ДОГОВОР-ОФЕРТА
На оказание услуг Удостоверяющего центра

г. Москва Редакция вступает в силу с 01 июня 2019 года

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

Обществом с ограниченной ответственностью «Джи-Эм-О Глобал Сайн Раша» (далее по тексту – «Компания GlobalSign») в лице Исполнительного директора Рыжикова Дмитрия Александровича, действующего на основании Доверенности № 7 от 01.05.2018 г., 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 на нижеследующих основаниях.

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

Услуги по выпуску Цифровых сертификатов предоставляются после завершения процедуры верификации Абонента. Оплата производится в течение 30 рабочих дней с момента получения Цифрового сертификата.

В настоящий Договор публичной оферты включены следующие политики и инструкции:

- The GlobalSign Certification Practice Statement (CPS);
- The CA/B Forum Baseline Requirements;
- The GlobalSign Warranty Policy;
- The GlobalSign Payment Terms; and
- The GlobalSign Refund & Cancellation Policy

Текущая версия вышеуказанных документов находится по адресу:
https://www.globalsign.com/en/repository/.
Текущая версия требований CA/B Forum Baseline Requirements находится по адресу
https://cabforum.org/baseline-requirements-documents/.

1.0 Термины и определения

В настоящем Договоре публичной оферты используются следующие термины и определения:

Абонент	Заказчик, подавший в лице своего Представителя 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 находящиеся 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 Договора публичной оферты 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, штат, провинция, город, округ 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 разделе 10.2 основных требований Консорциума CA/Browser Forum к процессу выдачи публично-доверяемых сертификатов («**Основные требования**») по запросу выдачи Цифрового сертификата. https://cabforum.org/wp-content/uploads/BRv1.2.3.pdf
Имя домена	символьное имя, служащее для идентификации интернет-узлов в системе доменных имен (DNS).
Компания «GlobalSign»	Компания «GlobalSign», в которую Абонент подал заявку на покупку Сертификата: «GMO GlobalSign Limited», «GMO GlobalSign, Inc.», «GMO GlobalSign Pte. Ltd», «GMO GlobalSign Certificate Services Pvt. Ltd», ООО «Джи-Эм-О Глобал Сайн Раша» или GMO GlobalSign Inc. (Филиппины) .
Компрометация ключа	Закрытый ключ считается скомпрометированным, если его данные были раскрыты неавторизованному лицу, неавторизованное лицо имело к нему доступ.
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 ее 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 публичной оферты; 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 путем выписки, обобщений или аналитических выкладок из Конфиденциальной информации.
Корневой сертификат	самоподписанный Сертификат, выданный Корневым Удостоверяющим центром для собственной идентификации и верификации Сертификатов, выданных Подчиненным Удостоверяющим центрам
Лицо, запрашивающее Цифровой сертификат	представитель Заказчика, который владеет прямо оговоренными полномочиями представлять Заказчика или третью сторону (например, в качестве поставщика услуг в сети Интернет или хостинговой компании), который заполняет и подает Заявки на получение Цифрового сертификата от имени Заказчика. Лица, запрашивающие Цифровой сертификат, могут быть предварительно утверждены посредством таких Управляемых услуг как MSSL или ePKI.
Лицо, утверждающее Цифровой сертификат	представитель Заказчика, который владеет прямо оговоренными полномочиями представлять Заказчика (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.

