Положение о сертификационной практике GlobalSign

(CPS – Certification Practice Statement)

Дата: 15 ноября 2023

Версия: 10.2

Английская версия настоящего Положения о сертификационной практики GlobalSign (CPS – Certification Practice Statement) является основной версией. В случае любого конфликта или несоответствия между английской CPS и любой локализованной или переведенной версией положения английской версии имеют преимущественную силу.

Содержание

История изменений документа

Версия	Дата публикации	Статус и описание
10.0	28 марта 2023	• Обновлено название сертификатов "PSD2" на "Open Banking". • Обновления бюллетеней CSC-13 и CSC-17 CA/B Форума. • Пересмотр OID • Удалено требование о цифровой подписи этого документа для выпуска. • Уточнена «уникальность темы» • Включение OP (РЦ) в качестве роли в процесс уведомления и отзыва. • Просмотр журналов аудита и архивных разделов записей • Обзор раздела по защите закрытых ключей и разработке криптографических модулей. • Уточнены ограничения на отзыв краткосрочных сертификатов. • Грамматические обновления, согласованность текста
10.1	21 августа 2023	Обновления базовых требований для S/MIME Обновления базовых требований для TLS (v2.0.0) Обновления причин отзыва и изменения статуса Проверка регистрационных органов и регистрационных органов предприятий Обзор заверений и гарантий Уточнены ограничения на отзыв краткосрочных сертификатов. Грамматические обновления, языковая последовательность
10.2	15 ноября 2023	Пересмотр периодов использования ключей Обновлен раздел приостановки сертификата.

Подтверждения

1.0 Введение

Настоящее Положение о сертификационной практике GlobalSign (CPS) применяется к продуктам и услугам компании GlobalSign NV/SA и аффилированных организаций ("GlobalSign"). В первую очередь это относится к выпуску и управлению жизненным циклом сертификатов, включая услуги по проверке. GlobalSign может также предоставлять дополнительные услуги, такие как простановка меток времени. CPS может периодически обновляться, как указано в разделе 1.5 «Управление политикой». Последнюю версию можно найти в репозитории GlobalSign по адресу https://www.globalsign.com/repository. (*Для удобства могут быть доступны версии на других языках. Но в случае каких-либо несоответствий преимущественную силу имеет версия на английском языке*).

CPS выделяет «процедуры, в соответствии с которыми цифровой сертификат выдается определенному сообществу и/или классу приложений с общими требованиями безопасности». В отношении содержания, оформления и формата CPS соответствует формальным требованиям рекомендаций RFC 3647, выпущенных Инженерной группой Интернета (IETF) в ноябре 2003 года (RFC 3647 заменяет RFC 2527). Рекомендации RFC от IETF — авторитетный источник стандартных практик в области электронных подписей и управления сертификатами. Названия некоторых разделов, которые не относятся к услугам GlobalSign, включены в данное CPS в соответствии со структурой RFC 3647. В этих разделах указано «Не предусмотрено». В случае необходимости дополнительная информация представлена в подразделах стандартной структуры. Выполнение требований RFC 3647 к формату улучшает и облегчает взаимодействие и сравнений условий с другими УЦ и заранее предоставляет Проверяющим сторонам необходимую информацию о практике и процедурах GlobalSign.

Данное CPS направлено на соблюдение следующих требований:

- Программы корневых сертификатов в браузерах
- RFC3647, Инфраструктура открытых ключей Интернета X.509: политика сертификации и основы практики сертификации, Чохани и др., ноябрь 2003 г.
  Требования Североамериканского совета по энергетическим стандартам (NAESB) по аккредитации для уполномоченных центров сертификации
- Принципы и критерии WebTrust для центров сертификации
- Принципы и критерии WebTrust для центров сертификации — базовый уровень SSL с сетевой безопасностью
- Принципы и критерии WebTrust для центров сертификации — расширенная проверка SSL
- Принципы и критерии WebTrust для центров сертификации — базовые требования к подписи кода
- Принципы и критерии WebTrust для центров сертификации – S/MIME
- Регламент №910/2014 Европейского парламента и Совета от 23 июля 2014 г. о сервисах электронной идентификации и доверия для электронных транзакций на внутреннем рынке и отмене Директивы 1999/93/EC
- Положения о сервисах электронной идентификации и доверия для электронных транзакций (поправки и др.) (выход из ЕС) 2019 года
- Положения о сервисах электронной идентификации и доверия для электронных транзакций 2016 года (2016 No.696)

GlobalSign соответствует текущим версиям требований:

- Базовые требования CA/Browser Forum к выпуску и управлению публично доверенными сертификатами («Базовые требования», BR для TLS)
- Руководство CA/Browser Forum по выпуску и управлению сертификатами с расширенной проверкой («Руководство EV»)
- Требования CA/Browser Forum к безопасности сети и системы сертификатов
- Базовые требования CA/Browser Forum к подписи кода («Базовые требования к подписи кода»)

- Базовые требования CA/Browser Forum для выдачи и управления общедоступными сертификатами S/MIME («Базовые требования для S/MIME») [1]

Все указанные документы опубликованы на http://www.cabforum.org. При наличии каких-либо противоречий между перечисленными требованиями и данным документом, документы CA/Browser Forum имеют приоритет.

В данном CPS рассматриваются технические, процедурные и кадровые политики и практики компании GlobalSign в течение всего жизненного цикла сертификатов, выпущенных GlobalSign. Также здесь рассматриваются требования к удостоверяющим центрам (УЦ), выпускающим сертификаты различных типов. Привязка к конкретному корневому УЦ может варьироваться в зависимости от выбора конкретного промежуточного и перекрестного сертификатов, используемых или предоставляемых платформой или клиентом.

