**Утверждаю**
**Генеральный директор**
**ТОО «Вериграм»**
**Байгожин А.К.**

**«01» декабря 2024г.**


# ПОЛИТИКА

ПРИМЕНЕНИЯ СЕРТИФИКАТОВ

Настоящая Политика применения сертификатов удостоверяющего центра ТОО "Вериграм" (далее – Политика) разработана в соответствии с законодательством Республики Казахстан и определяет регламент и механизмы работы удостоверяющего центра ТОО "Вериграм", в части управления процессом выдачи сертификатов, общие правила применения, процедуры проверки, способы использования сертификатов.

**Статья 1. Общие положения**

1. Настоящая Политика определяет порядок изготовления и применения сертификатов при подписании электронных документов.

2. Действие настоящей Политики распространяется на всех работников Компании, применяющих ее в работе.

3. В настоящей Политике используются следующие понятия, условные обозначения и сокращения:

1) **владелец сертификата** – физическое лицо/юридическое лицо, на имя которого выдано сертификат, правомерно владеющее закрытым ключом, соответствующим открытому ключу, указанному в сертификате;

2) **закрытый ключ ЭЦП** – последовательность электронных цифровых символов, предназначенная для создания электронной цифровой подписи с использованием средств электронной цифровой подписи;

3) **заявитель** – физическое лицо/юридическое лицо, подавшее документы на выдачу или отзыв сертификата;

4) **заявление** – документ на выдачу или отзыв сертификата, по форме, установленной законодательством Республики Казахстан;

5) **корневой УЦ РК** - удостоверяющий центр, осуществляющий подтверждение принадлежности и действительности открытых ключей электронной цифровой подписи удостоверяющих центров;

6) **открытый ключ ЭЦП** – последовательность электронных цифровых символов, доступная любому лицу и предназначенная для подтверждения подлинности электронной цифровой подписи в электронном документе;

7) **Сертификат** – регистрационное свидетельство, электронный документ, выдаваемый удостоверяющим центром для подтверждения соответствия электронной цифровой подписи требованиям, установленным законодательством Республики Казахстан

8) **СОС** – список отозванных сертификатов, часть регистра сертификатов, содержащий сведения о сертификатах, действие которых прекращено, их серийные номера, дату и причину отзыва;

9) **удостоверяющий центр (УЦ)** – ТОО "Вериграм", удостоверяющее соответствие открытого ключа электронной цифровой подписи закрытому ключу электронной цифровой подписи, а также подтверждающее достоверность сертификатов;

9-1) **участник УЦ** – владельцы сертификатов, ТОО "Вериграм", иные третьи лица, участвующие в процессах сбора, обработки, хранения, передачи, поиска и распространения электронных документов;

10) **хранилище сертификатов** – регистр всех сертификатов, в том числе, СОС, доступный участникам удостоверяющего центра, в порядке, установленном внутренними документами удостоверяющего центра;

11) **электронная цифровая подпись (далее – ЭЦП)** – набор электронных цифровых символов, созданный средствами электронной цифровой подписи и подтверждающий достоверность электронного документа, его принадлежность и неизменность содержания.

*Иные специфические термины и сокращения, используемые по тексту Политики, применяются в соответствии со значением, закрепленном в законодательстве Республики Казахстан, во внутренних документах удостоверяющего центра или принятым в международной практике.*

**Статья 2. Цель и задачи.**

1. Целью настоящей Политики является поддержание общих правил применения, процедур проверки, способов использования сертификатов в соответствии с требованиями законодательства Республики Казахстан.

2. Задачами Политики является осуществление контроля:

1) за соблюдением требований законодательства и внутренних документов Компании при осуществлении деятельности УЦ;

2) за надлежащим применением ЭЦП при подписании электронных документов владельцами сертификатов.

**Статья 3. Принципы применения сертификатов**

1. Применение сертификатов УЦ должно осуществляться в соответствии со следующими принципами:

1) принцип законности. Соблюдение законодательства Республики Казахстан при применении сертификатов;

2) принцип целостности информации. Организация безопасного хранения и использования ЭЦП в соответствии с требованиями настоящей Политики.