Подозрительный код	код, который является функционально вредоносным или серьезно 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 путем, не соответствующим замыслу его проектировщиков, компрометируя достоверность платформ, на которых они выполняются.
Подчиненные УЦ	центры сертификации, чьи Цифровые сертификаты подписаны корневым удостоверяющим центром, или другими подчиненными УЦ.
Полностью определённое имя домена («FQDN»)	доменное имя, которое включает пометки всех вышестоящих узлов в системе доменных имен 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 Заказчика	физическое лицо, которое является агентом Заказчика, действующее согласно прямо оговоренных полномочий, предоставленных ему Заказчиком.
Протокол проверки статуса Цифрового сертификата OCSP	межсетевой протокол (IP) (типа "запрос-ответ") используется для получения статуса отзыва Цифрового сертификата в режиме реального времени от доверенного субъекта («**OCSP-респондера»**).
Регистрант доменного имени	иногда упоминается как «владелец» доменного имени, но более правильно, человек (люди) или юридическое лицо (лица), зарегистрированные в реестре доменных имен как имеющие право контролировать использование доменного имени. Ими могут быть физические или юридические лица, которые числятся как «Регистранты» по данным WHOIS или регистра доменных имен.
Регистратор доменных имен	лицо или организация, регистрирующие доменные имена под эгидой или по согласованию с: (I) Интернет-корпорацией по присвоению имен и номеров (ICANN), (II) с национальными органами/ реестрами доменных имен, или (III) справочно-информационными центрами сети Интернет (в том числе их Аффилиатами, 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 имен («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, блок, или юридическое лицо, идентифицированные в Цифровом сертификате в качестве субъекта. Субъектом является либо Абонент, либо устройство, управляемое и эксплуатируемое Абонентом.
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 публичной оферты.
Управляемая услуга MSSL	Облачная служба, которая реализует метод управления SSL-сертификатами по запросу. Система мгновенно выдает 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 заявитель / абонент является Аффилиатом ЦС.
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 произведенным преобразованиям. Данные, подписанные цифровыми подписями, имеют отношение к электронным данным с прилагаемыми цифровыми подписями.
Цифровой сертификат	электронные данные, в которые входит Открытый ключ, идентифицирующий информацию о его владельце, и информацию о сроке действия с Электронной подписью от имени Компании «GlobalSign».
OCSP-респондер	Имеет значение, установленное в определении термина Протокол проверки статуса Цифрового сертификата OCSP.
Wildcard сертификат	Цифровой сертификат, содержащий звездочку (*) в крайнем левом положении любого из полностью уточненных доменных имен субъекта, содержащихся в сертификате.
Microsoft	компания Microsoft Corporation, юридическое лицо, зарегистрированное в соответствии с законодательством штата Вашингтон, США, с адресом местонахождения One Microsoft Way, Redmond, WA 98052.

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 (с «Начала срока действия» до «Действителен до»), Компания «GlobalSign» предоставляет Абоненту полномочия использовать запрошенный им Цифровой сертификат для выполнения операций с Закрытым и (или) Открытым ключом. Обязательства Абонента, изложенные в разделе 4.0 относительно защиты Закрытого ключа, применяются с Даты вступления в силу.

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 публичной оферты 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 Цифрового 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 доступными в электронном виде для всех Сертификатов, подписанных и выданных Удостоверяющим центром Компании «GlobalSign»:

1. Списки отзыва Цифровых сертификатов (CRL) для каждого сертификата, с указанием точки распространения сертификата CRL;
2. Респондеры Протокола проверки статуса Цифрового сертификата (OCSP) для любого Цифрового сертификата с респондером Протокола проверки статуса Цифрового сертификата (OCSP), и
3. 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 публичной оферты 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. Отзыв Цифрового сертификата Абонента производится

Компанией «GlobalSign» в течение двадцати четырех (24) часов при следующих обстоятельствах:

1. Абонент в письменном виде направляет запрос в Компанию «GlobalSign» о желании Абонента отозвать Цифровой сертификат;
2. Абонент указывает, что оригинальная Заявка на получение Цифрового сертификата не санкционирована и не может быть санкционирована задним числом;
3. Компания «GlobalSign» получает свидетельства Компрометации закрытого ключа Абонента, соответствующего Открытому ключу;
4. Компания «GlobalSign» получает свидетельства того, что проверка авторизации доменного имени или управление Полностью квалифицированного доменного имени или IP-адреса не являются надежными.

