

ДОГОВОР-ОФЕРТА на оказание услуг Удостоверяющего центра – версия 5.3

г. Москва

Редакция вступает в силу с 1 мая 2023 года

Несмотря на перевод настоящего Договора на язык, отличный от английского, версия настоящего Договора на английском языке всегда является контрольной и единственной основой для толкования условий настоящего Договора.

ВНИМАТЕЛЬНО ПРОЧИТЕ НАСТОЯЩИЙ ДОГОВОР, ПРЕЖДЕ ЧЕМ ИСПОЛЬЗОВАТЬ ЦИФРОВОЙ СЕРТИФИКАТ, ВЫДАННЫЙ ВАМ ИЛИ ВАШЕЙ ОРГАНИЗАЦИИ. ПРИ ПОДАЧЕ ЗАЯВКИ НА ПОЛУЧЕНИЕ ЦИФРОВОГО СЕРТИФИКАТА ВЫ ПРИНИМАЕТЕ УСЛОВИЯ НАСТОЯЩЕГО ДОГОВОРА. ЕСЛИ ВЫ НЕ ПРИНИМАЕТЕ УСЛОВИЯ НАСТОЯЩЕГО ДОГОВОРА, НЕМЕДЛЕННО ОТМЕНИТЕ ЗАКАЗ В ТЕЧЕНИЕ СЕМИ (7) ДНЕЙ С МОМЕНТА ВЫПУСКА ЦИФРОВОГО СЕРТИФИКАТА, ЧТОБЫ ПОЛУЧИТЬ ПОЛНЫЙ ВОЗВРАТ СТОИМОСТИ. ЕСЛИ У ВАС ВОЗНИКЛИ ВОПРОСЫ ПО НАСТОЯЩЕМУ ДОГОВОРУ, ОБРАТИТЕСЬ К НАМ ПО ЭЛЕКТРОННОМУ АДРЕСУ: legal@globalsign.com

«GlobalSign» — это организация, у которой Абонент размещает заказ на приобретение Сертификата, GMO GlobalSign K.K. (Япония), GlobalSign China Co., Ltd. (Китай), GMO GlobalSign Ltd. (Великобритания), GlobalSign NV (Бельгия), GMO GlobalSign, Inc. (США), GMO GlobalSign Pte. Ltd (Сингапур), GMO GlobalSign Inc. (Филиппины), GMO GlobalSign Certificate Services Pvt. Ltd (Индия), ООО «Джи-Эм-О Глобал Сайн Раша» (Россия), GMO GlobalSign Solutions in Technology S/A (Бразилия) или GMO GlobalSign FZ LLC (Объединенные Арабские Эмираты). Несмотря на вышесказанное, если Абонент заказывает Квалифицированный сертификат eIDAS Великобритании, «GlobalSign» означает GMO GlobalSign Ltd. (Великобритания), если Абонент заказывает Квалифицированный сертификат eIDAS ЕС, «GlobalSign» означает GlobalSign NV (Бельгия).

Общество с ограниченной ответственностью «Джи-Эм-О Глобал Сайн Раша» (далее по тексту – Компания «GlobalSign») в лице Генерального директора Рыжикова Дмитрия Александровича, действующего на основании Устава, в соответствии с п. 2 ст. 437 Гражданского кодекса Российской Федерации, предлагает любому физическому или юридическому лицу, желающему воспользоваться услугами Компании GlobalSign, заключить договор публичной оферты (далее – «Договор») на нижеследующих основаниях. Договор действует с даты размещения заявки на выпуск сертификата (далее — «Дата вступления в силу»).

Предметом Публичной оферты является оказание услуг по выпуску Цифровых сертификатов и предоставление услуг согласно разделу 3.0 данного Договора публичной оферты.

Если вы являетесь Партнером и выступаете в качестве уполномоченного представителя Абонента при подаче заявки на получение сертификата или связанных с ним услуг, вы заявляете и гарантируете Компании «GlobalSign» и доверяющим сторонам, что вы получили полномочия Абонента на заключение настоящего Договора от его имени и должны соблюдать и обеспечивать соблюдение Абонентом настоящего Договора.

Если Абонент приобретает или использует услуги через Партнера, то настоящим Абонент заявляет и гарантирует, что он уполномочил Партнера действовать от имени Абонента в отношении услуг, включая, но не ограничиваясь, размещение заказа, принятие услуг, эксплуатацию, продление и отзыв Цифрового сертификата Абонента. Уполномочивая Партнера предоставлять или перепродавать услуги Абоненту, Абонент настоящим подтверждает своё согласие с настоящим Договором в отношении использования услуг. Если Абонент не согласен с условиями настоящего Договора, то он не вправе приобретать или использовать соответствующие услуги Компании GlobalSign.

Услуги по выпуску Цифровых сертификатов предоставляются после завершения процедуры верификации Абонента. Оплата производится в течение 15 (пятнадцати) календарных дней с момента выпуска Цифрового сертификата.

1.0 Термины и определения

В настоящий Договор включены следующие политики и инструкции:

- The GlobalSign Certification Practice Statement (CPS);
- The GlobalSign Warranty Policy;
- The GlobalSign Payment Terms;

Текущие версии вышеуказанных документов находятся по адресу:

<https://www.globalsign.com/en/repository/>, <https://www.globalsign.com/en/company/corporate-policies> и <https://www.globalsign.com/ru-ru/repository-ru>.

Текущая версия требований CA/B Forum Baseline Requirements находится по адресу <https://cabforum.org/baseline-requirements-documents/>.

В настоящем Договоре используются следующие термины и определения:

Абонент	Заявитель, подавший самостоятельно либо в лице своего Представителя, в том числе Партнера, заявку на получение (или обновление) Цифрового сертификата и получивший такой Цифровой сертификат после его выпуска Удостоверяющим центром.
Аффилиаты	Корпорация, товарищество, совместное предприятие или иное юридическое лицо, контролируемое или находящееся под общим контролем другого юридического лица или органа, агентства, отдела или любого предприятия под непосредственным контролем государственного органа.
Бенефициары Цифрового сертификата	Абоненты, которые являются участниками Абонентского Договора или приняли Условия использования Цифрового сертификата, все Поставщики программного обеспечения, с которыми Компания «GlobalSign» заключила контракт на включение своих корневых сертификатов в приложения программного обеспечения (например, Microsoft), распространяемые таким Поставщиком программного обеспечения, и все полагающиеся стороны, которые разумно полагаются на действительный сертификат.
Государственная организация	Юридическое лицо, агентство, департамент, министерство, филиал или аналогичное государственное учреждение, являющееся частью государственной системы страны, управляемое государством, или политическое подразделение внутри страны (например: город, округ, провинция и т. д.).
Доступ к информации организации	Расширение Цифрового сертификата, которое указывает на способ доступа к информации и услугам для издателя Цифрового сертификата, в котором находится расширение
Закрытый ключ	Математически сгенерированный ключ, который держится владельцем в секрете и используется, чтобы создавать Электронные подписи или для расшифровки электронных данных.
Запрос Цифрового сертификата	Последовательность описана в основных требованиях Консорциума CA/Browser Forum к выдаче и управлению публично-доверенными сертификатами (« Основные требования »), требованиях Консорциума CA/B Forum к выдаче и управлению публично-доверенными сертификатами с расширенной проверкой, основных требованиях Консорциума CA/B Forum к выдаче и управлению публично-доверенными сертификатами подписи кода
Имя домена	Символьное имя, служащее для идентификации интернет-узлов в системе доменных имён (DNS).
Квалифицированный сертификат	Сертификат, соответствующий требованиям, установленным регламентом eIDAS / UK eIDAS.
Квалифицированное устройство для создания подписей (QSCD)	Устройство для создания электронной подписи/печати, отвечающее требованиям приложения II к регламенту eIDAS.
Компрометация ключа	Закрытый ключ считается скомпрометированным, если его данные были раскрыты неавторизованному лицу, неавторизованное лицо имело к нему доступ, или существует практический метод, с помощью которого неавторизованное лицо может раскрыть его значение.
Консорциум CA/Browser Forum	Группа экспертов в данной отрасли, в которую входят Удостоверяющие центры и Поставщики программного обеспечения. Подробная информация об этой группе экспертов доступна по ссылке: www.cabforum.org

