



ТОО «Интернет-компания PS»

Условия использования услуги

# **Выпуск, продление и перевыпуск SSL-сертификата**

Версия от 22.11.2024

[www.ps.kz](http://www.ps.kz)

Целью данного документа является описание параметров предоставления услуги ТОО «Интернет-компания PS» «Выпуск, продление и перевыпуск SSL-сертификата» (далее — Услуга) для обеспечения согласованного уровня качества оказания Услуги.

Настоящий документ Соглашение об уровне обслуживания или SLA («Соглашение»):

- описывает Услугу;
- устанавливает порядок предоставления Заказчику Услуги;
- являются неотъемлемой частью Публичного договора, опубликованного по адресу: <https://www.ps.kz/agreements/offer> («Оферта»).

Предоставляемая Услуга в соответствии с НК РК 03–2019 «Общий классификатор видов экономической деятельности», введенном в действие Министерством индустрии и инфраструктурного развития Республики Казахстан с 1 января 2020 года, включена в подкласс 63.11.1.

Термины, которые используются, но не определены в Соглашении, имеют значение, присвоенное им в Оферте и в разделе «Помощь» на Сайте Исполнителя: <https://www.ps.kz/faq>. Соглашение содержит пункты с активными гиперссылками на веб-страницы с более подробной информацией, которые являются неотъемлемой частью Соглашения.

Исполнитель вправе без какого-либо специального уведомления вносить изменения в Соглашение, в связи с чем Заказчик обязуется регулярно отслеживать эти изменения. Действующая редакция Условий размещена по адресу: <https://www.ps.kz/agreements/ssl-sla.pdf>. Использование Заказчиком Услуги после изменения Соглашения является подтверждением его согласия с новой редакцией.

## 1. Общие положения

1.1. Услуга предусматривает сопровождение процесса выпуска, продления или перевыпуска SSL-сертификата для надежной и безопасной передачи данных между сайтом и браузером.

1.2. Термины и определения

- **SSL-сертификат** (далее — сертификат) — цифровой документ, оформленный в соответствии с международным стандартом RFC-2986 и подтверждающий соответствие между опубликованным в нем открытым ключом владельца SSL-сертификата и субъектом сертификата (юридическим лицом или сервером, имя которого указано в поле Subject сертификата);
- **CSR (Certificate Signing Request)** — открытый ключ, генерируемый при запросе на выдачу SSL-сертификата, содержащий информацию о домене и организации, являющийся неотъемлемой частью Услуги и необходимый для установки сертификата;
- **Private Key** — закрытый ключ, генерируемый при запросе на выдачу SSL-сертификата, являющийся неотъемлемой частью услуги и необходимый для установки сертификата;
- **Сертификационный центр** — юридическое лицо, осуществляющее выпуск, продление, перевыпуск, отзыв SSL-сертификатов;
- **SAN (Subject Alternative Name)** — дополнительное поле в SSL-сертификате, которое позволяет указать несколько доменных имен, субдоменов или IP-адресов, защищаемых одним сертификатом.

1.3. Исполнитель является официальным дистрибьютором по оказанию Услуги на основании соглашений с Сертификационными центрами.

1.4. Исполнитель не гарантирует выпуск, продление, перевыпуск SSL-сертификата, так как выпуск SSL-сертификатов осуществляет Сертификационный центр, указанный в пункте 1.5. Соглашения, в порядке и сроке, установленных соответствующим Сертификационным центром для выпуска разных типов SSL-сертификатов.

1.5. В рамках Услуги SSL-сертификат может быть выдан Сертификационными центрами Symantec, Sectigo, GeoTrust, Trustwave, GoGetSSL.

1.6. Порядок и сроки выпуска, продления, перевыпуска, отзыва сертификатов могут быть пересмотрены Сертификационным центром в одностороннем порядке.

## 2. Состав Услуги

2.1. Услуга включает:

2.1.1. проверку оформленной на сайте Исполнителя заявки Заказчика на выпуск, продление или перевыпуск SSL-сертификата с учетом требований Сертификационного центра;

2.1.2. направление в автоматизированном порядке заявки Заказчика на выпуск, продление или перевыпуск SSL-сертификата в Сертификационный центр;

2.1.3. предоставление консультационной помощи по вопросам получения, выпуска, продления или перевыпуска и использования SSL-сертификата;

2.1.4. получение SSL-сертификата от Сертификационного центра с последующей его передачей Заказчику на адрес электронной почты, соответствующий требованиям п. 3.6. Соглашения;

2.1.5. техническую поддержку по вопросам установки SSL-сертификата.