Отзыв Цифрового сертификата Абонента должен быть выполнен Компанией «GlobalSign» в течение двадцати четырех (24) часов и должен быть выполнен в течение 5 (пяти) дней при следующих обстоятельствах:

1. Сертификат более не соответствует требованиям типа алгоритма и размера ключа согласно основным требованиям Консорциума CA/Browser Forum;
2. Компании «GlobalSign» получает доказательства неправильного использования сертификата;
3. Компания «GlobalSign» получает информацию о том, что Абонент нарушает какое-либо обязательство согласно настоящему договору публичной оферты или Условиям использования;
4. Компании «GlobalSign» становится известно о каких-либо обстоятельствах, указывающих на то,

что использование Полностью квалифицированного доменного имени или IP-адреса в Цифровом сертификате более не разрешено законом (например, в случае лишения судом права Регистранта доменного имени на использование Доменного имени, расторжения соответствующего лицензионного соглашения или соглашение о предоставлении услуг между Регистрантом доменного имени и Заявителем или Регистрант доменного имени не восстановил Доменное имя);

5. Компания «GlobalSign» получает информацию о том, что Цифровой сертификат «Wildcard» используется для аутентификации мошеннического подчиненного Полностью квалифицированного доменного имени;
6. Компании «GlobalSign» становится известно о существенных изменениях информации, которая содержится в Цифровом сертификате;
7. Компания «GlobalSign» получает информацию о том, что Цифровой сертификат выдан не в соответствии с Основными требованиями, с требованиями Правил сертификации Компании «GlobalSign» (CP) или настоящими Положениями о правилах сертификации (CPS) ;
8. Компания «GlobalSign» приходит к заключению о том, что какая-либо информация, которая содержится в Цифровом сертификате, является неверной или вводит в заблуждение;
9. Компания «GlobalSign» прекращает обслуживание по любой из указанных причин и не принимает мер для того, чтобы другой Удостоверяющий центр обеспечивал поддержку отзыва Цифрового сертификата;
10. Истекает, отзывается или прекращается право Компании «GlobalSign» на выдачу Цифровых сертификатов в соответствии с Основными требованиями, за исключением случаев, когда Компания «GlobalSign» принимает меры для того, чтобы продолжить ведение репозитория Списка отзыва Цифровых сертификатов (CRL) / Протокола проверки статуса Цифрового сертификата (OCSP);
11. Отзыв Цифрового сертификата требуется в соответствии с Правилами сертификации Компании «GlobalSign» (CP) и/или в соответствии с Положениями о правилах сертификации (CPS);
12. Техническое содержание формата Цифрового сертификата представляет собой неприемлемый риск для Поставщиков прикладного программного обеспечения или Зависимых сторон (например, Консорциум CA/Browser Forum может посчитать, что устаревший криптографический алгоритм, алгоритм подписи или размер ключа могут представлять неприемлемый риск, и что такие Цифровые сертификаты должны быть отозваны и заменены Удостоверяющим центром в течение указанного периода времени);
13. Компании «GlobalSign» становится известно о продемонстрированном или проверенном методе, который компрометирует Закрытый ключ Абонента, о разработанных методах, которые могут легко вычислить его на основе открытого ключа (например, слабый ключ Debian, см. http://wiki.debian.org/SSLkeys), или если есть явные доказательства того, что конкретный метод, используемый для создания закрытого ключа, был ошибочным;
14. Компания «GlobalSign» получает информацию о том, что Цифровой сертификат был использован для подписи вредоносного программного обеспечения.