Конфиденциальная информация	Любая информация (научно-техническая, технологическая, производственная, финансово-экономическая или иная, в том числе о средствах защиты информации, идентификации, аутентификации, авторизации (логинах, паролях и т.д.), статистическая, информация о клиентах, о продуктах, услугах, результатах исследований и т.д.), передаваемая Заказчиком Исполнителю в любой возможной форме (устной, письменной, электронной, иной), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности её третьим лицам, к которой нет свободного доступа на законном основании и обозначенная передающей Стороной как конфиденциальная (в том числе в момент раскрытия); факт заключения и содержание Договора; персональные данные, определяемые в соответствии с законодательством Российской Федерации, передаваемые Абонентом (его Представителем), обработка и хранение которых осуществляется Компанией «GlobalSign», а также любая информация, полученная путём выписки, обобщений или аналитических выкладок из Конфиденциальной информации.
Корневой сертификат	Самоподписанный Сертификат, выданный Корневым Удостоверяющим центром для собственной идентификации и верификации Сертификатов, выданных Подчинённым Удостоверяющим центрам
Лицо, запрашивающее Цифровой сертификат	Представитель Абонента либо Партнера, который владеет прямо оговорёнными полномочиями его представлять в качестве Лица, запрашивающего Цифровой сертификат, или представлять третью сторону (например, в качестве поставщика услуг в сети Интернет или хостинговой компании), который заполняет и подаёт Заявки на получение Цифрового сертификата от имени Абонента. Лица, запрашивающие Цифровой сертификат, могут быть предварительно утверждены посредством таких Управляемых услуг как MSSL или ePKI.
Лицо, утверждающее Цифровой сертификат	Представитель Абонента либо Партнера, который владеет прямо оговорёнными полномочиями его представлять (i) в качестве Лица, запрашивающего Цифровой сертификат, или представлять третью сторону в качестве Лиц, запрашивающих Цифровой сертификат, и (ii) утверждать Заявки на получение Цифровых сертификатов, поданные другими Лицами, запрашивающими Цифровой сертификат.
Орган регистрации («ОР»)	Орган, ответственный за идентификацию и аутентификацию в целом или частично «Субъекта», которому впоследствии будут выданы Цифровые сертификаты. «ОР» может помогать в процессе подачи заявки на выдачу Цифрового сертификата или в процессе его аннулирования.
Открытый ключ	Математически сгенерированный ключ, который находится в свободном доступе и используется для проверки Цифровых сертификатов, созданных при помощи соответствующего Закрытого ключа, и для шифрования электронных данных, которые могут быть расшифрованы только при помощи соответствующего Закрытого ключа.
Пара ключей	Закрытый ключ и ассоциированный с ним Открытый ключ.
Партнер	Юридическое лицо, уполномоченное Компанией «GlobalSign» перепродавать или предоставлять услуги Абоненту
Подозрительный код	код, который является функционально вредоносным или серьёзно уязвимым благодаря содержанию программ-шпионов, вредоносных программ и других кодов, которые устанавливаются без согласия пользователя и/или противодействуют собственному удалению, и кодов, которые могут быть использованы путём, не соответствующим замыслу его проектировщиков, компрометируя достоверность платформ, на которых они выполняются.
Подчинённые УЦ	Центры сертификации, чьи Цифровые сертификаты подписаны корневым удостоверяющим центром, или другими подчинёнными УЦ.
Полностью определённое имя домена («FQDN»)	Доменное имя, которое включает пометки всех вышестоящих узлов в системе доменных имён в Интернете.
Поставщик программного обеспечения	Поставщик программного обеспечения в интернет-браузерах или других приложениях программного обеспечения проверяющей стороны, которые отображают или используют сертификаты и включают в себя корневые сертификаты.

Представитель Абонента	Физическое лицо, уполномоченное Абонентом, действовать от его имени согласно прямо оговорённых полномочий, предоставленных ему Абонентом.
Протокол проверки статуса OCSP	Межсетевой протокол (типа "запрос-ответ") используется для получения статуса отзыва Цифрового сертификата в режиме реального времени от доверенного субъекта («OCSP-респондера»).
Регламент eIDAS ("eIDAS")	Регламент Европейского Парламента и Совета Европейского Союза 910/2014 от 23 июля 2014 г. об электронной идентификации и удостоверительных сервисах для электронных транзакций на внутреннем рынке и об отмене Директивы 1999/93/EC
Регламент UK eIDAS ("UK eIDAS")	Регламент Великобритании eIDAS об электронной идентификации и удостоверительных сервисах для электронных транзакций от 2016 года..
Регистрант доменного имени	Иногда упоминается как «владелец» доменного имени, но более правильно, человек (люди) или юридическое лицо (лица), зарегистрированные в реестре доменных имён как имеющие право контролировать использование доменного имени. Ими могут быть физические или юридические лица, которые числятся как «Регистранты» по данным WHOIS или регистра доменных имён.
Регистратор доменных имён	Лицо или организация, регистрирующие доменные имена под эгидой или по согласованию с: (I) Интернет-корпорацией по присвоению имён и номеров (ICANN), (II) национальными органами/реестрами доменных имён, или (III) справочно-информационными центрами сети Интернет (в том числе их Афффилиатами, подрядчиками, делегатами, наследниками или правопреемниками).
Североамериканский совет по энергетическим стандартам («NAESB»)	Стандарты по безопасности открытых/закрытых ключей (PKI) – WEQ-012 v3.0 и требования Североамериканского совета по энергетическим стандартам к удостоверению для уполномоченных удостоверяющих центров. Подробные данные по техническим и управленческим вопросам, требования к которым должен выполнять Удостоверяющий центр, чтобы стать Удостоверяющим центром, уполномоченным Североамериканским советом по энергетическим стандартам.
Система доменных имён («DNS»)	Интернет-сервис, который переводит доменные имена в IP-адреса.
Список отозванных Цифровых сертификатов («CRL»)	Список, включающий в себя электронные данные с информацией об отозванных Цифровых сертификатах
Субъект	Физическое лицо, устройство, система или юридическое лицо, идентифицированные в Цифровом сертификате в качестве объекта. Если Субъектом является устройство или система, то оно должно находиться под контролем и управлением Абонента.
Удостоверяющий центр («УЦ»)	Компания «GlobalSign» или предприятие, владеющее сертификатом Компании «GlobalSign» на выдачу Цифрового сертификата Субъекту. Компания «GlobalSign» является Удостоверяющим центром Заказчика согласно настоящему Договору.
Управляемая услуга MSSL	Облачная служба, которая реализует метод управления SSL-сертификатами по запросу. Система мгновенно выдаёт SSL-сертификаты высокой доверенности, может оптимизировать рабочие процессы, использующие стандарт SSL, уменьшить затраты на их содержание и вовремя предупредить об истечении срока действия сертификатов
Управляемая услуга ePKI	Облачная служба управляемой инфраструктуры PKI, используемая для выпуска клиентских сертификатов GlobalSign и управления ими
Условия использования	Положения, касающиеся сохранности и приемлемых путей применения Цифрового сертификата, выданного в соответствии с основными требованиями, когда Абонент является Афффилиатом УЦ.

Хранитель Цифрового сертификата	Лицо, назначенное ответственным за хранение Цифрового сертификата. Им может быть то же лицо, что и Абонент, либо другое лицо.
Цифровая подпись	Для кодирования сообщений с помощью асимметричной криптосистемы и хэш-функции таким образом, что лицо, имеющее начальное сообщение и открытый ключ подписавшего может с точностью определить, были ли произведены какие-либо изменения с использованием закрытого ключа, соответствующего открытому ключу подписавшего и было ли исходное сообщение изменено благодаря произведённым преобразованиям. Данные, подписанные цифровыми подписями, имеют отношение к электронным данным с прилагаемыми цифровыми подписями.
Цифровой сертификат	Электронный документ, который использует цифровую подпись для привязки открытого ключа и удостоверения личности.
OCSP-респондер	Имеет значение, установленное в определении термина Протокол проверки статуса Цифрового сертификата OCSP.
Wildcard сертификат	Цифровой сертификат, содержащий звёздочку (*) в крайнем левом положении любого из полностью уточнённых доменных имён субъекта, содержащихся в сертификате.

2.0 Полномочия на использование Цифровых сертификатов

2.1 Предоставление полномочий.