CPS применим к абоненту и/или доверяющей стороне, которые используют, полагаются или пытаются полагаться на сертификационные услуги, предоставляемые удостоверяющим центром, ссылающимся на данный CPS.

Для абонентов данное CPS вступает в силу и становится обязательным при принятии Абонентского договора или Условий использования. Для доверяющих сторон данное CPS становится обязательным, если они полагаются на сертификат, выданный в соответствии с этим CPS. Кроме того, абоненты обязаны в соответствии с Абонентским договором информировать доверяющие стороны, что CPS для них обязателен к исполнению.

Версия CPS на английском языке является основной. В случае каких-либо противоречий или несоответствий между английской и любой локализованной или переведенной версией, преимущественную силу имеют положения английской версии.

1.1 Обзор

Данное CPS относится ко всей иерархии сертификатов, выпускаемых компанией GlobalSign. Цель документа — представить практику и процедуры GlobalSign по управлению сертификатами, а также соответствие собственным и отраслевым требованиям по выпуску сертификатов согласно стандартам, изложенным выше. Кроме того, Регламент eIDAS (Regulation (EU)N910/2014) ("eIDAS"), eIDAS (Великобритания) и Положения об электронной идентификации и доверительных услугах для электронных транзакций 2016 года ("UK eIDAS") признают электронные подписи для аутентификации, а также безотзывности и ответственности за содержание документов. В связи с этим GlobalSign предоставляет услуги в рамках применимых статей Закона. Доверенные услуги в Великобритании управляются и предоставляются через GMO GlobalSign LTD., аффилированное лицо GlobalSign.

Данное CPS описывает услуги GlobalSign по сертификации и управлению жизненным циклом сертификатов любого подчиненного УЦ, сертификатов клиентов, серверов и других конечных организаций.

В настоящем CPS рассматриваются следующие типы сертификатов:

PersonalSign 1	Персональный сертификат низкой надежности
PersonalSign 2	Персональный сертификат средней надежности
PersonalSign 2 Pro	Персональный сертификат средней надежности со ссылкой на профессиональную информацию
PersonalSign 2 Pro DepartmentSign	Машина, устройство, отдел или должность сертификата средней надежности со ссылкой на профессиональную информацию

[1] Действуют с 1 сентября 2023 г.

PersonalSign 3 Pro	Персональный сертификат аутентификации высокой надежности со ссылкой на профессиональную информацию
Партнеры PersonalSign	Частный удостоверяющий центр, созданный как якорь доверия, выпускающий сертификаты PersonalSign 2 Pro или PersonalSign 2 Pro DepartmentSign
IntranetSSL	Сертификат аутентификации веб-серверов, не привязанный к публичному доверенному корню GlobalSign
DomainSSL	Сертификат для аутентификации веб-серверов
AlphaSSL	Сертификат для аутентификации веб-серверов
OrganizationSSL	Сертификат для аутентификации веб-серверов
SSL расширенной проверки (EV)[2]	Сертификат для аутентификации веб-серверов
Метки времени GlobalSign	Сертификат для аутентификации источников времени
AATL	Сертификат средней аппаратной надежности для использования с документами Adobe AATL и Microsoft Office
Подпись кода[3]	Сертификат для аутентификации объектов данных
Подпись кода с расширенной проверкой[1]	Сертификат для аутентификации объектов данных
Уполномоченные сертификаты УЦ Североамериканского совета по энергетическим стандартам (NAESB)	Персональный, ролевой, серверный сертификат или сертификат устройства рудиментарного, базового либо среднего уровня заверения со ссылкой на профессиональную информацию, авторизованный уполномоченным УЦ
Hosted Root (хостированный корень)	Услуга, при которой GlobalSign поддерживает корневой ключ и сертификат от имени организации, не являющейся членом GlobalSign, и параллельно предоставляет перекрестный сертификат до тех пор, пока корень не будет встроен в корневые хранилища. В течение этого периода организация, не являющаяся владельцем GlobalSign, обеспечивает аудит WebTrust от своего имени.
Квалифицированные сертификаты для электронных подписей	eIDAS/UK eIDAS-совместимые квалифицированные сертификаты, используемые для обеспечения электронных подписей
Квалифицированные сертификаты для электронных печатей	eIDAS/UK eIDAS-совместимые квалифицированные сертификаты, используемые для обеспечения электронных печатей
Квалифицированные сертификаты веб-аутентификации	eIDAS/UK eIDAS квалифицированные сертификаты для веб-аутентификации (SSL)
Сертификаты для квалифицированной временной метки	Сертификаты, используемые для подписания квалифицированных временных меток, соответствующих требованиям eIDAS
S/MIME	Сертификат для подписи, проверки, шифрования и расшифровки электронной почты.

Примечание. По состоянию на 1 сентября 2023 г. все выданные сертификаты S/MIME (в рамках «Базовых требований для S/MIME») должны быть сертификатами S/MIME BR.

Сертификаты GlobalSign:

- Могут использоваться для электронных подписей для замены рукописных подписей по выбору сторон сделки.

---

[2] Эти сертификаты выпускаются и управляются в соответствии с Руководством EV и Базовыми требованиями для подписи кода. Остальные типы сертификатов должны выпускаться и управляться в соответствии с Базовыми требованиями, если на это указывает включение OID политики CA/Browser Forum, как описано в разделе 1.2 ниже.

[3] Эти сертификаты выпускаются и управляются в соответствии с Базовыми требованиями к подписи кода.

- Могут использоваться для аутентификации веб-ресурсов, таких как серверы и другие устройства.
- Могут использоваться для цифровой подписи кода, документов и других объектов данных.
- Могут использоваться для шифрования данных.