Отзыв Цифрового сертификата Абонента может производиться Компанией «GlobalSign» в течение коммерчески разумного периода времени при следующих обстоятельствах:

1. Абонент или администратор организации запрашивает отзыв Цифрового сертификата через учетную запись Центра сертификации Компании «GlobalSign» (GCC), который контролирует жизненный цикл Цифрового сертификата;
2. Абонент запрашивает отзыв через аутентифицированный запрос в службу поддержки Компании «GlobalSign» или Орган регистрации Компании «GlobalSign»;
3. Компания «GlobalSign» получает информацию о том, что Абонент добавлен в « черный список» в качестве заблокированной стороны или нежелательного лица, или проводит операцию с запрещенного места согласно юрисдикции Компании «GlobalSign»;
4. Компания «GlobalSign» по собственному усмотрению определяет, что дальнейшее использование Цифрового сертификата может скомпрометировать безопасность, репутацию или доверие к Удостоверяющему центру Компании «GlobalSign» или к Компании «GlobalSign»;
5. Компания «GlobalSign» получила запрос на отмену Цифрового сертификата;
6. Если сертификат был перевыпущен, то Компания «GlobalSign» может отозвать предыдущий сертификат;
7. Компания «GlobalSign» имеет право отозвать Цифровые сертификаты в случае, если лицензионное соглашение было расторгнуто или истекло;

8. Компания «GlobalSign» определяет, что дальнейшее использование Цифрового сертификата наносит ущерб бизнесу Компании «GlobalSign» или третьих лиц. При рассмотрении вопроса о том, может ли использование Цифрового сертификата нанести ущерб бизнесу или репутации Компании «GlobalSign» или третьей стороны, Компания «GlobalSign» принимает во внимание, кроме прочего следующее: происхождение и количество полученных жалоб; идентификацию заявителя(ей); применимое действующее законодательство; ответ на возможное неправомерное использование со стороны Абонента;
9. Если компания Microsoft определит, что Цифровой сертификат подписи кода содержит ложную информацию о названии организации, либо используется для вредоносного программного обеспечения, то компания Microsoft имеет право связаться с Компанией «GlobalSign» и запросить отзыв Цифрового сертификата. Компания «GlobalSign» либо отзывает Цифровой сертификат, либо запрашивает исключение запроса в течение 2 (двух) рабочих дней с момента получения запроса. Компания Microsoft может либо удовлетворить, либо отклонить исключение по своему усмотрению. В случае, если компания Microsoft не утвердит исключение, то Компания «GlobalSign» отзывает Цифровой сертификат не позднее чем через 2 (два) рабочих дня;
10. Если компания Microsoft определит, что Цифровой сертификат SSL или Цифровой сертификат подписи кода используется для распространения вредоносного программного обеспечения, то компания Microsoft имеет право связаться с Компанией «GlobalSign» и запросить отзыв Цифрового сертификата. Компания «GlobalSign» либо отзывает Цифровой сертификат, либо запрашивает исключение запроса в течение 2 (двух) рабочих дней с момента получения запроса. Компания Microsoft может либо удовлетворить, либо отклонить исключение по своему усмотрению. В случае, если компания Microsoft не утвердит исключение, то Компания «GlobalSign» отзывает Цифровой сертификат не позднее чем через 2 (два) рабочих дня;
11. Компания «GlobalSign» отзывает Цифровой сертификат в случае смерти Абонента.

3.3 Генерирование ключа.

Если Пары ключей генерируются Компанией «GlobalSign» от имени Абонента и предлагаются токены, PKCS#12 или AutoCSR, Компания «GlobalSign» использует надежные системы для генерирования таких Пар ключей, при этом применяются следующие условия. Компания «GlobalSign» не генерирует Пары ключей для публично доверенных сертификатов SSL.

- 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 расширенной проверки, Абонент предупрежден о том, что Компания «GlobalSign» не будет выпускать ключи длиною менее чем 2048 бит, и для Цифрового сертификата подписи кода с расширенной проверкой будет предлагать только алгоритм шифрования SHA2.

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 Цифровой 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 производить временную маркировку кода, подписанного Цифровым сертификатом подписи кода, в качестве безвозмездной услуги при

рациональном её использовании. Следуя передовой практике, Компания «GlobalSign» рекомендует устанавливать метку времени при подписи программного кода. 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 к PDF-документам Цифрового сертификата Adobe CDS

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

3.7 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 нее дополнительную плату, если количество операций отметки времени превышает установленный лимит.