Начиная с Даты вступления в силу и на срок, указанный в каком-либо выданном Цифровом сертификате («Действителен с» до «Действителен до»), Компания «GlobalSign» предоставляет Абоненту полномочия использовать запрошенный им Цифровой сертификат для выполнения операций с Закрытым и (или) Открытым ключом.

2.2 Ограничения полномочий.

Абонент обязуется использовать Цифровой сертификат только с криптографическим программным обеспечением, имеющим действующую лицензию.

3.0 Услуги, предоставляемые Компанией «GlobalSign»

После принятия настоящего Договора и уплаты необходимых взносов, помимо «Предоставления полномочий», Компания «GlobalSign» или сторонний поставщик услуг, назначенный Компанией «GlobalSign», обязуется предоставлять следующие услуги Абоненту с момента выдачи Цифрового сертификата.

3.1 Услуги по предоставлению Списка отзыва Цифровых сертификатов (CRL), Протокола проверки статуса Цифрового сертификата (OCSP) и информации об Органах, выдающих сертификаты.

Компания «GlobalSign» обязуется принимать разумные меры, необходимые для того, чтобы создать, собрать и сделать следующее доступным в электронном виде для всех Сертификатов, подписанных и выданных Удостоверяющим центром Компании «GlobalSign»:

- Списки отзыва Цифровых сертификатов (CRL) для каждого сертификата с указанием точки распространения сертификата CRL;
- Респондеры Протокола проверки статуса Цифрового сертификата (OCSP) для любого Цифрового сертификата с респондером Протокола проверки статуса Цифрового сертификата (OCSP);
- Информацию о Цифровом сертификате в местах Доступа к информации Организации; при условии, что Компания «GlobalSign» не может нести ответственность за невыполнение своих обязанностей согласно настоящему Договору в результате какой-либо задержки или невозможности выполнения обязанностей вследствие поломки оборудования или сбоя средств связи, которые не находятся под контролем Компании «GlobalSign».

3.2 Службы отзыва Цифровых сертификатов

Компания «GlobalSign» может отозвать сертификат по обстоятельствам, указанным в CPS, или если Компания «GlobalSign» получит уведомление, или иным образом станет известно, что Абонент нарушил какие-либо из существенных обязательств по настоящему Договору.

3.3 Генерирование ключа

Если Пары ключей генерируются Компанией «GlobalSign» от имени Абонента и предлагаются токены или PKCS#12, Компания «GlobalSign» использует надёжные системы для генерирования таких Пар ключей, при этом применяются следующие условия:

- Компания «GlobalSign» генерирует Пары ключей при помощи платформы, которая подходит для этой цели и обеспечивает шифрование Закрытых ключей при их передаче Абоненту;
- Компания «GlobalSign» использует ключ подходящей длины и алгоритм для Электронной подписи;
- В случае выпуска Цифрового сертификата подписи кода с расширенной проверкой, Абонент предупреждён о том, что Компания «GlobalSign» не будет выпускать ключи длиной менее чем 2048 бит, и для Цифрового сертификата подписи кода с расширенной проверкой будет предлагаться только алгоритм шифрования SHA2.

Компания «GlobalSign» не генерирует Пары ключей для публично доверенных сертификатов SSL.

3.4 Услуги по установке удостоверения безопасности сайта для веб-страниц (SiteSeal), использующих Цифровые сертификаты SSL/TLS, и ответы OCSP/CRL-респондеров

Компания «GlobalSign» предоставляет Заявителю разрешение использовать удостоверение безопасности сайта Компании «GlobalSign» на веб-странице Заявителя с максимальным количеством проверок — пятьсот тысяч (500 000) в день. Компания «GlobalSign» оставляет за собой право ограничить или прервать доступ к удостоверениям безопасности сайта в случае превышения ограничения.

Компания «GlobalSign» предоставляет услуги по проверке действительности выданного Цифрового сертификата 24 часа в сутки, 7 дней в неделю через респондер Протокола проверки статуса Цифрового сертификата или CRL-респондер. Для каждого Цифрового сертификата установлено ограничение — пятьсот тысяч (500 000) проверок в день. Компания «GlobalSign» оставляет за собой право принудительного использования технологии «OCSP Stapling» в случае превышения ограничения.

3.5 Услуги метки времени для Цифровых сертификатов подписи кода

Компания «GlobalSign» предлагает возможность устанавливать временную маркировку кода, подписанного Цифровым сертификатом подписи кода, в качестве безвозмездной услуги при рациональном её использовании. Следуя передовой практике, Компания «GlobalSign» рекомендует Абоненту устанавливать метку времени при подписи программного кода, используя соответствующие сервера временных меток. Компания «GlobalSign» устанавливает ограничение рационального количества временных маркировок в течение срока действия Цифрового сертификата подписи кода и оставляет за собой право отменить услугу или предусмотреть дополнительную плату за услугу, если количество временных маркировок окажется чрезмерным по мнению Компании «GlobalSign».

3.6 Услуги метки времени для Цифровых сертификатов Adobe Authorized Trust List (AATL)

Компания «GlobalSign» может предоставить платную услугу метки времени для подписи документов Portable Document Format (PDF) и Microsoft Office. Лимит подписей в год согласно данной услуге согласовывается при подаче заявки. Компания «GlobalSign» оставляет за собой право отменить услугу или взыскать за неё дополнительную плату, если количество операций отметки времени превышает установленный лимит.

4.0 Обязанности и гарантии Абонента

Абонент и/или Партнер гарантируют Компании «GlobalSign» и Бенефициарам Цифрового сертификата:

4.1 Точность данных.

Абонент/Партнер всегда предоставляет точную, полную и достоверную информацию Компании «GlobalSign» в Заявке на получение Цифрового сертификата или по запросу Компании «GlobalSign» в связи с выдачей Цифрового сертификата, включая, но не ограничиваясь именем субъекта, URL к информационным источникам и дополнительного описания при оформлении Цифровых сертификатов подписи кода.

4.2 Защита Закрытого ключа.

Абонент принимает все разумные меры для того, чтобы в единоличном порядке осуществлять контроль, обеспечивать конфиденциальность, постоянно защищать Закрытый ключ, связанный с запрашиваемым Цифровым сертификатом и любыми связанными с ним данные активации или устройства, напр., пароль или токен.

Для Цифровых сертификатов подписи кода Абонент должен принимать единоличный контроль, обеспечивать конфиденциальность и должным образом защищать в соответствии с разделом 4.15 Закрытый ключ, соответствующий Открытому ключу, который должен быть включён в сертификат (и любые связанные с ним данные активации или устройства, напр., пароль или токен). Абонент заявляет, что он будет генерировать и управлять любым устройством, хранящим Закрытые ключи, безопасным способом, как описано в документе о лучших практиках подписания кода. Абонент должен использовать

пароли, которые генерируются случайным образом и содержат не менее 16 символов, содержащих прописные буквы, строчные буквы, цифры и символы.

4.3 Повторное применение закрытого ключа.

Абонент обязуется не использовать Закрытый ключ для Цифрового сертификата подписи кода, если Открытый ключ для него уже используется или будет использоваться для иного Цифрового сертификата.

4.4 Ненадлежащее использование.

Абонент обязан предоставлять надлежащие сетевые и другие средства защиты, чтобы предотвратить неавторизованное или ненадлежащее использование закрытого ключа, а Компания «GlobalSign» может отменить сертификат без предварительного уведомления при наличии несанкционированного доступа к закрытым ключам.

4.5 Принятие Цифрового сертификата.

Абонент обязуется использовать Цифровой сертификат только после просмотра и проверки данных, которые содержатся в Цифровом сертификате. Если Абонент не уведомит Компанию «GlobalSign» в течение семи (7) дней с момента получения, Услуга по выпуску Цифрового сертификата считается принятой.

4.6 Использование Цифрового сертификата Компании «GlobalSign».

Абонент обязуется устанавливать Цифровой сертификат только на серверах, которые соответствуют данному Цифровому сертификату, использовать Цифровой сертификат Компании «GlobalSign» в строгом соответствии действующему законодательству и строго соблюдать условия Договора и условия использования.

Цифровой сертификат ни в коем случае не должен использоваться в преступной деятельности, такой как фишинговые атаки, мошенничество, сертификация и подпись вредоносных программ. Абонент принимает на себя дополнительные обязательства и гарантии, касающиеся неосознанной подписи программ, которые содержат Подозрительный код, распространения контента, который вводит в заблуждение, создаёт неудобства или раздражает получателя, напр., Программное обеспечение, которое включает нежелательный функционал, нераскрытый должным образом пользователю до начала установки, или признается нежелательным/подозрительным коммерческими антивирусными приложениями.