**Статья 4. Использование Сертификатов**

1. Сертификаты используются Владельцами сертификатов при подписании электронных документов, а также для аутентификации Владельцев сертификатов, в соответствии со сведениями, указанными в этих Сертификатах.

2. Сферой применения ЭЦП Владельца сертификата является подписание электронных документов электронной цифровой подписью.

3. Сертификат связывает значение Открытого ключа ЭЦП с информацией, которая идентифицирует пользователя, использующего соответствующий Закрытый ключ ЭЦП. Сертификат применяется Владельцем сертификата, которому необходимо задействовать Открытый ключ ЭЦП из Сертификата для проверки ЭЦП. Степень доверия к сертификату определяется требованиями:

1) Регламентом деятельности Удостоверяющего центра;

2) Политикой;

3) Законодательством Республики Казахстан.

**Статья 5. Содержание Сертификата**

1. Сертификат содержит следующие сведения:

1) номер сертификата и срок его действия;

2) данные, позволяющие идентифицировать владельца ЭЦП;

3) открытый ключ ЭЦП;

4) информацию о сферах применения и ограничениях применения ЭЦП;

5) реквизиты УЦ.

2. Удостоверяющий центр по согласованию с участником УЦ может включать в Сертификат дополнительную информацию, необходимую для электронного документооборота.

3. УЦ выдает Сертификаты, соответствующие рекомендациям ITU-T X.509 версии 3 и RFC 5280 (Certificate and Certificate Revocation List (CRL) Profile). Выданные Сертификаты содержат в полях "Субъект" и "Поставщик" сведения, представленные в соответствии с рекомендациями ITU-T X.501 (Distinguished Names (далее - DN).

4. Указанные в Сертификате личные данные Владельца сертификата, должны точно совпадать со сведениями, указанными в документах, удостоверяющих его личность.

5. Для всех типов Сертификатов, атрибут C (Country) содержит двухбуквенный код страны (ISO 3166-1 alpha-2).

5-1. Для Сертификатов юридических лиц атрибут O (Organization) содержит название юридического лица.

6. Для Сертификатов физических лиц, атрибут CN (Common Name) содержит фамилию и имя физического лица – Владельца сертификата (строго в указанном порядке). Для Сертификатов юридических лиц, атрибут CN (Common Name) содержит фамилию и имя физического лица работника юридического лица – Владельца сертификата (строго в указанном порядке). Чтобы исключить неоднозначность между различными физическими лицами с одним и тем же именем, атрибут CN Сертификата может содержать другой дополнительный текст, кроме идентификационного имени физического лица. Дополнительный текст должен быть отформатирован так, чтобы его нельзя было перепутать с именем физического лица. Рекомендуется, чтобы текст следовал за именем физического лица после пробела в качестве разделителя и был заключен в круглые скобки. УЦ не проверяет содержимое

атрибута CN, и поэтому третьим лицам, использующим сведения о Сертификате, полученные в УЦ, для проверки принадлежности ЭЦП Владельцу Сертификата запрещается полагаться на содержание текста. Для Сертификатов сервера атрибут CN содержит ROOTCA. Для Сертификатов служб атрибут CN содержит название службы.

7. Атрибут Serial Number (SN) может быть использован для идентификации организации и физических лиц. Содержит идентификатор в соответствии с рекомендациями CWA 16036 (CyberIdentity - Unique Identification Systems For Organizations and Parts Thereof).

8. Атрибут UID (Unique ID) может использоваться для различия имен (фамилии и имени физического лица), которые в ином случае были бы одинаковыми. Содержит идентификатор, присвоенный физическому лицу уполномоченными государственными органами.

9. Дополнительно, могут использоваться атрибуты OU (Organization Unit), L (Locality) и E (email).