В данном CPS определены должности, обязанности и практики всех организаций, участвующих в жизненном цикле, использовании и управлении сертификатами GlobalSign. Положения данного CPS распространяются на практику, уровень услуг, обязанности и ответственность всех участвующих сторон, включая GlobalSign, GlobalSign РЦ, абонентов и доверяющих сторон. Некоторые положения могут также применяться к другим организациям, таким как поставщики сертификационных услуг, поставщики приложений и др.

Политика сертификатов GlobalSign (CP) дополняет это CPS. Ее цель — указать, *«что должно соблюдаться»*, и, следовательно, установить рамки операционных правил для широкого спектра продуктов и услуг GlobalSign.

В данном CPS говорится о том, *«как Центр сертификации придерживается Политики сертификатов»*. При этом данное CPS отличается лучшей детализацией и предоставляет конечному пользователю обзор процессов, процедур и условий, которые GlobalSign использует при создании и обслуживании сертификатов, которыми управляет. В дополнение к CP и CPS, GlobalSign поддерживает дополнительные документированные политики по таким вопросам:

- Непрерывность бизнеса и аварийное восстановление
- Политика безопасности
- Кадровая политика
- Политика управления ключами
- Процедуры регистрации

Другие релевантные документы:

- Гарантийная политика GlobalSign, в которой рассматриваются вопросы гарантий, предоставляемых GlobalSign.
- Политика конфиденциальности GlobalSign по защите персональных данных.
- Политика сертификатов GlobalSign, в которой рассматриваются цели доверия для корневых сертификатов GlobalSign.

Абонент или доверяющая сторона для УЦ, выдающего сертификаты GlobalSign, должны руководствоваться данным CPS для установления доверия сертификату, выданному GlobalSign, а также для получения информации о практике GlobalSign. Также необходимо установить достоверность всей цепочки сертификатов иерархии, включая сертификат корневого УЦ и все рабочие сертификаты. Достоверность цепочки можно установить на основе утверждений в данном CPS. Для квалифицированных сертификатов проверка цепочки сертификатов должна быть успешно проведена до якоря доверия GlobalSign в соответствующем списке доверия eIDAS ЕС или Великобритании.

Все действующие политики GlobalSign подлежат аудиту уполномоченными третьими сторонами, о чем GlobalSign сообщает на своем общедоступном веб-сайте с помощью печати WebTrust Seal of Assurance. Дополнительная информация может быть предоставлена по запросу.

1.1.1 Именование сертификатов

Вот сертификаты корневого УЦ GlobalSign, которые регулируются данным CPS:

Публичные корневые сертификаты УЦ GlobalSign

- GlobalSign Root CA – R1 с отпечатком EBD41040E4BB3EC742C9E381D31EF2A41A48B6685C96E7CEF3C1DF6CD4331C99
- GlobalSign Root CA – R3 с отпечатком CBB522D7B7F127AD6A0113865BDF1CD4102E7D0759AF635A7CF4720DC963C53B
- GlobalSign Root CA – R5 с отпечатком 179FBC148A3DD00FD24EA13458CC43BFA7F59C8182D783A513F6EBEC100C8924
- GlobalSign Root CA – R6 с отпечатком 2CABEAFE37D06CA22ABA7391C0033D25982952C453647349763A3AB5AD6CCF69
- GlobalSign Root CA – R46 с отпечатком 4FA3126D8D3A11D1C4855A4F807CBAD6CF919D3A5A88B03BEA2C6372D93C40C9
- GlobalSign Root CA – E46 с отпечатком CBB9C44D84B8043E1050EA31A69F514955D7BFD2E2C6B49301019AD61D9F5058

GlobalSign активно содействует включению вышеуказанных корневых сертификатов в аппаратные и программные платформы, способные поддерживать сертификаты и связанные с ними криптографические услуги. По возможности, GlobalSign стремится заключать договоры с поставщиками платформ для эффективного управления жизненным циклом корневых сертификатов. При этом GlobalSign активно поощряет поставщиков платформ по их собственному усмотрению включать корневые сертификаты GlobalSign CA без договорных обязательств. GlobalSign Root CA R2 и GlobalSign Root CA R4 больше не принадлежат компании GlobalSign.

Публичные не-TLS корневые сертификаты УЦ GlobalSign

- GlobalSign Client Authentication Root R45 с отпечатком 165C7E810BD37C1D57CE9849ACCD500E5CB01EEA37DC550DB07E598AAD2474A8
- GlobalSign Client Authentication Root E45 с отпечатком 8B0F0FAA2C00FE0532A8A54E7BC5FD139C1922C4F10F0B16E10FB8BE1A634964
- GlobalSign Code Signing Root R45 с отпечатком 7B9D553E1C92CB6E8803E137F4F287D4363757F5D44B37D52F9FCA22FB97DF86
- GlobalSign Code Signing Root E45 с отпечатком 26C6C5FD4928FD57A8A4C5724FDD279745869C60C338E262FFE901C31BD1DB2B
- GlobalSign Document Signing Root R45 с отпечатком 38BE6C7EEB4547D82B9287F243AF32A9DEEB5DC5C9A87A0056F938D91B456A5A
- GlobalSign Document Signing Root E45 с отпечатком F86973BDD0514735E10C1190D0345BF89C77E1C4ADBD3F65963B803FD3C9E1FF
- GlobalSign Secure Mail Root R45 с отпечатком 319AF0A7729E6F89269C131EA6A3A16FCD86389FDCAB3C47A4A675C161A3F974
- GlobalSign Secure Mail Root E45 с отпечатком 5CBF6FB81FD417EA4128CD6F8172A3C9402094F74AB2ED3A06B4405D04F30B19
- GlobalSign Timestamping Root R45 с отпечатком 2BCBBFD66282C680491C8CD7735FDBBAB7A8079B127BEC60C535976834399AF7
- GlobalSign Timestamping Root E46 с отпечатком 4774674B94B78F5CCBEF89FDDEBDABBD894A71B55576B8CC5E6876BA3EAB4538
- GlobalSign IoT Root R60 с отпечатком 36E80B78775DDA9D0BAC964AC29D5A5EC4F3684E0C74445E954A191C2939B8E0
- GlobalSign IoT Root E60 с отпечатком 43ED443C1F0CD46C9914B4272C24DC42CF6FE62B4AAB37585878A26D882AE4CB