Абонент обязан использовать Цифровой сертификат и связанный с ним Закрытый ключ только в разрешённых и законных целях, в том числе не использовать Цифровой сертификат для подписания Подозрительного кода и использовать Цифровой сертификат и Закрытый ключ исключительно в соответствии со всеми применимыми законами и исключительно в соответствии с Договором.

4.6.1 Подпись файлов PDF.

Если Цифровой сертификат используется для подписи документов в формате PDF, Абонент обязуется предоставить информацию, которая позволяет идентифицировать лицо, подписавшее определённый документ.

4.6.2 Цифровой сертификат подписи кода с расширенной проверкой.

Абонент принимает дополнительные обязательства и гарантии и обязуется использовать Цифровой сертификат подписи кода с расширенной проверкой следующим образом:

- Подписывать только коды, соответствующие требованиям Консорциума CA/Browser Forum, приведённым в Базовых требованиях к выдаче и управлению Общедоступными сертификатами подписи кода;
- Использовать в строгом соответствии с действующим законодательством;
- Использовать исключительно для разрешённых видов деятельности компании;
- Использовать в строгом соответствии с настоящим Договором.

Если Абоненту становится известно (любыми способами) о том, что подписанный код содержит вредоносное программное обеспечение или серьёзную уязвимость, он обязан незамедлительно сообщить об этом Компании «GlobalSign».

4.6.3 Условие Microsoft

Абонент признает, что компания Microsoft может самостоятельно определять Компрометацию ключа; службы и приложения Microsoft могут самостоятельно изменять репутацию клиента, что влияет на приостановку действия Цифрового сертификата независимо от статуса отзыва Цифрового сертификата.

4.7 Отчётность и отзыв.

Абонент обязуется прекратить использование Цифрового сертификата и связанного с ним Закрытого ключа (за исключением расшифровки) и немедленно подать запрос в Компанию «GlobalSign» на отзыв Цифрового сертификата, если (а) информация, содержащаяся в Цифровом сертификате, становится неточной или неправильной; или (б) имеется факт или подозрение в некорректном использовании, утере, краже или компрометации Закрытого ключа, связанного с Открытым ключом Цифрового сертификата, а также в утере контроля над Закрытым ключом из-за компрометации данных активации (напр., PIN кода) или иных причин; или (с) в случае Цифрового сертификата подписи кода имеются доказательства использования Цифрового сертификата для подписи Подозрительного кода.

Запросы на отзыв Цифрового сертификата должны быть отправлены через личный кабинет, используемый для выпуска Цифрового сертификата, или через обращение на report-abuse@globalsign.com.

4.7.1 Причины отзыва: Абонент подтверждает понимание причин отзыва Цифрового сертификата, в том числе указанных в разделе 4.9.1 CPS.

4.7.2 Уведомление GlobalSign об изменениях статуса: Если Сертификат выдается Абоненту (“Новый сертификат”) на основе другого действительного сертификата, находящегося у Абонента (“Исходный сертификат”), и впоследствии Исходный сертификат был отменен или отозван, Абонент обязан сообщить Компании «GlobalSign» об измененном статусе сертификата. После такого уведомления GlobalSign проведет расследование, чтобы определить, необходимо ли приостановить действие или отозвать новый сертификат.

4.8 Прекращение использования Цифрового сертификата.

Абонент должен немедленно прекратить использование Закрытого ключа, связанного с Открытым ключом Цифрового сертификата, при отзыве Цифрового сертификата или в случае компрометации выпускающего УЦ;

4.9 Реагирование.

Абонент должен следовать инструкциям Компании «GlobalSign» относительно случаев Компрометации ключа или неправильного использования Цифрового сертификата в течение сорока восьми (48) часов;

4.10 Подтверждение и принятие.

Абонент принимает Положения о правилах сертификации (CPS). Абонент подтверждает и соглашается с тем, что Компания «GlobalSign» имеет право незамедлительно отозвать Цифровой сертификат в случае нарушения Заявителем условий Договора или Условий использования, или в случае, если Компании «GlobalSign» становится известно о том, что Цифровой сертификат используется в преступных целях, таких как фишинговые атаки, мошенничество или распространение вредоносного программного обеспечения. В случае использования Цифровых сертификатов подписи кода с расширенной проверкой совместно с услугами и программным обеспечением Microsoft, Абонент также уведомлён, что независимо от того, что Цифровой сертификат не отозван Компанией «GlobalSign», он может быть отозван компанией Microsoft без уведомления в случаях, если она признает его компрометацию, подписанный им код вредоносным, подозрительным или наносящим вред пользователям соответствующих программных приложений Microsoft;

4.11 Распространение информации.

В отношении Цифровых сертификатов подписи кода Абонент признает и соглашается с тем, что, если (а) Цифровой сертификат или Абонент определены как источник Подозрительного кода, или (б) полномочия на запрос Цифрового сертификата не могут быть проверенными, или (с) Цифровой сертификат отозван не по запросу заявителя (напр., в результате Компрометации ключа, обнаружения вредоносного ПО и т.д.), то Компания «GlobalSign» уполномочена предоставить информацию об Абоненте, подписанном ПО, Цифровом сертификате и т.д. другим Удостоверяющим центрам, а также отраслевым группам, включая Консорциум CA/Browser Forum.

4.12 Соблюдение основных требований.

Абонент признает и соглашается с тем, что Компания «Globalsign» может вносить изменения в Договор, если это необходимо для соблюдения любых изменений основных требований Консорциума CA/B Forum к выдаче и управлению публично-доверенными сертификатами, требований Консорциума CA/B Forum к выдаче и управлению публично-доверенными сертификатами с расширенной проверкой, основных требований Консорциума CA/B Forum к выдаче и управлению публично-доверенными сертификатами подписи кода, требований программ корневых сертификатов поставщиков браузеров или любых других

применимых требований.

4.13 Исключительный контроль доменов для Цифровых сертификатов SSL/TLS.

Абонент подтверждает, что ему принадлежит исключительное право контроля над доменом (доменами) или IP-адресами, указанными в списке альтернативных доменных имён (SubjectAltNames), указанным в заявке на получение Цифрового сертификата SSL/TLS. Как только исключительный контроль над каким-либо доменом (доменами) прекращается, Абонент обязуется незамедлительно сообщить об этом Компании «GlobalSign» согласно обязательствам, указанным в пункте «Отчётность и отзыв».

4.14 Исключительный контроль над электронными адресами для Цифровых сертификатов «PersonalSign».

Абонент подтверждает, что ему принадлежит исключительное право контроля над электронными адресами согласно заявке на получение Цифрового сертификата «PersonalSign». Как только исключительный контроль над каким-либо электронным адресом прекращается, Абонент обязуется незамедлительно сообщить об этом Компании «GlobalSign» согласно обязательствам, указанным в пункте «Отчётность и отзыв».

4.15 Генерирование и использование ключей

Если Пары ключей генерируются Абонентом или Партнером, то следует использовать надёжные системы для генерирования Пар ключей, при этом применяются следующие условия:

- Пары ключей должны генерироваться при помощи подходящей для этой цели платформы. В случае AATL подписи документов следует использовать платформу, совместимую со стандартом FIPS 140-2 2-го уровня;
- Следует использовать ключ с подходящей для Цифровой подписи длиной и алгоритмом;
- Абонент обязан удостовериться, что Открытый ключ, предоставленный Компанией «GlobalSign», полностью соответствует Закрытому ключу.

Если Пары ключей генерируются с помощью аппаратного обеспечения, согласно требованиям соответствующего Положения о правилах сертификации (CPS):

- Абонент управляет процессами, включая, но не ограничиваясь, изменения данных активации, которые обеспечивают использование любого Закрытого ключа в аппаратных модулях системы безопасности (HSM) или токенах, через Хранителя Цифрового сертификата, обладающим необходимой квалификацией и знаниями,
- Абонент гарантирует прохождение Хранителем Цифрового сертификата должного обучения мерам безопасности в целях, для которых был выдан Цифровой сертификат,
- Все Хранители Цифровых сертификатов обязуются принимать разумные меры, необходимые для поддержания полного контроля, соблюдения конфиденциальности, должной защиты Закрытых ключей, которые соответствуют Открытым ключам и подходят к запрашиваемому Цифровому сертификату, а также любым связанным механизмам аутентификации для получения доступа к ключам — например, пароли к токенам или аппаратному модулю системы безопасности.