4.0 Обязанности и гарантии Абонента

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

4.1 Точность данных.

Абонент 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 с расширенной проверкой.

4.2 Защита Закрытого ключа.

Заявитель принимает все разумные меры для того чтобы в единоличном порядке осуществлять контроль, обеспечивать конфиденциальность, постоянно защищать Закрытый ключ, включаемый в запрашиваемый Цифровой сертификат (Цифровые сертификаты), любые связанные с ним данные активации или устройства, например, пароль или токен. Для Цифровых сертификатов подписи кода Абонент обязан предоставлять надлежащие сетевые и другие средства защиты, чтобы предотвратить ненадлежащее использование закрытого ключа, а Компания «Globalsign» может отменить сертификат без предварительного уведомления при наличии несанкционированного доступа к закрытым ключам.

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 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.

4.6 Использование Цифрового сертификата Компании «GlobalSign».

Абонент обязуется устанавливать Цифровой сертификат только на серверах, которые соответствует данному Цифровому сертификату, использовать Цифровой сертификат Компании «GlobalSign» в строгом соответствии действующему законодательству и строго соблюдая условия настоящему договору публичной оферты или Условиям 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, создает неудобства или раздражает получателя, напр., Программное обеспечение, которое включает нежелательные функционал, не раскрытый должным образом пользователю до начала установки, или признается нежелательным/подозрительным коммерческими антивирусными приложениями

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 определенный документ

4.6.2 Цифрового сертификата 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, приведенным в Руководстве по выдаче и управлению Цифровыми сертификатами подписи кода с расширенной проверкой;
- Использовать в строгом соответствии с действующим законодательством;
- Использовать исключительно для разрешенных видов деятельности компании;
- Использовать в строгом соответствии с настоящим договором публичной оферты.

Если Абоненту становится известно (любыми способами) о том, что подписан код, содержащий вредоносное программное обеспечение или серьезную 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 Отчетность и отзыв.
Абонент обязуется прекратить использование Цифрового сертификата и связанного с ним Закрытого ключа и немедленно подать запрос в Компанию «GlobalSign» на отзыв Цифрового сертификата, если (a) информация, содержащаяся в Цифровом сертификате, становится неточной или неправильной; или (b) имеется факт или подозрение в некорректном использовании или компрометации Закрытого ключа, связанного Открытым ключом Цифрового сертификата; или (c) в случае Цифрового сертификата подписи кода имеются доказательства использования Цифрового сертификата для подписи Подозрительного кода.

4.8 Прекращение использования Цифрового сертификата.
Абонент должен немедленно прекратить использование Закрытого ключа, связанного с Открытым ключом Цифрового сертификата, при отзыве Цифрового сертификата;

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 публичной оферты 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 расширенной проверки совместно с услугами и программным обеспечением Microsoft, Абонент также уведомлен, 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 (a) Цифровой сертификат или Абонент определены как источник Подозрительного кода, или (b) полномочия на запрос Цифрового сертификата не могут быть проверенными, или (c) Цифровой сертификат отозван не по запросу заявителя (напр., в результате Компрометации ключа, обнаружения вредоносного ПО и т.д.), то Удостоверяющий центр уполномочен 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 публичной оферты, если это необходимо для соблюдения любых изменений Минимальных требований к выдаче и управлению публично-доверяемыми сертификатами подписи кода («Основные требования»), опубликованных по адресу https://aka.ms/csbr

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 имен (SubjectAltNames), указанными 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 «Отчетность и отзыв» ниже.

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 в Компанию «GlobalSign» согласно обязательствам, указанным в пункте «Отчетность и отзыв» ниже.