Приведенные выше корневые сертификаты являются публичными, проверенными WebTrust сертификатами, которые настроены для использования без TLS, чтобы соответствовать функциональности различных продуктов GlobalSign. GlobalSign активно содействует включению вышеуказанных корневых сертификатов в аппаратные и программные платформы, способные поддерживать сертификаты и связанные с ними криптографические услуги. По возможности, GlobalSign стремится заключать договоры с поставщиками платформ для эффективного управления жизненным циклом корневых сертификатов. При этом GlobalSign активно поощряет поставщиков платформ по их собственному усмотрению включать корневые сертификаты GlobalSign CA без договорных обязательств.

Непубличные корневые сертификаты УЦ GlobalSign

- GlobalSign Non-Public Root CA – R1 с отпечатком 8D2EEFC79397F86BD4DB5B16A84144156D7EE352B57DE36B2C4FC738081DF9C9
- GlobalSign Non-Public Root CA – R2 с отпечатком 24FD17248F3B76F82AF2FD9C57D60F3EF60551508EE98DC460FD3A67866ECCEA
- GlobalSign Non-Public Root CA – R3 с отпечатком A3BB9A2462E728818A6D30548BD3950B8C8DAE1B63FC89FE66E10BB7BAB5725A
- GlobalSign Non-Public Root R43 with fingerprint D6273949002299CC84DA84984EAF3F20F4B09CC2A7B241DFD4B361A8432460EB
- GlobalSign Trusted Platform Module Root CA с отпечатком F27BF02C6E00C73D915EEB6A6A2F5FBF0C31AE0393149E6B5C31E41B113841C3
- GlobalSign Trusted Platform Module ECC Root CA с отпечатком 5A8C7B5EB888CFCE9322068E80E82B28B554FFEB7FDC9638DCB3763077401D26

1.1.1.1 Публичное раскрытие сертификатов подчиненных УЦ, выдающих сертификаты

Корневые программы браузеров требуют публичного раскрытия всех подчиненных УЦ, не имеющих технических ограничений (ограничения на имя и ограничения на использование расширенных ключей). Все «активные» сертификаты подчиненных УЦ, которые напрямую или транзитивно связаны с любым сертификатом публичного корня, перечислены в Общей базе данных УЦ (CCADB). Не отозванные сертификаты УЦ, вышедшие из эксплуатации, сообщаются на полугодовой основе корневым программам с помощью сообщений об уязвимостях или электронных писем, как того требует соответствующая корневая программа. Об отозванных сертификатах подчиненных УЦ также сообщается таким же образом либо вскоре после отзыва, если это обычная процедура, либо сразу после, если это требуется с точки зрения безопасности.

Сертификаты позволяют субъектам, участвующим в электронной транзакции, подтверждать свою личность перед другими участниками или подписывать данные в цифровой форме. Сертификат GlobalSign подтверждает связь между названным субъектом (Абонентом) и его открытым ключом. Процесс получения сертификата включает идентификацию, присвоение имени, аутентификацию и регистрацию Абонента, а также аспекты управления сертификатом, такие как выдача, отзыв и истечение срока действия сертификата. В процессе выдачи сертификата GlobalSign обеспечивает подтверждение личности субъекта сертификата путем привязки открытого ключа, который использует Абонент. GlobalSign предоставляет сертификаты, которые можно использовать для подтверждения безотзывности, ответственности за содержание, шифрования и аутентификации. Использование этих сертификатов может быть дополнительно ограничено конкретным деловым или договорным контекстом или уровнем транзакций в поддержку гарантийной политики или других ограничений, налагаемых приложениями, в которых используются сертификаты.

1.2 Название и идентификация документа

Данный документ представляет собой Положение о сертификационной практике GlobalSign.

Идентификатор OID для GlobalSign NV/SA (GlobalSign) представляет собой: iso (1) идентифицированная-организация (3) dod (6) интернет (1) частное (4) предприятие (1) GlobalSign (4146).

GlobalSign следующим образом организует свои дуги OID для различных сертификатов и документов, описанных в данном CPS:

Категория	OID	Описание

TLS	**1.3.6.1.4.1.4146.10.1**	**Дуга политик TLS**
	1.3.6.1.4.1.4146.10.1.1	Политика TLS расширенной проверки
	1.3.6.1.4.1.4146.10.1.2	Политика TLS проверки организации
	1.3.6.1.4.1.4146.10.1.3	Политика TLS проверки домена
Аутентификация	**1.3.6.1.4.1.4146.10.2**	**Дуга политик аутентификации**
	1.3.6.1.4.1.4146.10.2.1	Политика аутентификации расширенной проверки
	1.3.6.1.4.1.4146.10.2.2	Политика аутентификации проверки организации
	1.3.6.1.4.1.4146.10.2.3	Политика аутентификации проверки домена
	1.3.6.1.4.1.4146.10.2.4	Политика аутентификации при проверке личности
S/MIME	**1.3.6.1.4.1.4146.10.3**	**Дуга политик S/MIME**
	1.3.6.1.4.1.4146.10.3.1	Политика S/MIME проверки организации
	1.3.6.1.4.1.4146.10.3.2	Политика S/MIME спонсорской проверки
	1.3.6.1.4.1.4146.10.3.3	Политика S/MIME проверки почтовых ящиков
	1.3.6.1.4.1.4146.10.3.4	Политика S/MIME индивидуальной проверки
	1.3.6.1.4.1.4146.1.40.70	Политика клиентских сертификатов (защита электронной почты)
Подпись кода	**1.3.6.1.4.1.4146.10.4**	**Дуга политик подписи кода**
	1.3.6.1.4.1.4146.10.4.1	Политика подписи кода с расширенной проверкой
	1.3.6.1.4.1.4146.10.4.2	Политика подписи кода с проверкой организации
Подпись документов	**1.3.6.1.4.1.4146.10.5**	**Дуга политик подписи документов**

