Согласование ключа (опционально)	Да/Не критично
CRL Distribution Point	Точка распространения списков отзыва		[1] Точка распределения списка отзыва (CRL) Имя точки распространения: Полное имя:	Да/Не критично

		URL=http://crl.ucgo.gov.kz/crl/*.crl	
Authority Information Access	Доступ к сведениям центра сертификации	[1] Доступ к сведениям центра сертификации Метод доступа = Поставщик центра сертификации (1.3.6.1.5.5.7.48.2) Дополнительное имя: URL=http://ucgo.gov.kz/cert/*.cer [2] Доступ к сведениям центра сертификации Метод доступа = Протокол определения состояния сертификата через сеть (1.3.6.1.5.5.7.48.1) Дополнительное имя: URL=http://ocsp.ucgo.gov.kz	Да/Не критично
Certificate Policy	Политика сертификата	[1] Политика сертификата: Идентификатор политики=1.2.398.3.2.1 [1,1] Сведения квалifikатора политики: Идентификатор квалifikатора политики=CPS Квалifikатор: URL=http://ucgo.gov.kz/cps	Да/Не критично
Subject Key Identifier	Идентификатор ключа субъекта	Серийный номер сертификата	Да/Не критично
Certificate Authority Key Identifier	Идентификатор ключа центра сертификации	Идентификатор ключа = серийный номер	Да/Не критично

4. Структура сертификата для сотрудников архива Удостоверяющего центра государственных органов (для подписи и цифровой аутентификации на алгоритме ГОСТ 34.310-2004)

Поле	Описание	OID, критичность	Содержание
------	----------	------------------	------------

Version	Версия		V3
Serial Number	Серийный номер		Значение целого числа в шестнадцатеричном представлении
Signature Algorithm	Алгоритм подписи	1.2.398.3.10.1.1.1.2	ГОСТ 34.310-2004
Issuer	Издатель (Уникальное имя)	C=2.3.4.6 O=2.5.4.10 CN=2.5.4.3	CN = Удостоверяющий центр Государственных органов O = Республика Казахстан C = KZ
Valid From	Действителен с	UTC TIME	День/месяц/год часы/минуты/секунды
Valid To	Действителен до	UTC TIME	День/месяц/год часы/минуты/секунды
Subject	Субъект (Уникальное имя)	C=2.3.4.6 CN=2.5.4.3 G=2.5.4.42 SN=2.5.4.5 Phone=2.5.4.2.0 OU=2.5.4.11 E=1.2.840.1.13.549.1.9.1 S=2.5.4.8 SURNAME=2.5.4.4 T=archiver	CN = ФАМИЛИЯ ИМЯ G = ОТЧЕСТВО (необязательное поле) SERIALNUMBER=IINXXXXXXXXXXXXX SN = Фамилия (необязательное поле) Phone = +7XXXXXXXXXXXXX (необязательное поле) E = ЭЛЕКТРОННАЯ ПОЧТА OU = BINXXXXXXXXXXXXX O=Организация S = ОБЛАСТЬ C = KZ T = Должность
Public Key	Открытый ключ	1.2.398.3.10.1.1.1.1 с параметрами 1.2.398.3.10.1.1.1.1.1 1.2.398.3.10.1.1.1.1.2	Значение
Дополнительные поля сертификата в формате X.509			
Extended Key Usage	Расширенное использование ключа	2.5.29.37	1.2.398.3.2.3.1 - Сотрудник Архива Президента Республики Казахстан 1.2.398.3.2.3.2 - Сотрудник Центрального государственного архива

			1.2.398.3.2.3.3 - Сотрудник Ведомственного архива 1.2.398.3.2.3.4 - Государственные служащие
Key Usage	Использование ключей	2.5.29.15, critical	Цифровая подпись, Неотрекаемость, Шифрование ключей
Certificate Policy	Политика сертификата	2.5.29.32	[1] Политика сертификата: Идентификатор политики=1.2.398.3.2.1 [1,1] Сведения квалификатора политики: Идентификатор квалификатора политики=CPS Квалификатор: URL=http://ucgo.gov.kz/cps
Certificate Authority Information Access	Доступ к сведениям центра 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://ucgo.gov.kz/cert/*.cer [2] Доступ к сведениям центра сертификации Метод доступа = Протокол определения состояния сертификата через сеть (1.3.6.1.5.5.7.48.1) Дополнительное имя: URL=http://ocsp.ucgo.gov.kz
CRL Distribution Point	Точка распространен ия списков отзыва	2.5.29.31	[1] Точка распределения списка отзыва (CRL) Имя точки распространения: Полное имя: URL=http://crl.ucgo.gov.kz/crl/*.crl
Subject Key Identifier	Идентификато р ключа субъекта	2.5.29.14	Серийный номер сертификата
Authority Key Identifier	Идентификато р ключа центра сертификаций	2.5.29.35	Значение идентификатора ключа центра сертификации в шестнадцатеричном формате
1.2.398.3.10.1 .2	Бинарные данные		Данные в шестнадцатеричном представлении (опционально)

**Лист согласования Политики применения сертификатов
удостоверяющего центра государственных органов Республики
Казахстан
(Certificate POLICY 7.0)**

№	ФИО	Должность	Подпись	Дата
1	Мусафиев А.И.	Project Manager		
2	Жандыбаев А.Е.	нат. упр		
3	Хайруллин А.М.	гир. деп. UOK		
4				
5				