4.15 Генерирование и использование ключей
Если Пары ключей генерируются Абонентом или Лицом, запрашивающим Цифровой сертификат, следует использовать надежные системы для генерирования Пар ключей, при этом применяются следующие условия:

1. Пары ключей должны генерироваться при помощи подходящей для этой цели платформы. В случае подписи документов в формате «PDF» для Adobe CDS, AATL подписи документов и защиты почты и подписи кода с расширенной проверкой следует использовать платформу, совместимую со стандартом FIPS 140-2, 2-го уровня,
2. Следует использовать ключ с подходящей для Цифровой подписи длиной и алгоритмом,
3. 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):

a. Абонент управляет процессами, включая, но не ограничиваясь, изменением данных активации, которые обеспечивают использование любого Закрытого ключа в аппаратных модулях системы безопасности (HSM) или токенах, только Хранителем Цифрового сертификата, обладающим необходимой квалификацией и знаниями,
b. Абонент гарантирует прохождение Хранителем Цифрового сертификата должного обучения мерам безопасности в целях, для которых был выдан Цифровой сертификат, и
c. 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 аппаратный модуль системы безопасности,

Для Цифровых сертификатов подписи кода Абонент должен использовать один из следующих способов для создания и защиты закрытых ключей. Globalsign рекомендует Абоненту использовать метод 1 или 2:

i. 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

ii. Аппаратный криптомодуль, сертифицированный как соответствующий по крайней мере FIPS 140 Level 2, общим критериям EAL 4+ или эквивалентный

iii. Еще 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+).

Для Цифровых сертификатов подписи кода с расширенной проверкой Абонент должен использовать один из следующих способов для создания и защиты закрытых ключей:

y. Аппаратный криптомодуль, сертифицированный как соответствующий FIPS 140-2 Level 2 или выше.
z. Токен с форм-фактором устройства USB-токена FIPS 140-2 Level 2 или выше.

В любое время в течение применения и жизненного цикла Цифрового сертификата Абонент должен иметь возможность, по запросу Компании «GlobalSign», представить доказательство того, что пара ключей, связанная с сертификатом (запросом), хранится на криптографическом устройстве, отвечающем требованиям FIPS 140-2 Level 2 (или эквивалента). Непредставление 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.

Для Квалифицированных сертификатов ключи должны быть сгенерированы и сохранены квалифицированным устройством для создания подписей (QSCD), которое отвечает требованиям, изложенным в приложении II Регламента №910/2014 Европейского парламента и Совета Европейского союза. Абонент соглашается использовать сертификат только в рамках QSCD, который был предоставлен или утвержден в письменной форме GlobalSign, и 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, приведенных в Стандарте деловой практики в оптовом электроэнергетическом секторе WEQ012 («Стандарты WEQ PKI» - https://www.naesb.org//weq/weq_standards.asp):

Абоненты, подпадающие под действие Стандартов «WEQ PKI», должны быть зарегистрированы в Реестре идентификации пользователей Североамериканского совета по энергетическим стандартами 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, определенной 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 определенную 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; и
- 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 надежного 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, АСА 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:

1. Защищать собственные закрытые ключи от доступа посторонних лиц;
2. Идентифицировать посредством Реестра идентификации пользователей NAESB EIR определенного пользователя, который выбрал Компанию «GlobalSign» в качестве авторизованного удостоверяющего центра;
3. Выполнять все договоренности и договоры, заключенные с Компанией «GlobalSign» согласно отчетам о сертификации Компании «GlobalSign», которые необходимы Компании «GlobalSign» для выдачи Цифровых сертификатов Конечным пользователям с целью обеспечения безопасности электронной связи;
4. 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:

5. Безопасность закрытого Цифрового сертификата и политику его использования;
6. Политику отзыва Цифровых сертификатов;
7. Идентификацию типа Абонента (например, лицо, должность, устройство или программа) и предоставление полной и точной информации по каждому запросу Цифрового сертификата.