4.15.1 Цифровые сертификаты подписи кода:

Для стандартных сертификатов подписи кода, выпущенных до 24 апреля 2023:

Абонент должен использовать один из следующих способов для создания и защиты закрытых ключей. Компания «GlobalSign» рекомендует Абоненту использовать метод 1 или 2:

1. Trusted Platform Module (TPM), содержащий в себе криптопроцессор, обеспечивает средства безопасного создания ключей шифрования, способных ограничить использование ключей. Этот модуль имеет следующие возможности: удалённую аттестацию, привязку и надёжное защищённое хранение
2. Аппаратный криптомодуль, сертифицированный как соответствующий по крайней мере FIPS 140 Level 2, общим критериям EAL 4+ или эквивалентный
3. Ещё один тип токена с форм-фактором устройства SD-карты или USB-токена (не обязательно сертифицированный как совместимый с FIPS 140 Level 2 или Common Criteria EAL 4+). Абонент гарантирует, что он будет хранить токен физически отдельно от устройства, на котором размещена функция подписи кода, до тех пор, пока не начнётся сеанс подписи.

Для сертификатов EV CodeSigning, выпущенных до 24 апреля 2023:

Закрытый ключ Абонента должен быть сгенерирован, сохранен и использован в криптомодуле, который соответствует или превосходит требования FIPS 140-2 level 2 или Common Criteria EAL 4+.

Для всех сертификатов подписи кода, выпущенных после 24 апреля 2023:

Абонент заявляет, что будет использовать один из следующих вариантов для генерации и защиты своих закрытых ключей сертификата подписи кода в аппаратном криптомодуле с форм-фактором, сертифицированном как соответствующий по крайней мере FIPS 140-2 Level 2 или общим критериям EAL 4+:

- Абонент использует аппаратный криптомодуль, соответствующий указанному требованию.
- Абонент использует облачное решение для генерации и защиты ключей со следующими требованиями: а. Создание, хранение и использование закрытого ключа должны оставаться в пределах границ безопасности аппаратного криптомодуля облачного решения, соответствующего указанным требованиям; б. Подписка на уровне, который управляет закрытым ключом, должна быть настроена таким образом, чтобы регистрировать все доступы, операции и изменения конфигурации к ресурсам, защищающим закрытый ключ.
- Абонент использует службу подписи, которая соответствует требованиям раздела 6.2.7.3 “Базовых требований к выдаче общедоступных сертификатов подписи кода и управлению ими”.

В любое время применения и жизненного цикла Цифрового сертификата Абонент должен иметь возможность по запросу Компании «GlobalSign» представить доказательство того, что пара ключей сгенерирована и защищена в соответствии с этими требованиями. Непредоставление таких доказательств может привести к отзыву Цифрового сертификата.

Абонент также гарантирует, что он будет хранить токен физически отдельно от устройства, на котором будет производиться подпись кода, до начала сеанса подписи.

4.15.3 Квалифицированные сертификаты: Абонент принимает и соглашается с тем, что:

- Закрытые ключи должны храниться (или соответственно использоваться) под единоличным контролем Субъекта (в случае квалифицированных сертификатов для электронных подписей) или под контролем Субъекта (в случае квалифицированных сертификатов для электронных печатей),
- Закрытые ключи должны использоваться только для электронных подписей (в случае квалифицированных сертификатов для электронных подписей) или электронных печатей (в случае квалифицированных сертификатов для электронных печатей),

Для квалифицированных сертификатов, для которых требуется устройство для создания квалифицированной подписи или печати (QSCD):

- Цифровые подписи должны создаваться только устройством QSCD,
- Закрытые ключи должны быть сгенерированы и сохранены в сертифицированном QSCD, который либо был предоставлен, либо одобрен в письменной форме Компанией «GlobalSign»,
- Статус сертификации QSCD должен контролироваться Абонентом, и в случае изменения статуса сертификации QSCD должны быть приняты соответствующие меры.

4.16 Обязательства Североамериканского совета по энергетическим стандартам (NAESB).

Абоненты Цифровых сертификатов Североамериканского совета по энергетическим стандартам («NAESB») признают понимание следующих обязательств Североамериканского совета по энергетическим стандартам, приведённых в Стандарте деловой практики в оптовом электроэнергетическом секторе WEQ012 («Стандарты WEQ PKI»):

Абоненты, подпадающие под действие Стандартов «WEQ PKI», должны быть зарегистрированы в Реестре идентификации пользователей Североамериканского совета по энергетическим стандартам и представить доказательства того, что они являются пользователями, которым разрешено заниматься торговой деятельностью на оптовом рынке электроэнергии. Пользователи и организации, которым требуется доступ к программам посредством аутентификации, определённой в Стандартах «WEQ PKI», которые не подпадают под требования к участникам оптового рынка электроэнергии (например, регулирующие агентства, университеты, консалтинговые фирмы и т. д.) должны пройти регистрацию.

Зарегистрированные пользователи и группы пользователей должны соответствовать всем требованиям к конечным пользователям, изложенным в Стандартах «WEQ PKI».

Каждая организация, которая является Абонентом, должна подтвердить удостоверяющему центру, что она ознакомилась и согласна с условиями следующих Стандартов «WEQ PKI».

4.16.1 Абонент признает потребность электроэнергетического сектора в безопасной закрытой электронной связи, которая способствует выполнению следующих целей:

- Конфиденциальность: гарантия пользователю того, что никто, кроме адресата, не сможет прочесть определённую часть данных;
- Аутентификация: гарантия одному пользователю того, что другой пользователь не сможет выдать себя за него;
- Целостность: гарантия невозможности изменить данные пользователя (намеренно или ненамеренно), независимо от времени и места;
- Предотвращение отказа от выполнения обязательств: сторона не может отрицать проведение транзакции или отправку электронного письма.

4.16.2 Абонент подтверждает проверку криптографии Открытого ключа, при которой используются Цифровые сертификаты для привязки личного или системного Открытого ключа к пользователю и поддержания обмена ключами с симметричным шифрованием.

4.16.3 Абонент ознакомился со Стандартами «WEQ PKI», которые связаны с созданием надёжного PKI.

4.16.4 Абонент ознакомился с Положениями о правилах сертификации Компании «GlobalSign» (CPS) для отраслевых стандартов.

При необходимости, Абонент обязан зарегистрировать юридическое лицо и защитить «Идентификационный код юридического лица», который будет опубликован в NAESB EIR и будет использоваться во всех абонентских заявках пользователя. В соответствии с требованиями WEQ-012 при выдаче Цифровых сертификатов для энергетической отрасли для приложений отличных от WEQ-012, ACA должны соответствовать стандартам WEQ PKI за исключением положений WEQ-012.12.1.9, WEQ-012-1.3.3 и WEQ-012.1.4.3, которые требуют регистрации пользователя в NAESB EIR.

Абоненты должны соответствовать следующим требованиям:

- Защищать собственные закрытые ключи от доступа посторонних лиц;
- Идентифицировать посредством Реестра идентификации пользователей NAESB EIR определённого пользователя, который выбрал Компанию «GlobalSign» в качестве авторизованного удостоверяющего центра;
- Выполнять все договорённости и договоры, заключённые с Компанией «GlobalSign» согласно отчётам о сертификации Компании «GlobalSign», которые необходимы Компании «GlobalSign» для выдачи Цифровых сертификатов Конечным пользователям с целью обеспечения безопасности электронной связи;
- Выполнять все необходимые обязанности согласно договору о сертификации Компании «GlobalSign», например, проходить процедуру подачи заявки на получение Цифрового сертификата, подтверждение или проверку личности Заказчика, и процедуру управления Цифровым сертификатом.
- Подтверждать наличие программы управления Цифровыми сертификатами PKI, прохождение всеми работниками обучения этой программе, и организацию контроля над соблюдением данной программы. Программа включает в себя, но не ограничивается, следующим:
- Безопасность закрытого Цифрового сертификата и политику его использования;
- Политику отзыва Цифровых сертификатов;
- Идентификацию типа Абонента (например, лицо, должность, устройство или программа) и предоставление полной и точной информации по каждому запросу Цифрового сертификата.