Категория	OID	Описание	Закрытый ключ
Квалифицированная	**1.3.6.1.4.1.4146.1.40.36**	**Квалифицированные eIDAS сертификаты – QSCD**	
	1.3.6.1.4.1.4146.1.40.36.1	Квалифицированные сертификаты для электронных подписей	Закрытый ключ на QSCD Управляется Абонентом
	1.3.6.1.4.1.4146.1.40.36.2	Квалифицированные сертификаты для электронных печатей	Закрытый ключ на QSCD Управляется Абонентом
	1.3.6.1.4.1.4146.1.40.37	Квалифицированные сертификаты eIDAS — не QSCD	
	1.3.6.1.4.1.4146.1.40.37.1	Квалифицированные сертификаты для электронных подписей	Закрытый ключ отсутствует на QSCD. Управляется Абонентом
	1.3.6.1.4.1.4146.1.40.37.2	Квалифицированные сертификаты для электронных печатей	Закрытый ключ отсутствует на QSCD. Управляется Абонентом
	1.3.6.1.4.1.4146.1.40.37.3	Квалифицированные сертификаты для электронных печатей - Open Banking	Закрытый ключ отсутствует на QSCD. Управляется Абонентом
	1.3.6.1.4.1.4146.1.40.38	**Квалифицированные eIDAS сертификаты – Удаленный QSCD**	
	1.3.6.1.4.1.4146.1.40.38.1	Квалифицированные сертификаты для электронных подписей	Закрытый ключ на QSCD Управляется от имени Абонента
	1.3.6.1.4.1.4146.1.40.38.2	Квалифицированные сертификаты для электронных печатей	Закрытый ключ на QSCD Управляется от имени Абонента
	1.3.6.1.4.1.4146.1.40.39	Квалифицированные сертификаты для аутентификации	
	1.3.6.1.4.1.4146.1.40.39.1	Квалифицированные сертификаты для аутентификации (физические лица)	
	1.3.6.1.4.1.4146.1.40.39.2	Квалифицированные сертификаты для аутентификации (юридические лица)	
	1.3.6.1.4.1.4146.1.40.39.3	Квалифицированные сертификаты для проверки подлинности веб-сайта (QWAC)	
	1.3.6.1.4.1.4146.1.40.39.4	Квалифицированные сертификаты для аутентификации веб-сайта (QWAC) — Open Banking	
	1.3.6.1.4.1.4146.1.40.41	**Квалифицированные eIDAS сертификаты – Удаленный не QSCD**	

1.3.6.1.4.1.4146.1.40.41.1	Квалифицированные сертификаты для электронных подписей	Закрытый ключ на QSCD Управляется от имени Абонента
1.3.6.1.4.1.4146.1.40.41.2	Квалифицированные сертификаты для электронных печатей	Закрытый ключ на QSCD Управляется от имени Абонента

Категория	**OID**	**Описание**	**Закрытый ключ**
	1.3.6.1.4.1.4146.1.44.36	**Квалифицированные eIDAS сертификаты UK – QSCD**	
	1.3.6.1.4.1.4146.1.44.36.1	Квалифицированные сертификаты для электронных подписей	Закрытый ключ на QSCD Управляется Абонентом
	1.3.6.1.4.1.4146.1.44.36.2	Квалифицированные сертификаты для электронных печатей	Закрытый ключ на QSCD Управляется Абонентом
	1.3.6.1.4.1.4146.1.44.37	**Квалифицированные eIDAS сертификаты UK – Не QSCD**	
	1.3.6.1.4.1.4146.1.44.37.1	Квалифицированные сертификаты для электронных подписей	Закрытый ключ на QSCD Управляется Абонентом
	1.3.6.1.4.1.4146.1.44.37.2	Квалифицированные сертификаты для электронных печатей	Закрытый ключ на QSCD Управляется Абонентом
	1.3.6.1.4.1.4146.1.44.37.3	Квалифицированные сертификаты для электронных печатей - Open Banking	Закрытый ключ отсутствует на QSCD. Управляется Абонентом
	1.3.6.1.4.1.4146.1.44.38	**Квалифицированные eIDAS сертификаты UK – Удаленный QSCD**	
	1.3.6.1.4.1.4146.1.44.38.1	Квалифицированные сертификаты для электронных подписей	Закрытый ключ на QSCD Управляется от имени Абонента
	1.3.6.1.4.1.4146.1.44.38.2	Квалифицированные сертификаты для электронных печатей	Закрытый ключ на QSCD Управляется от имени Абонента
	1.3.6.1.4.1.4146.1.44.39	Квалифицированные сертификаты UK для аутентификации	
	1.3.6.1.4.1.4146.1.44.39.1	Квалифицированные сертификаты для аутентификации (физические лица)	