5.0 Разрешение на публикацию информации

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

6.0 Ограниченная гарантия Компании «GlobalSign»

ЗА ИСКЛЮЧЕНИЕМ СЛУЧАЕВ, ЗАПРЕЩЕННЫХ ЗАКОНОДАТЕЛЬСТВОМ, ИЛИ ЗА ИСКЛЮЧЕНИЕМ ПОЛОЖЕНИЙ НАСТОЯЩЕГО ДОГОВОРА ПУБЛИЧНОЙ ОФЕРТЫ, 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 КОМПАНИИ «GLOBALSIGN», 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 ОДНОЙ ТЫСЯЧИ ДОЛЛАРОВ США (USD 1 000) НА ОДИН ЦИФРОВОЙ СЕРТИФИКАТ, ПРИ УСЛОВИИ, ЧТО ОГРАНИЧЕНИЕ СОСТАВЛЯЕТ ДВЕ ТЫСЯЧИ ДОЛЛАРОВ США (USD 2 000) НА ОДИН ЦИФРОВОЙ СЕРТИФИКАТ ДЛЯ ЦИФРОВЫХ СЕРТИФИКАТОВ С РАСШИРЕННОЙ ПРОВЕРКОЙ ИЛИ ДЛЯ ЦИФРОВЫХ СЕРТИФИКАТОВ ПОДПИСИ КОДА С РАСШИРЕННОЙ ПРОВЕРКОЙ.

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 ПУБЛИЧНОЙ ОФЕРТЫ.

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

7.0 Срок действия и условия расторжения Договора публичной оферты

Настоящий Договор публичной оферты прекращает действие при более раннем наступлении одного из следующих событий:

- Окончание срока действия Цифрового сертификата, выданного Абоненту напрямую, опосредованно или с использованием служб MSSL или EPKI, которые все еще действительны;

- Невыполнение Абонентом какого-либо материального обязательства согласно настоящему договору публичной оферты , если такое нарушение не устраняется в течение пяти (5) дней с момента получения уведомления об этом от Компании «GlobalSign».

8.0 Последствия расторжения

После расторжения настоящего договора публичной оферты 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, 8 и 9 настоящего договора публичной оферты, которые будут находиться в силе и действовать до полного их выполнения.

9.0 Прочие положения

9.1 Регулирующее законодательство

Если одной из сторон Договора публичной оферты является компания ООО «Джи-Эм-О Глобал Сайн Раша», то настоящий Договор публичной оферты регулируется и толкуется согласно законодательству Российской Федерации, невзирая на принципы коллизионного права. Местом рассмотрения споров являются суды Российской Федерации.

Если одной из сторон Договора публичной оферты является компания «GMO GlobalSign Limited», то настоящий Договор публичной оферты регулируется и толкуется согласно законодательству Англии и Уэльса, невзирая на принципы коллизионного права. Местом рассмотрения споров являются суды Англии.

Если одной из сторон Договора публичной оферты является компания «GMO GlobalSign, Inc.», то настоящий Договор публичной оферты регулируется и толкуется согласно законодательству штата Нью-Хэмпшир, США, невзирая на принципы коллизионного права. Местом рассмотрения споров являются суды штата Нью-Хэмпшир.

Если одной из сторон Договора публичной оферты является компания «GMO GlobalSign Pte. Ltd.», то настоящий Договор регулируется и толкуется согласно законодательству Сингапура, невзирая на принципы коллизионного права. Местом рассмотрения споров являются суды Сингапура.

Если одной из сторон Договора публичной оферты является Компания «GMO GlobalSign Certificate Services Pvt. Ltd», настоящий Договор публичной оферты регулируется и толкуется согласно законодательству Индии и сопутствующих законов Штата, невзирая на принципы коллизионного права. Местом рассмотрения споров являются суды Индии.

Если одной из сторон Договора публичной оферты является компания «GMO GlobalSign Philippines (GSPH)», то настоящий Договор публичной оферты регулируется и толкуется согласно законодательству Республики Филиппины, невзирая на принципы коллизионного права. Местом рассмотрения споров являются суды г. Макати, Республика Филиппины.