10. DN должно быть уникальным для каждого Заявителя. Если DN, представленное Заявителем не уникально, то УЦ требует Заявителя повторно представить запрос с изменением атрибута CN, для обеспечения уникальности DN. Согласно настоящему документу два DN считаются идентичными, если они отличаются только регистром, количеством символов подчеркивания или пробелов между словами. Таким образом, регистр, символы подчеркивания или пробела не должны использоваться для различия DN. Сертификат должно относиться к уникальному физическому лицу/юридическому лицу. Сертификат должно использоваться только Владельцем сертификата. УЦ гарантирует, что DN не будет использоваться повторно другим Заявителем. Если Заявитель запрашивает Сертификат с таким же DN, как в уже существующем Сертификате (независимо от статуса этого Сертификата), и запрос не является запросом на изменение Сертификата, то уполномоченный работник УЦ может обратиться к персональной удостоверяющей информации, чтобы проверить, что Заявитель является тем же субъектом, который был идентифицирован при получении первоначального Сертификата. Если идентичность не может быть установлена, DN не будет использоваться повторно. В случаях полного совпадения сведений, указываемых в нескольких Сертификатовах, принадлежащих разным Владельцам сертификатов, в них вносится специальный атрибут (например, SN), позволяющий однозначно идентифицировать их владельцев.

11. Выданные Сертификаты и СОС вносятся в Хранилище сертификатов. УЦ обеспечивает публикацию СОС на verigram.kz, с указанием серийного номера, даты и причины отзыва сертификата в СОС.

12. Сведения о статусе Сертификатов публикуются в соответствии с Регламентом деятельности Удостоверяющего центра.

12-1. Срок хранения отозванных сертификатов в УЦ составляет не менее пяти лет.

**Статья 6. Изготовление Сертификатов и установка ключевой пары**

1. УЦ изготавливает Сертификаты в соответствии со сведениями, указанными в Заявлении.

2. Открытый и Закрытый ключи ЭЦП формируются с применением сертифицированного СКЗИ, в соответствии с алгоритмом ГОСТ 34.310-2004.

3. Параметры генерации и проверки качества Закрытого ключа ЭЦП определяются сертифицированным СКЗИ в соответствии с СТ РК 1073–2007 автоматически.

**Статья 7. Расширения Сертификатов**

1. Сертификаты могут содержать следующие дополнения:

| | |
|---|---|
| authorityKeyIdentifier | Идентификатор ключа уполномоченного лица УЦ |
| subjectKeyIdentifier | Идентификатор ключа Владельца сертификата |
| ExtendedKeyUsage | Область (области) использования ключа, при которых электронный документ с ЭЦП будет иметь юридическое значение. Возможные значения: Server Authentication,<br>Client Authentication,<br>Secure e-mail,<br>Time stamping,<br>IPSec (Tunnel, User). |

| | |
|---|---|
| KeyUsage | Цифровая подпись,<br>Неотрекаемость,<br>Шифрование ключей,<br>Шифрование данных. |
| Basic constraints (optional) | Тип субъекта |
| cRLDistributionPoint | Точка распространения списка аннулированных (отозванных) Сертификатов |
| certificatePolicies | Политика Сертификатов: |
| Authority Information Access (optional) | Способ получения информации о статусе Сертификатов |

**Статья 8. Объектные идентификаторы алгоритмов**

1. УЦ использует следующие идентификаторы алгоритмов средства ЭЦП:

| | |
|---|---|
| ГОСТ 34.10-2004 | iso(1) org(3) dod(6) internet(1) private(4) enterprise(1) gt(6801) crypt(1) gost(2) sign(2) |
| ГОСТ 28147-89 | iso(1) org(3) dod(6) internet(1) private(4) enterprise(1) gt(6801) crypt(1) gost(2) enc(4) |
| sha256WithRSAEncryption | {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)} |

**Статья 9. Структура Сертификата корневого УЦ РК (Алгоритм ГОСТ 34.310-2004)**

| **Название** | **Содержание** |
|---|---|
| Версия | V3 |
| Серийный номер | Уникальный серийный номер Сертификата |
| Алгоритм подписи | Алгоритм подписи ГОСТ 34.310-2004 |
| Поставщик | CN = Verigram<br>O = Verigram Limited Liability Partnership<br>C = KZ |
| Субъект | CN = Verigram<br>O = Verigram Limited Liability Partnership<br>C = KZ |
| Срок действия | действителен с: YYMMDDHHMMSSZ UTC действителен по: YYMMDDHHMMSSZ UTC |
| Открытый ключ | Значение открытого ключа в бинарном виде |
| Расширения сертификатов | Дополнения сертификатов (см. пункт 7) |