5.0 Полномочия

Компания «GlobalSign» может предоставлять учетные данные для доступа и/или использования служб или сертификатов Абонентов или Партнера. Лицо, получившее такой доступ, в том числе Абонент или Партнер несет ответственность за сохранение конфиденциальности и безопасности ваших учетных данных и несет полную ответственность за все действия, которые происходят с этими учетными данными.

6.0 Оплата

Если Цифровой сертификат приобретается через Партнера Компании «GlobalSign», Абонент должен уплатить Партнеру в соответствии с условиями, согласованными между Абонентом и Партнером.

Абонент признает и соглашается, что (i) если Абонент не оплачивает соответствующие платежи (например, если Абонент приобрёл Цифровой сертификат через Партнера и не оплачивает соответствующие сборы), или (ii) если Партнер не оплачивает услуги Компании «GlobalSign», то в соответствии с соглашением между Компанией «GlobalSign» и Партнером, независимо от того, оплатил

ли Абонент Партнеру, Абонент не может использовать Цифровой сертификат, Компания «GlobalSign» может отозвать неоплаченные Цифровые сертификаты.

7.0 Разрешение на публикацию информации

Абонент согласен с тем, что Компания «GlobalSign» может опубликовать серийный номер Цифрового сертификата Абонента в связи с распространением Списка отзыва Цифровых сертификатов Компании «GlobalSign» и возможных откликов протокола проверки статуса Цифрового сертификата OCSP внутри и за пределами иерархии Компании «GlobalSign».

8.0 Тестовые Цифровые сертификаты

Компания «GlobalSign» может предоставлять Цифровые сертификаты для тестирования («Тестовые Цифровые сертификаты»). Абонент может использовать Тестовые Цифровые сертификаты только во внутренней, непроизводственной среде в рамках некоммерческого тестирования.

Право на использование Тестового Цифрового сертификата может быть ограничено во времени и дополнительно ограничено в дополнительных соглашениях между Абонентом и Компанией «GlobalSign», в этом случае право Абонента на использование будет прекращено после указанной даты. Компания «GlobalSign» может по собственному усмотрению прекратить право использования любого Тестового Цифрового сертификата в любое время. Абонент обязан прекратить использование Тестового Цифрового сертификата.

Отказ от Гарантий. АБОНЕНТ ПРИЗНАЕТ, ЧТО ТЕСТОВЫЕ ЦИФРОВЫЕ СЕРТИФИКАТЫ ПРЕДОСТАВЛЯЮТСЯ "КАК ЕСТЬ" И БЕЗ КАКИХ-ЛИБО ГАРАНТИЙ. В МАКСИМАЛЬНОЙ СТЕПЕНИ, РАЗРЕШЕННОЙ ПРИМЕНИМЫМ ЗАКОНОДАТЕЛЬСТВОМ, КОМПАНИЯ «GLOBALSIGN» ПРЯМО ОТКАЗЫВАЕТСЯ ОТ ВСЕХ ЗАВЕРЕНИЙ И ГАРАНТИЙ ЛЮБОГО РОДА, ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ, ВКЛЮЧАЯ, ПОМИМО ПРОЧЕГО, ЛЮБЫЕ ГАРАНТИИ ТОВАРНОЙ ПРИГОДНОСТИ, ПРИГОДНОСТИ ДЛЯ ОПРЕДЕЛЕННОЙ ЦЕЛИ ИЛИ НЕНАРУШЕНИЯ, ОТНОСЯЩИЕСЯ К ЛЮБЫМ ТЕСТОВЫМ СЕРТИФИКАТАМ, ИСПОЛЬЗОВАНИЮ АБОНЕНТОМ ИЛИ ЛЮБОЙ НЕВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ТЕСТОВЫХ СЕРТИФИКАТОВ, РЕЗУЛЬТАТАМ ИХ ИСПОЛЬЗОВАНИЯ И НАСТОЯЩЕМУ ДОГОВОРУ.

ОГРАНИЧЕНИЕ ОТВЕТСТВЕННОСТИ. КОМПАНИЯ «GLOBALSIGN» НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ ПЕРЕД АБОНЕНТОМ ЗА ЛЮБЫЕ ПРЕТЕНЗИИ, ТРЕБОВАНИЯ ИЛИ УБЫТКИ, ВКЛЮЧАЯ БЕЗ ОГРАНИЧЕНИЯ ПРЯМЫЕ, КОСВЕННЫЕ ИЛИ ОСОБЫЕ УБЫТКИ, ВОЗНИКАЮЩИЕ В РЕЗУЛЬТАТЕ ИСПОЛЬЗОВАНИЯ ЛЮБЫХ ТЕСТОВЫХ ЦИФРОВЫХ СЕРТИФИКАТОВ И ИСПОЛЬЗОВАНИЯ ИЛИ ОТКАЗА ОТ ИСПОЛЬЗОВАНИЯ ТЕСТОВОГО ЦИФРОВОГО СЕРТИФИКАТА ПО ЛЮБОЙ ПРИЧИНЕ, НЕЗАВИСИМО ОТ ТОГО, ОСНОВАНЫ ЛИ ТАКИЕ ДЕЙСТВИЯ НА ДОГОВОРЕ ИЛИ ИНЫМ ОБРАЗОМ, ВКЛЮЧАЯ ХАЛАТНОСТЬ.

9.0 Ограниченная гарантия Компании «GlobalSign»

ЗА ИСКЛЮЧЕНИЕМ СЛУЧАЕВ, ЗАПРЕЩЕННЫХ ЗАКОНОДАТЕЛЬСТВОМ, ИЛИ ЗА ИСКЛЮЧЕНИЕМ ПОЛОЖЕНИЙ НАСТОЯЩЕГО ДОГОВОРА, В КОТОРЫХ ПРЕДУСМОТРЕНО ИНОЕ, КОМПАНИЯ «GLOBALSIGN» НЕ ПРЕДОСТАВЛЯЕТ НИКАКИХ ГАРАНТИЙ, ВКЛЮЧАЯ ГАРАНТИЮ ТОВАРНОЙ ПРИГОДНОСТИ И (ИЛИ) ГАРАНТИЮ ПРИГОДНОСТИ ДЛЯ ИСПОЛЬЗОВАНИЯ ПО НАЗНАЧЕНИЮ.

В ЧАСТИ ВЫДАЧИ КОМПАНИЕЙ «GLOBALSIGN» И УПРАВЛЕНИЯ СЕРТИФИКАТОМ В СООТВЕТСТВИИ С ОСНОВНЫМИ ТРЕБОВАНИЯМИ И ПОЛОЖЕНИЯМИ О ПРАВИЛАХ СЕРТИФИКАЦИИ, ТРЕБОВАНИЯМИ ВЫПУСКА СЕРТИФИКАТОВ С РАСШИРЕННОЙ ПРОВЕРКОЙ, ТРЕБОВАНИЯМИ ВЫПУСКА СЕРТИФИКАТОВ ПОДПИСИ КОДА КОМПАНИЯ «GLOBALSIGN» НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ ПЕРЕД АБОНЕНТОМ, ЗАВИСИМОЙ СТОРОНОЙ ИЛИ КАКОЙ-ЛИБО ТРЕТЬЕЙ СТОРОНОЙ ЗА КАКОЙ-ЛИБО УЩЕРБ ИЛИ ПОТЕРИ, ПОНЕСЕННЫЕ В РЕЗУЛЬТАТЕ ИСПОЛЬЗОВАНИЯ ИЛИ ПОЛАГАНИЯ НА ТАКОЙ ЦИФРОВОЙ СЕРТИФИКАТ. В ПРОТИВНОМ СЛУЧАЕ, ОТВЕТСТВЕННОСТЬ КОМПАНИИ «GLOBALSIGN» ПЕРЕД АБОНЕНТОМ, ЗАВИСИМОЙ СТОРОНОЙ ИЛИ ТРЕТЬИМ ЛИЦОМ ЗА ПОДОБНЫЙ УЩЕРБ ИЛИ ПОТЕРИ НИ ПРИ КАКИХ ОБСТОЯТЕЛЬСТВАХ НЕ ПРЕВЫШАЕТ ДВУХ ТЫСЯЧ ДОЛЛАРОВ США (USD 2 000) ДЛЯ СЕРТИФИКАТОВ С РАСШИРЕННОЙ ПРОВЕРКОЙ (EV) SSL И ПОДПИСИ КОДА И НЕ ПРЕВЫШАЕТ ОДНОЙ ТЫСЯЧИ ДОЛЛАРОВ США (USD 1 000) НА ОДИН ЦИФРОВОЙ СЕРТИФИКАТ ОСТАЛЬНЫХ ТИПОВ.