9.2 Обязательный характер

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

9.3 Исчерпывающий характер Договора публичной оферты

Настоящий договор публичной оферты совместно со всеми документами, на которые присутствуют

ссылки в настоящем договоре публичной оферты, какие-либо соглашения о предоставлении товаров или услуг, или соглашение о перепродаже (если сторона настоящего Договора публичной оферты является лицом, осуществляющим перепродажу), представляет собой полное соглашение между сторонами и отменяет все предыдущие устные или письменные договоренности, обязательства, соглашения о взаимопонимании, переписку, относящуюся к предмету настоящего Абонентского договора.

Согласно настоящему Договору публичной оферты Компания «Microsoft» в явном порядке указывается в качестве стороннего получателя Цифровых сертификатов подписи кода и Цифровых сертификатов подписи кода с расширенной проверкой.
Абонент признает, что Microsoft может самостоятельно определить, что подписанный Цифровым сертификатом программный код является вредоносным, опасным или может внести изменения в работу программного обеспечения или услуг Microsoft, компания «Microsoft» может отозвать такой Цифровой сертификат без предварительного уведомления.

9.4 Раздельность положений Договора публичной оферты

Если одно из положений настоящего Договора публичной оферты или его применение станут по какой-либо причине недействительными или невыполнимыми, остальные положения настоящего Договора публичной оферты и их применение к другим лицам или обстоятельствам должно наилучшим способом передавать намерения сторон настоящего Договора публичной оферты. В ДОГОВОРЕ ПУБЛИЧНОЙ ОФЕРТЫ 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.

9.5 Уведомления

Если Абонент желает или от него требуется отправление уведомления, требования или запроса в Компанию «GlobalSign» относительно настоящего Договора публичной оферты, 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/company/contact.htm, с пометкой: Юридический Отдел. Такая переписка вступает в силу с момента получения.

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

В случае физических лиц, Компания «GlobalSign» может проверять такие пункты как имя и фамилия, адрес и другую личную информацию, предоставленную во время подачи заявки на основе баз данных третьей стороны. Вступая в настоящий Договор публичной оферты, 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 учет 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.

Если со стороны Компании «GlobalSign» Договор публичной оферты заключен ООО «Джи-Эм-О Глобал Сайн Раша», 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 действующим законодательством Российской Федерации.

Целью обработки персональных данных является надлежащее исполнение сторонами условий настоящего Договора публичной оферты. Объем подлежащих обработке персональных данных определяется Компанией «GlobalSign» с учетом 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 публичной оферты 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 публичной оферты, 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 несет ответственность за последствия несанкционированной обработки персональных данных.

Лицо, предоставляющее персональные данные, несет 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.

9.7 Торговые марки и логотипы

В целях настоящего Договора или выполнения условий настоящего Договора публичной оферты , 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.

10.0 Поддержка Клиентов

В случае ошибки в Цифровом сертификате, Абонент обязуется немедленно оповестить об этом Компанию «GlobalSign», сообщив об этом в один из нижеперечисленных международных офисов http://www.globalsign.com/company/contact.htm. Если Абонент не сообщает об этом в течение семи (7) дней после получения, Цифровой сертификат считается принятым.

Компания «GlobalSign» обязуется компенсировать средства согласно Политике компенсации Компании «GlobalSign», опубликованной по ссылке: http://www.globalsign.com/repository/

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

Адрес:
Российская Федерация, 115114, г. Москва, Шлюзовая набережная, д. 8, стр. 1, 4-ый этаж, офис 401

ИНН: 7723863185
КПП: 770501001
ОГРН: 1137746133370
р/с: 40702810500760003649 в Филиале Центральный, Банк ВТБ (ПАО), г. Москва
БИК: 044525411
к/с: 30101810145250000411