1.3.6.1.4.1.4146.1.44.39.2	Квалифицированные сертификаты для аутентификации (юридические лица)	
1.3.6.1.4.1.4146.1.44.40	Квалифицированные сертификаты UK eIDAS для аутентификации веб-сайтов (QWAC)	
1.3.6.1.4.1.4146.1.44.40.1	Квалифицированные сертификаты для проверки подлинности веб-сайта (QWAC)	
1.3.6.1.4.1.4146.1.44.40.2	Квалифицированные сертификаты для аутентификации веб-сайта (QWAC) — Open Banking	
1.3.6.1.4.1.4146.1.44.41	**Квалифицированные eIDAS сертификаты UK – Удаленный не QSCD**	
1.3.6.1.4.1.4146.1.44.41.1	Квалифицированные сертификаты для электронных подписей	Закрытый ключ на QSCD Управляется от имени Абонента
1.3.6.1.4.1.4146.1.4.41.2	Квалифицированные сертификаты для электронных печатей	Закрытый ключ на QSCD Управляется от имени Абонента

Категория	OID	Описание
Удостоверяющие центры	1.3.6.1.4.1.4146.1.45.1	Локальный УЦ для квалифицированных сертификатов
	1.3.6.1.4.1.4146.1.45.2	Внешний УЦ для квалифицированных сертификатов
Метки времени	1.3.6.1.4.1.4146.1.30	Политика сертификатов меток времени
	1.3.6.1.4.1.4146.1.31	Политика сертификатов меток времени – AATL
	1.3.6.1.4.1.4146.1.32	Политика сертификатов меток времени – сертификаты для квалифицрованных меток времени (QTS) в соответствии с регламентом eIDAS
	1.3.6.1.4.1.4146.1.33	Политика сертификатов меток времени – сертификаты для квалифицрованных меток времени (QTS) в соответствии с регламентом UK eIDAS
	1.3.6.1.4.1.4146.1.34	Политика сертификатов меток времени на хостинге
	1.3.6.1.4.1.4146.1.35	Политика сертификатов меток времени на хостинге – AATL
	1.3.6.1.4.1.4146.2	Политика, согласно которой службы меток времени под управлением GlobalSign включают ответы с метками времени IETF RFC 3161
	1.3.6.1.4.1.4146.2.2	Политика меток времени, охватывающая токены меток времени (TST), выпущенные в соответствии с IETF RFC 3161 по алгоритму Secure Hash Algorithm v1 (SHA1)
	1.3.6.1.4.1.4146.2.3	Политика меток времени, охватывающая токены меток времени (TST), выпущенные в соответствии с IETF RFC 3161 по алгоритму Secure Hash Algorithm v2 (SHA2)
	1.3.6.1.4.1.4146.2.3.1	Политика меток времени, охватывающая токены меток времени (TST), выпущенные в соответствии с IETF RFC 3161 по алгоритму Secure Hash Algorithm v1 (SHA1) с иерархией удостоверяющих центров R6
	1.3.6.1.4.1.4146.2.3.1.1	Политика меток времени, охватывающая токены меток времени (TST), выпущенные в соответствии с IETF RFC 3161 по алгоритму Secure Hash Algorithm v2 (SHA2) с иерархией удостоверяющих центров R6
	1.3.6.1.4.1.4146.2.3.1.2	Политика меток времени для подписи кода CodeSign, охватывающая токены меток времени (TST), выпущенные в соответствии с IETF RFC 3161 по алгоритму Secure Hash Algorithm v2 (SHA2) с иерархией удостоверяющих центров R6
	1.3.6.1.4.1.4146.2.4	Политика, по которой службы меток времени GlobalSign включают ответы с метками времени IETF RFC 3161 исключительно для служб расширенной проверки подписи кода
	1.3.6.1.4.1.4146.2.6	Токены меток времени, аккредитованные в Японии – AATL
	1.3.6.1.4.1.4146.2.7	Токены меток времени, аккредитованные в Японии – не AATL
Политики по другим сертификатам	1.3.6.1.4.1.4146.1.40	Политика сертификатов не общего использования (Non-Generic)
	1.3.6.1.4.1.4146.1.40.20	Политика выпускающего УЦ в Японской сети центров сертификации (JCAN)
	1.3.6.1.4.1.4146.1.40.30	Политика в отношении сертификатов GlobalSign AATL

	1.3.6.1.4.1.4146.1.40.30.2	Политика в отношении сертификатов GlobalSign AATL (класс 2)
	1.3.6.1.4.1.4146.1.80	Политика клиентских сертификатов электронного обмена данными в розничной торговле
	1.3.6.1.4.1.4146.1.81	Политика серверных сертификатов электронного обмена данными в розничной торговле
	1.3.6.1.4.1.4146.1.90	Политика TPM доверенного корня
	1.3.6.1.4.1.4146.1.95	Политика протокола для онлайн-статуса сертификата
	1.3.6.1.4.1.4146.3	Документы GlobalSign, такие как Политика сертификатов (CP) и Положение о сертификационной практике (CPS)
	1.3.6.1.4.1.4146.4	Расширения сертификата, специфичные для GlobalSign, Интернет вещей (IoT)
	1.3.6.1.4.1.4146.5	Политики GlobalSign по оценке времени
	1.3.6.1.4.1.4146.5.1	Политика службы оценки времени, аккредитованной GlobalSign в Японии
Цепочки УЦ и перекрестная подпись	1.3.6.1.4.1.4146.1.60	Политика по цепочкам УЦ – Доверенный корень и Хостированный корень
	1.3.6.1.4.1.4146.1.60.1	Политика по цепочкам УЦ – Хостированный корень (совместима с базовыми требованиями)
Частная иерархия	1.3.6.1.4.1.4146.11.1	Дуга политики сертификатов частной иерархии
	1.3.6.1.4.1.4146.11.1.1	Дуга общих клиентских сертификатов
	1.3.6.1.4.1.4146.11.1.1.1	IntranetSSL
	1.3.6.1.4.1.4146.11.1.1.2	IntranetS/MIME
	1.3.6.1.4.1.4146.11.1.1.3	Политика демонстрационных сертификатов – Не следует доверять, поскольку может содержать неточную информацию. Используется для тестирования и интеграции
	1.3.6.1.4.1.4146.11.1.2	Внутренние сертификаты GlobalSign
	1.3.6.1.4.1.4146.11.1.3	Фирменные сертификаты клиента

Устаревшие OID

Следующие OID отмечены как устаревшие. Где это применимо, они заменяются новой иерархией, указанной в таблице выше.