## 3. Порядок оказания Услуги

3.1. Заказчик оформляет заявку в Консоли управления на Интернет-ресурсе Исполнителя (<https://console.ps.kz/>) самостоятельно либо, при необходимости, формирует заказ совместно с Исполнителем. Для подачи заявки на выпуск, продление или перевыпуск SSL-сертификата Заказчик:

- определяет тип сертификата;
- определяет физическое или юридическое лицо, на которое будет оформляться сертификат;
- сохраняет (или использует готовый) CSR;
- сохраняет (или использует готовый) Private Key;
- оплачивает выставленный счет в Консоли управления.

3.2. Услуга оказывается после поступления денежных средств на расчетный счет Исполнителя.

3.3. После оплаты Заказчиком выставленного счета Сертификационный центр по поступившей заявке запускает процедуру валидации сертификата, соответствующую типу сертификата, указанному в заявке Заказчика.

3.4. Для выдачи SSL-сертификата Сертификационным центром проводятся разные проверки в зависимости от типа выбранного сертификата:

- проверка по доменному имени;
- проверка по организации;
- расширенная проверка для особых типов.

3.5. Доменное имя, на которое производится выдача SSL-сертификата, должно принадлежать Заказчику.

3.6. Адрес электронной почты, на который Сертификационный центр вышлет письмо для проверки доменного имени, должен соответствовать одному из вариантов:

- admin@ваш\_домен
- administrator@ваш\_домен
- hostmaster@ваш\_домен
- webmaster@ваш\_домен
- postmaster@ваш\_домен

Использование другого адреса допускается лишь в том случае, если доменное имя зарегистрировано в международной зоне (.com, .net, .org и т. д.), и данный адрес электронной почты указан во WHOIS-записи о владельце домена.

Для некоторых сертификатов могут быть доступны и другие способы проверки домена:

- проверка с помощью DNS-записи: CSR хешируется, хеш-значения необходимо указать в CNAME или TXT-записи домена;
- проверка с помощью HTTP(S): CSR хешируется, хеш-значения необходимо указать в текстовом файле и поместить его в корневой каталог сайта.

Процесс валидации по доменному имени занимает от 5 минут до 10 дней в зависимости от своевременности содействия Заказчика и исполнения им действий, требуемых Сертификационным центром в процессе валидации.

3.7. Проверка по организации (OV) включает в себя:

- проверку домена;
- проверку информации о юридическом лице, указанном в Заявке, путем обращения к соответствующему Реестру;
- звонок от сотрудников Сертификационного центра в качестве завершающего этапа валидации.

Процесс валидации по организации может занять от 3 до 5 дней в зависимости от своевременности содействия Заказчика и исполнения им действий, требуемых Сертификационным центром в процессе валидации.

3.8. Расширенная проверка (EV) включает в себя:

- проверку домена;
- проверку информации об юридическом лице, указанном в Заявке, путем обращения к соответствующему Реестру;
- звонок от сотрудников Сертификационного центра в качестве завершающего этапа валидации.

Процесс расширенной проверки может занять до 10 дней в зависимости от своевременности содействия Заказчика и исполнения им действий, требуемых Сертификационным центром в процессе валидации.

3.9. В случае успешного завершения процедуры валидации Заказчик получает архив с файлами сертификата на электронную почту, указанную при оформлении Заявки на Услугу.

3.10. Установку файлов сертификата на хостинг Заказчик осуществляет самостоятельно или с помощью технической поддержки Исполнителя (по запросу) из Консоли управления или авторизованной электронной почты на [support@ps.kz](mailto:support@ps.kz).

3.11. Услуга считается оказанной с даты выдачи Сертификационным центром SSL-сертификата на имя лица, указанного Заказчиком в Заявке на Услугу.

3.12. Услуга оказывается в сроки, предусмотренные правилами и регламентом Сертификационного центра для типа выбранного SSL-сертификата, при условии осуществления Заказчиком оплаты, согласно разделу 4 Соглашения, и предоставления дополнительных сведений, в случае их запроса Исполнителем или Сертификационным центром.

3.13. Заказчик признает и подтверждает, что надлежащее и своевременное оказание Исполнителем Услуг зависит от содействия Заказчика, а также исполнения Заказчиком следующих встречных обязательств в процессе получения Услуги:

- своевременное предоставление всех сведений (включая документы и исчерпывающие пояснения), запрошенных Исполнителем, Сертификационным центром в связи с оказанием Услуг. Предоставленная информация должна быть полной, актуальной, точной и достоверной;
- своевременное принятие и совершение действий, требуемых Сертификационным центром.

3.14. В случае выявления несоблюдения Заказчиком сроков предоставления сведений и информации Сертификационному центру, а также выполнения необходимых технических процедур для валидации сертификата, Исполнитель вправе:

- направить в Сертификационный центр запрос об отзыве Заявки на Услугу;
- отклонить Заявку Заказчика на Услугу.