**Статья 10. Структура Сертификата Участника УЦ (Алгоритм ГОСТ 34.310-2015)**

| **Название** | **Содержание** |
|---|---|
| Версия | V3 |
| Серийный номер | Уникальный серийный номер Сертификата |
| Алгоритм подписи | Алгоритм подписи ГОСТ 34.310-2004 |
| Поставщик | CN = Verigram<br>O = Verigram Limited Liability Partnership<br>C = KZ |

| | |
|---|---|
| Субъект | Физические лица:<br>SERIALNUMBER = ИИН<br>CN = ФИО<br>C = KZ<br>Phone = номер телефона<br><br>Юридические лица:<br>SERIALNUMBER = ИИН<br>CN = ФАМИЛИЯ ИМЯ<br>OU = БИН<br>O = НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ<br>C = KZ<br>Phone = номер телефона<br>Title = Должность (Первый руководитель/Сотрудник с правом подписи/ Сотрудник организации)<br>DN = Департамент |
| Срок действия | действителен с: YYMMDDHHMMSSZ UTC действителен по: YYMMDDHHMMSSZ UTC |
| Открытый ключ | Значение открытого ключа в бинарном виде |
| Алгоритм открытого ключа | Объектный идентификатор алгоритма |
| Расширения сертификатов | Дополнения сертификатов (см. пункт 7) |
| Подпись | ЭЦП |

**Статья 11. Описание СОС**

1. УЦ формирует СОС в электронной форме в формате, основанном на рекомендациях ITU-T X.509v3 и RFC 5280 (Certificate and Certificate Revocation List (CRL) Profile).

**Расширения СОС**

1. УЦ может использовать следующие дополнения:

| | |
|---|---|
| CRL number | Порядковый номер СОС |
| Authority Key Identifier | Идентификатор ключа уполномоченного лица УЦ |
| Reason Code | Код причины отзыва сертификата.<br>Возможные значения (включая, но не ограничивая):<br>Компрометация ключа пользователя;<br>Компрометация ключа УЦ;<br>Прекращение действия Сертификата. |

**Структура СОС (Алгоритм ГОСТ 34.310-2004)**

| Название | Содержание |
|---|---|
| Версия | V2 |
| Поставщик | CN = Verigram<br>O = Verigram Limited Liability Partnership<br>C = KZ |
| Дата выпуска | действителен с: YYMMDDHHMMSSZ UTC |
| Дата обновления | действителен по: YYMMDDHHMMSSZ UTC |
| Отозванные Сертификаты | Последовательность следующего вида:<br>CertificateSerialNumber (серийный номер Сертификата)<br>Time (дата и время обработки заявления на отзыв ) |
| Алгоритм подписи | Алгоритм подписи ГОСТ 34.310-2004 |
| Подпись | Цифровая подпись. |

**Статья 12. Заключительные положения**

1. Структура настоящей Политики разработана в соответствии с внутренним документом Компании, регламентирующим порядок разработки, оформления и утверждения внутренних документов Компании.

2. Политика вступает в силу с момента ее публикации на сайте www.verigram.kz и действует до публикации в новой редакции.

3. УЦ имеет право в одностороннем внесудебном порядке вносить изменения/дополнения в Политику, путем размещения изменений/дополнений (в том числе новой редакции) на сайте www.verigram.kz.

4. Официальным уведомлением Участников УЦ об утверждении изменений/дополнений в Политику является ее публикация на сайте www.verigram.kz.

5. Все изменения, вносимые в Политику, вступают в силу и становятся обязательными к исполнению всеми участниками УЦ немедленно после их опубликования.

6. За несоблюдение требований Политики Участники УЦ несут ответственность в соответствии с законодательством Республики Казахстан и внутренними документами УЦ.

7. Вопросы, порядок урегулирования которых не определен Политикой, подлежат разрешению в соответствии с требованиями законодательства Республики Казахстан и внутренних документов УЦ.