Категория	OID	Описание
TLS	1.3.6.1.4.1.4146.1.1	Политика сертификатов расширенной проверки – SSL – Устаревш.
	1.3.6.1.4.1.4146.1.1.1	Квалифицированные сертификаты в соответствии с регламентом eIDAS – Квалифицированные сертификаты веб-аутентификации (QWAC) – Устаревш.
	1.3.6.1.4.1.4146.1.1.2	Квалифицированные сертификаты в соответствии с регламентом eIDAS – Квалифицированные сертификаты веб-аутентификации (QWAC) – Open Banking – Устаревш.
	1.3.6.1.4.1.4146.1.2	Политика сертификатов расширенной проверки – Подпись кода – Устаревш.
	1.3.6.1.4.1.4146.1.10	Политика сертификатов проверки домена – Устаревш.
	1.3.6.1.4.1.4146.1.10.10	Политика сертификатов проверки домена – AlphaSSL – Устаревш.
	1.3.6.1.4.1.4146.1.20	Политика сертификатов проверки организации – Устаревш.
	1.3.6.1.4.1.4146.1.25	Политика сертификатов проверки IntranetSSL – Устаревш.
Квалифицированные	1.3.6.1.4.1.4146.1.40.35	Квалифицированные сертификаты eIDAS (общие) – Устаревш.
	1.3.6.1.4.1.4146.1.40.35.1	Квалифицированные сертификаты для электронных печатей (юридические лица с QSCD) – под управлением Абонента – Устаревш.
	1.3.6.1.4.1.4146.1.40.35.1.1	Квалифицированные сертификаты для электронных печатей (юридические лица) – Open Banking – Устаревш.
	1.3.6.1.4.1.4146.1.40.35.2	Квалифицированные сертификаты для электронных подписей (физические лица с QSCD) – под управлением Абонента – Устаревш.
	1.3.6.1.4.1.4146.40.40.1	Квалифицированные сертификаты для аутентификации веб-сайта (QWAC) — Устаревш.
	1.3.6.1.4.1.4146.40.40.2	Квалифицированные сертификаты для аутентификации веб-сайта (QWAC) — Open Banking — Устаревш.
Подпись кода	1.3.6.1.4.1.4146.1.50	Политика сертификатов подписи кода (сертификаты от GlobalSign с содержанием 1.3.6.1.4.1.4146.1.50 выдаются и управляются в соответствие с Базовыми требованиями к подписи кода)
Аутентификация	1.3.6.1.4.1.4146.1.40.60	Политика клиентских сертификатов (клиентская аутентификация)
Клиентские сертификаты	1.3.6.1.4.1.4146.1.40.10	Политика клиентских сертификатов (EPKI – Enterprise PKI – Устаревш.)
	1.3.6.1.4.1.4146.1.40.40	Политика клиентских сертификатов (EPKI для частных УЦ – Устаревш.)
	1.3.6.1.4.1.4146.1.40.50	Политика клиентских сертификатов (Частная иерархия – AEG – Устаревш.)
Другие	1.3.6.1.4.1.4146.1.26	Политика демонстрационных сертификатов – Не следует доверять, поскольку может содержать неточную информацию. Используется для тестирования и интеграции. (Устаревш.)

	1.3.6.1.4.1.4146.1.70	Политика высокопроизводительного УЦ
	1.3.6.1.4.1.4146.1.100	Политика сертификатов устройств Интернета вещей (устаревш.)

Общественные OID

Сертификаты, соответствующие требованиям определённой организации или сообщества, включают один из дополнительных идентификаторов, перечисленных ниже.

Организация	OID	Описание
CA/Browser Forum	2.23.140.1.1	Политика сертификатов расширенной проверки
	2.23.140.1.2.1	Политика сертификатов проверки домена
	2.23.140.1.2.2	Политика сертификатов проверки организации
	2.23.140.1.3	Политика сертификатов подписи кода EV
	2.23.140.1.4.1	Политика минимальных требований к сертификатам подписи кода
	2.23.140.1.4.2	Политика минимальных требований к временным меткам подписи кода
	2.23.140.1.5.1.1	Политика устаревших сертификатов с проверкой почтового ящика S/MIME
	2.23.140.1.5.1.2	Политика многоцелевого сертификата с проверкой почтового ящика S/MIME
	2.23.140.1.5.1.3	Строгая политика сертификатов, проверенная почтовым ящиком S/MIME
	2.23.140.1.5.2.1	Политика устаревших сертификатов, проверенная организацией S/MIME
	2.23.140.1.5.2.2	Политика многоцелевого сертификата, проверенная организацией S/MIME
	2.23.140.1.5.2.3	Строгая политика сертификатов, подтвержденная организацией S/MIME
	2.23.140.1.5.3.1	Политика устаревших сертификатов, подтвержденная спонсором S/MIME
	2.23.140.1.5.3.2	Политика многоцелевого сертификата, проверенная спонсором S/MIME
	2.23.140.1.5.3.3	Строгая политика сертификатов, подтвержденная спонсором S/MIME
	2.23.140.1.5.4.1	Политика устаревших сертификатов S/MIME с индивидуальной проверкой
	2.23.140.1.5.4.2	Политика многоцелевого сертификата S/MIME с индивидуальной проверкой
	2.23.140.1.5.4.3	Строгая политика сертификатов S/MIME с индивидуальной проверкой
ETSI	0.4.0.194112.1.0	QCP-n: политика сертификатов для квалифицированных сертификатов ЕС, выданных физическим лицам
	0.4.0.194112.1.1	QCP-l: политика сертификатов для квалифицированных сертификатов ЕС, выданных юридическим лицам
	0.4.0.194112.1.2	QCP-n-qscd: политика сертификатов для квалифицированных сертификатов ЕС, выданных физическим лицам с закрытым ключом, связанным с сертифицированным открытым ключом в QSCD
	0.4.0.194112.1.3	QCP-l-qscd: политика сертификатов для квалифицированных сертификатов ЕС, выданных юридическим лицам с закрытым ключом, связанным с сертифицированным открытым ключом в QSCD