## 4. Оплата Услуги

4.1. Стоимость Услуги определяется согласно тарифам Исполнителя: <https://www.ps.kz/ssl>.

4.2. Перевыпуск сертификата может осуществляться неограниченное количество раз в рамках оплаченного периода на бесплатной основе.

4.3. При отказе Сертификационного центра в выпуске или продлении сертификата осуществляется возврат средств, оплаченных Заказчиком по Услуге, только в случае, если с момента выпуска сертификата Сертификационным центром прошло не более 14 (четырнадцать) календарных дней, и причина отказа в выпуске или продлении сертификата не противоречит порядку предоставления Услуги, утвержденному Сертификационным центром.

4.4. Сертификационный центр оставляет за собой право отозвать или отменить сертификат в одностороннем порядке в связи с изменением политики его предоставления.

4.5. В случае отзыва SSL-сертификата (Сертификационным центром или Заказчиком) сумма, уплаченная за оказанную Услугу, подлежит возврату при условии, если с момента первичного выпуска сертификата Сертификационным центром прошло не более 14 (четырнадцати) календарных дней.

4.6. Установка сертификата на бесплатной основе по запросу Заказчика производится Исполнителем при оказании следующих услуг при условии стандартной настройки: Хостинг сайтов (в том числе и Хостинг сайтов для CMS 1С-Битрикс), VPS-хостинг, Облачные серверы, Virtuozzo Application Platform. В случае нестандартных или специфичных настроек, Заказчик обязуется предоставить необходимые инструкции по установке.

## 5. Особые условия

5.1. Срок действия сертификата составляет от 1 года до 3 лет в зависимости от оплаченного Заказчиком периода. Продление сертификата осуществляется не менее чем за 10 (десять) рабочих дней до даты окончания действия сертификата сроком на 1 (один) год.

5.2. Стороны понимают и признают, что возможен отказ Сертификационного центра в выпуске, продлении или перевыпуске SSL, а также отзыв уже оформленного сертификата.

5.3. Заказ Услуги на выпуск, продление, перевыпуск, отзыв сертификата осуществляется только с электронной почты, указанной при регистрации в Консоли управления Заказчика.

5.4. SSL-сертификат подписывается электронной цифровой подписью Сертификационного центра, что гарантирует неизменность содержащейся в SSL-сертификате информации.

5.5. При приобретении сертификата с мультидоменной защитой до окончания его срока действия Заказчик может приобрести дополнительные SAN (Subject Alternative Name) помимо тех, которые включены в базовый пакет SSL-сертификата. При этом Заказчику необходимо учесть, что:

- стоимость дополнительных SAN зависит от количества и типа SAN, а также от типа выбранного сертификата;
- запрос на покупку дополнительных SAN может быть сделан в любое время после активации SSL-сертификата;
- срок действия дополнительных SAN совпадает со сроком действия SSL-сертификата;
- максимальное количество дополнительных SAN, которое может быть добавлено к SSL-сертификату, зависит от типа выбранного сертификата и условий предоставления Услуги;
- Заказчик несет ответственность за предоставление точной и актуальной информации о дополнительных SAN.

5.6. В случае установки сертификата Исполнителем Заказчик обязуется предоставить актуальные и совместимые файлы для установки (ключи в формате .csr и .key, архив с файлами сертификата).

5.7. В случае, если файлы сертификата окажутся несовместимы с предоставленными Заказчиком ключами, Исполнитель инициирует процесс перевыпуска сертификата.

5.8. В случае, если хостинг приобретен у другого провайдера, а заказ на SSL-сертификат был оформлен и оплачен Заказчиком у Исполнителя, установка сертификата не производится.

5.9. Техническая поддержка осуществляется круглосуточно посредством обращения Заказчика через Консоль управления и обработки Исполнителем запросов в Тикет-системе.

Запросы по вопросам установки сертификата обрабатываются Исполнителем в порядке очередности круглосуточно в течение от 4 до 24 часов с момента поступления запроса в установленном порядке.

Исполнитель будет стремиться к максимально быстрой реакции на обращения Заказчика. Время разрешения запроса может увеличиваться в связи со сложностью запросов Заказчика и спецификой взаимодействия с Сертификационным центром.

Консультационная, информационная поддержка обеспечивается путем обращения Заказчика по телефону, через Консоль управления и обработки Исполнителем обращения в Тикет-системе, в соответствии с контактами Заказчика и временными рамками, предусмотренными <https://www.ps.kz/company/contacts>.

Запросы на получение консультационной поддержки процесса выпуска, продления, перевыпуска сертификата обрабатываются Исполнителем в рабочее время с 10:00 до 19:00 в будние дни (суббота, воскресенье, а также праздничные дни — выходные).