ЭТА ВЕРХНЯЯ ГРАНИЦА ОТВЕТСТВЕННОСТИ ОГРАНИЧИВАЕТ ОБЪЕМ ВОССТАНОВИМОГО УЩЕРБА ИЛИ ПОТЕРЬ ЗА ПРЕДЕЛАМИ КОНТЕКСТА ГАРАНТИЙНОЙ ПОЛИТИКИ КОМПАНИИ «GLOBALSIGN». НА СУММЫ, ВЫПЛАЧИВАЕМЫЕ В РАМКАХ ГАРАНТИЙНОЙ ПОЛИТИКИ, РАСПРОСТРАНЯЮТСЯ СОБСТВЕННЫЕ ВЕРХНИЕ ГРАНИЦЫ ОТВЕТСТВЕННОСТИ. НИ ПРИ КАКИХ ОБСТОЯТЕЛЬСТВАХ КОМПАНИЯ «GLOBALSIGN» НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ ЗА КАКОЙ-ЛИБО КОСВЕННЫЙ УЩЕРБ, НЕПРЕДНАМЕРЕННЫЙ УЩЕРБ, ФАКТИЧЕСКИЙ УЩЕРБ, ОПРЕДЕЛЯЕМЫЙ ОСОБЫМИ ОБСТОЯТЕЛЬСТВАМИ, ИЛИ ПОСЛЕДУЮЩИЙ УЩЕРБ, ВОЗНИКАЮЩИЙ ИЗ ИЛИ В СВЯЗИ

С ИСПОЛЬЗОВАНИЕМ, ПРЕДОСТАВЛЕНИЕМ, ПОЛАГАНИЕМ, ЛИЦЕНЗИРОВАНИЕМ, ИСПОЛНЕНИЕМ ИЛИ НЕИСПОЛНЕНИЕМ ТРАНЗАКЦИЙ С ИСПОЛЬЗОВАНИЕМ ЦИФРОВЫХ СЕРТИФИКАТОВ, ЭЛЕКТРОННЫХ ПОДПИСЕЙ, ИЛИ ПРОЧИМИ ТРАНЗАКЦИЯМИ ИЛИ УСЛУГАМИ, ПРЕДЛАГАЕМЫМИ ИЛИ ПОДРАЗУМЕВАЕМЫМИ В НАСТОЯЩЕМ АБОНЕНТСКОМ ДОГОВОРЕ.

НАСТОЯЩЕЕ ОГРАНИЧЕНИЕ ОТВЕТСТВЕННОСТИ ОСТАЕТСЯ НЕИЗМЕННЫМ НЕЗАВИСИМО ОТ КОЛИЧЕСТВА ЭЛЕКТРОННЫХ ПОДПИСЕЙ, ТРАНЗАКЦИЙ ИЛИ ПРЕТЕНЗИЙ, ОТНОСЯЩИХСЯ К ЦИФРОВОМУ СЕРТИФИКАТУ.

10.0 Срок действия и условия расторжения Договора

10.1. Настоящий Договор вступает в силу с момента его акцептирования при размещении заказа и прекращает действие в следующих случаях:

10.1.1. при невыполнении Абонентом какого-либо материального обязательства согласно настоящему Договору, если такое нарушение не устраняется в течение пяти (5) дней с момента получения уведомления об этом от Компании «GlobalSign». В данном случае Компании «GlobalSign» имеет право отозвать неоплаченные Цифровые сертификаты и заблокировать личный кабинет Абонента;

10.1.2. в одностороннем порядке Стороной при направлении письменного уведомления (в том числе по электронной почте, указанной в реквизитах Договора) в адрес другой Стороны незамедлительно в следующих случаях:

(а) существенное нарушение другой Стороной условий настоящего Договора, если подобное нарушение продолжается в течение 10 (десяти) дней после направления уведомления о невыполнении договорных обязательств;

(б) другая Сторона инициирует процесс банкротства, прекращает ведение экономической деятельности или находится в процессе ликвидации; или

(с) другая Сторона не имеет возможности исполнять существенную часть своих обязательств, установленных настоящим Договором, в результате какого-либо события (или событий), связанного с обстоятельствами непреодолимой силы, продолжающимися более 1 (одного) месяца.

(д) при введении экономических, финансовых и иных санкций в отношении Абонента;

10.1.3. при предъявлении государственными органами или учредителями Компании GlobalSign требования о приостановке и/или прекращении деятельности на территории Российской Федерации, в соответствии с Дополнительным соглашением Сторон, либо расторжение настоящего договора в течение 2 (двух) недель, либо приостановка действия настоящего Договора на срок введенных ограничений.

В указанном случае все ранее выпущенные Сертификаты продолжают свое действие в течение срока, на который они выпущены;

10.1.4. Любая Сторона вправе расторгнуть договор в одностороннем внесудебном порядке, уведомив другую сторону, за 30 календарных дней до даты расторжения.

11.0 Последствия расторжения

11.1. После расторжения настоящего Договора по какой-либо причине Компания «GlobalSign» имеет право отозвать Цифровой сертификат Абонента согласно действующим процедурам Компании «GlobalSign». После отзыва Цифрового сертификата Абонента по какой-либо причине все права, предоставленные Абоненту согласно пункту 2, аннулируются. Такое расторжение никоим образом не влияет на Разделы 4, 5, 6, 7, 8 и 11 настоящего Абонентского договора, которые будут находиться в силе и действовать до полного их выполнения.

11.2. При расторжении настоящего Договора Абонент незамедлительно выплачивает в пользу компании «GlobalSign» суммы, подлежащие уплате за период, заканчивающийся в день прекращения и/или расторжения.

12.0 Прочие положения

12.1 Регулирующее законодательство

Законы (i), которые регулируют толкование, толкование и исполнение настоящего Соглашения и всех вопросов, претензий или споров, связанных с ним, включая иски о правонарушениях, и (ii) суды, обладающие исключительной юрисдикцией в отношении любых вопросов, претензий или споры, изложены в таблице ниже.

Объект GlobalSign в сводке заказа	Применимое право	Место проведения
GMO GlobalSign K.K.	Япония	Окружной суд Токио, Япония
GlobalSign China Co., Ltd.	Китай	Шанхай, Китай
GMO GlobalSign Ltd.	Англия и Уэльс	Лондон, Англия

GlobalSign NV	Бельгия	Левен, Бельгия
GMO GlobalSign, Inc. (US)	Нью-Гэмпшир, США	Суды штата и федеральные суды Нью-Гэмпшира
GMO GlobalSign Pte. Ltd	Сингапур	Сингапур
GMO GlobalSign Inc.	Филиппины	Макати-Сити, Филиппины
GMO GlobalSign Certificate Services Pvt. Ltd	Законы Республики Индия	Дели, Индия
GMO GlobalSign Russia LLC	Законодательство Российской Федерации	Москва, Россия
GMO GlobalSign Solutions in Technology S/A	Бразилия	Белу-Оризонти, Бразилия
GMO GlobalSign FZ LLC	Объединенные Арабские Эмираты	Дубай, Объединенные Арабские Эмираты

В отношении квалификационных сертификатов eIDAS Великобритании и ЕС споры, связанные с финансовыми или коммерческими вопросами, будут разрешаться в соответствии с применимым законодательством и местом, указанным выше.

Для квалификационных сертификатов eIDAS Великобритании, для споров, связанных с сертификатами, регулирующее право и место проведения будут такими же, как указано выше для GMO GlobalSign Ltd. Для квалифицированных сертификатов eIDAS ЕС, для споров, связанных с сертификатами, регулирующее право и место рассмотрения будут такими же, как указано выше для GlobalSign NV.

12.2 Обязательный характер

Если не указано иное, настоящий Договор носит обязательный характер и распространяется на правопреемников, исполнителей, наследников, представителей и администраторов сторон настоящего Договора. Никакие права, возникающие из настоящего Договора и Цифрового сертификата Абонента, не могут быть переданными Абонентом третьей стороне. Любая умышленная передача или делегирование прав является недействительной, а также даёт Компании «GlobalSign» право расторгнуть настоящий Договор в одностороннем порядке.

12.3 Исчерпывающий характер Договора

Настоящий Договор совместно со всеми документами, на которые присутствуют ссылки в настоящем Договоре, какие-либо соглашения о предоставлении товаров или услуг, или соглашение о перепродаже (если сторона настоящего Договора является лицом, осуществляющим перепродажу), представляет собой полное соглашение между сторонами и отменяет все предыдущие устные или письменные договорённости, обязательства, соглашения о взаимопонимании, переписку, относящуюся к предмету настоящего Договора.

12.4 Раздельность положений Договора

Если одно из положений настоящего Договора или его применение станут по какой-либо причине недействительными или невыполнимыми, остальные положения настоящего Договора и их применение к другим лицам или обстоятельствам должно наилучшим способом передавать намерения сторон настоящего Договора. В ДОГОВОРЕ ПРЯМО УКАЗАНО И СОГЛАСОВАНО СТОРОНАМИ, ЧТО КАЖДОЕ ПОЛОЖЕНИЕ НАСТОЯЩЕГО ДОГОВОРА, КОТОРОЕ КАСАЕТСЯ ОГРАНИЧЕНИЯ ДЕЙСТВИЯ, ОТКАЗА ОТ ГАРАНТИЙ ИЛИ ИСКЛЮЧЕНИЯ УЩЕРБА, ЯВЛЯЕТСЯ ОТДЕЛЬНЫМ И НЕЗАВИСИМЫМ ОТ ДРУГИХ ПОЛОЖЕНИЙ И МОЖЕТ ВСТУПАТЬ В СИЛУ САМО ПО СЕБЕ.

12.5 Уведомления

Если Абонент желает или от него требуется отправление уведомления, требования или запроса в Компанию «GlobalSign» относительно настоящего Договора, любое подобное обращение составляется в письменной форме и считается отправленным надлежащим образом при отправлении курьерской службой, которая может подтвердить факт доставки в письменном виде или по почте, заказным письмом с уведомлением о вручении по адресу одного из нижеперечисленных международных филиалов Компании «GlobalSign»: <https://www.globalsign.com/en/company/contact>, с пометкой: для Юридического Отдела.

12.6 Соблюдение экспортного законодательства

Каждая сторона обязуется соблюдать все применимые федеральные, государственные и местные законы и подзаконные акты в связи со своей деятельностью по настоящему Соглашению, включая, но не

ограничиваясь, все применимые законы о санкциях, законы об импорте и экспорте, ограничения, меры контроля национальной безопасности и нормативные акты (совместно именуемые “Законы”). Абонент не будет импортировать, экспортировать, реэкспортировать или разрешать экспорт или реэкспорт какого-либо сертификата или любого другого продукта в нарушение каких-либо законов.

12.7 Обработка и хранение персональных данных, предоставленных Абонентом Компании «GlobalSign»

Компания «GlobalSign» обязуется соблюдать собственную политику конфиденциальности (размещенной в <https://www.globalsign.com/en/repository>) при получении и использовании информации от Абонента. Компания «GlobalSign» может внести изменения в политику конфиденциальности в любое время, разместив измененную политику конфиденциальности на своем веб-сайте.

Компания «GlobalSign» может проверять такие пункты как имя и фамилия физического лица, адрес и другую личную информацию, предоставленную во время подачи заявки на основе баз данных третьей стороны. Это необходимо для оказания услуги выпуска Цифрового сертификата. Вступая в настоящий Договор, Абонент соглашается на проведение таких проверок. Во время проведения таких проверок конфиденциальная информация, предоставленная Абонентом, может быть разглашена зарегистрированным агентствам кредитной информации, которые могут вести учёт такой информации. Данные проверки проводятся с целью подтверждения личности, а кредитная проверка как таковая не проводится. Эта процедура никоим образом не влияет на кредитный рейтинг Абонента.

Обработка персональных данных, включая их сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение осуществляется в соответствии с Федеральным законом Российской Федерации от 27.07.2007 №152-ФЗ.

Целью обработки персональных данных является надлежащее исполнение сторонами условий настоящего Договора. Объем подлежащих обработке персональных данных определяется Компанией «GlobalSign» с учётом необходимости идентификации лиц, обладающих полномочиями действовать в качестве Абонента или Представителя Абонента, если Абонентом является юридическое лицо, а также определения их полномочий.

В случае, если персональные данные предоставляются непосредственно субъектом персональных данных, предполагается, что дальнейшая их обработка Компанией «GlobalSign» осуществляется с целью исполнения настоящего Договора и не требует дополнительного выражения в той или иной форме согласия субъекта персональных данных, если осуществляется в соответствии с вышеуказанной целью обработки персональных данных.

В случае, если персональные данные предоставляются не субъектом персональных данных, лицо, их предоставляющее (Абонент, Представитель Абонента), гарантирует, что право предоставления персональных данных и их последующей обработки предоставлено субъектом персональных данных для заключения или исполнения настоящего Договора, либо им предоставлен доступ неограниченного круга лиц к своим персональным данным. В случае, если доступ к персональным данным не предоставлен их субъектом, Компания «GlobalSign» не несёт ответственность за последствия несанкционированной обработки персональных данных.

Лицо, предоставляющее персональные данные, несёт ответственность за их полноту и достоверность, а также, если оно не является субъектом персональных данных, за то, что предоставление персональных данных осуществляется им на законном основании.

Компания «GlobalSign» может обрабатывать, раскрывать и/или передавать эту информацию своим аффилированным лицам, агентам и субподрядчикам по мере необходимости для проверки и выдачи Сертификата, включая обработку, раскрытие и/или передачу в страны, которые могут иметь законы о защите данных, которые являются менее защитными, чем законы страны, в которой находится Абонент.

ПОДАЧА ЗАЯВКИ НА ПОЛУЧЕНИЕ ЦИФРОВОГО СЕРТИФИКАТА ПОДТВЕРЖДАЕТ ПРИНЯТИЕ ВСЕХ УСЛОВИЙ НАСТОЯЩЕГО ДОГОВОРА, В ТОМ ЧИСЛЕ УКАЗАННЫХ В НАСТОЯЩЕМ ПУНКТЕ И ПОЛИТИКЕ КОНФИДЕНЦИАЛЬНОСТИ (размещенной в <https://www.globalsign.com/en/repository>), А ТАКЖЕ ПОДТВЕРЖДАЕТ СОГЛАСИЕ НА ОБРАБОТКУ, РАСКРЫТИЕ И/ИЛИ ПЕРЕДАЧУ ПЕРСОНАЛЬНЫХ ДАННЫХ В ПОРЯДКЕ, ПРЕДУСМОТРЕННОМ В НАСТОЯЩЕМ ДОГОВОРЕ И ПОЛИТИКЕ КОНФИДЕНЦИАЛЬНОСТИ.

12.8 Торговые марки и логотипы

В целях настоящего Договора или выполнения условий настоящего Договора, Абонент и Компания

«GlobalSign» не получают никаких прав на торговую марку, фирменное название, логотип или обозначения изделий другой стороны, и не смогут использовать их для любых целей, кроме тех, на выполнение которых было получено письменное разрешение от стороны, которая владеет всеми правами на такие торговые марки, фирменные названия, логотипы или обозначения изделий.

13.0 Поддержка Клиентов

По вопросам поддержки Абонент может обращаться в Компанию «GlobalSign» через support@globalsign.com или через любой из наших международных офисов, перечисленных в списке, или на <https://www.globalsign.com/en/company/contact>.

13.1 Политика возврата денежных средств

Если Абонент не полностью удовлетворен выданным Цифровым сертификатом, если Цифровой сертификат был заказан непосредственно у GlobalSign, Абонент может запросить возврат средств в течение семи (7) дней с момента выдачи Цифрового сертификата. Любой возврат будет произведен за вычетом любых сборов, понесенных GlobalSign.

Компания GlobalSign: ООО «Джи-Эм-О Глобал Сайн Раша»

Адрес:

Российская Федерация, 119435, г. Москва, Саввинская набережная, д. 15, 6-й этаж, помещение №1

ИНН: 7723863185

КПП: 770401001

ОГРН: 1137746133370

р/с: 40702810500760003649 в Филиале Центральный, Банк ВТБ (ПАО), г. Москва

БИК: 044525411

к/с: 30101810145250000411

[Версия 5.3 1 мая 2023]