	0.4.0.194112.1.4	QCP-w: сертификат для квалифицированного сертификата веб-сайта ЕС, выданного физическому или юридическому лицу и связывающего веб-сайт с этим лицом
NAESB	2.16.840.1.114505.1.12.1.2	Рудиментарные гарантии NAESB
	2.16.840.1.114505.1.12.2.2	Базовые гарантии NAESB
	2.16.840.1.114505.1.12.3.2	Средние

1.3 Участники PKI

1.3.1 Удостоверяющие центры

GlobalSign — это удостоверяющий центр, выдающий сертификаты в соответствии с данным CPS. В качестве удостоверяющего центра GlobalSign выполняет функции, связанные с управлением жизненным циклом сертификата, такие как регистрация Абонентов, выпуск, продление срока действия, распространение и отзыв сертификата. GlobalSign также предоставляет информацию о статусе сертификата через репозиторий в виде точки распространения Списка Отзыва Сертификатов (COC) и/или ответчика по протоколу Online Certificate Status Protocol (OCSP). Удостоверяющий центр (УЦ) также может быть описан терминами *«Центр Сертификации»* (ЦС) или "GlobalSign" для обозначения цели выпуска сертификатов по запросу Регистрационного Центра (РЦ), подчиненного УЦ.

Данное CPS относится ко всем сертификатам в иерархии GlobalSign. За поддержку документа отвечает орган GlobalSign PACOM1 – CA Governance Policy Authority, состоящий из членов руководства GlobalSign и назначенный его Советом директоров. Через этот орган компания GlobalSign осуществляет конечный контроль над жизненным циклом и управлением корневого УЦ GlobalSign и всех нижестоящих УЦ, входящих в иерархию.

GlobalSign также является Центром сертификации времени (TSA) и обеспечивает доказательство существования данных в определенный момент времени. При необходимости GlobalSign может передать на аутсорсинг определенные услуги TSA, чтобы обеспечить дополнительную независимую проверку функций, связанных со временем.

По мере появления новых сервисов или их необходимости в конкретных приложениях GlobalSign обеспечивает доступность всех сервисов, относящихся к управлению сертификатами в рамках корней GlobalSign, включая, без ограничений, выдачу, аннулирование и проверку статуса сертификатов. GlobalSign также управляет основной системой онлайн-регистрации и программными интерфейсами для всех типов сертификатов, выпущенных подчиненными УЦ.

Некоторые задачи, связанные с жизненным циклом сертификата, делегированы отдельным РЦ, которые действуют на основе соглашения об обслуживании с GlobalSign.

1.3.2 Регистрационные центры

GlobalSign осуществляет делегирование в соответствии с разделом 1.3.2 GlobalSign CP.

GlobalSign может выступать в качестве регистрационного центра для выпускаемых им сертификатов. В этом случае GlobalSign несет ответственность за:

- Принятие, оценку, утверждение или отклонение регистрации заявок на сертификаты.
- Регистрацию Абонентов на услуги сертификации.
- Предоставление систем для облегчения идентификации Абонентов (в соответствии с типом запрашиваемого сертификата).

- Использование нотариально заверенных или иным образом уполномоченных документов или источников информации для оценки и подтверждения подлинности заявки от заявителя.
- Запросы на выдачу сертификатов через процесс многофакторной аутентификации после утверждения заявки.
- Инициирование процесса отзыва сертификата у соответствующего подчиненного УЦ или партнерского подчиненного УЦ.

Помимо идентификации и проверки подлинности заявителей на получение сертификатов, регистрационный центр (РЦ) может также инициировать или передавать запросы на аннулирование сертификатов и запросы на обновление и перевыпуск ключей для сертификатов.

РЦ могут применять более строгие методы проверки, если этого требует их внутренняя политика.

GlobalSign также может делегировать выполнение всех или любой части требований Раздела 3.2 Уполномоченной третьей стороне, за исключением следующих разделов, при условии, что процесс в целом соответствует всем требованиям Раздела 3.2:

Тип сертификата	**Секция**
TLS и EV TLS	3.2.7 (Аутентификация доменных имен) и 3.2.8 (Аутентификация IP-адресов)
S/MIME	3.2.9 (Аутентификация адресов электронной почты)

Прежде чем GlobalSign уполномочит делегированную третью сторону выполнять делегированную функцию, GlobalSign по контракту потребует от делегированной третьей стороны:
1. Отвечать квалификационным требованиям раздела 5.3.1, если это применимо к делегируемой функции;
2. Сохранять документацию в соответствии с разделом 5.5.2;
3. Соблюдать другие положения применимых требований CA/Browser Forum, применимых к делегированной функции; и
4. Соблюдать (а) CP и/или CPS УЦ или (б) практическое заявление Делегированной третьей стороны, соответствие которого, по данным УЦ, требованиям форума CA/Browser Forum и другим применимым требованиям.
В случае РЦ EPKI (Enterprise PKI) и MSSL (Managed SSL) сертификаты ограничены предварительно определенной и проверенной конфигурацией GlobalSign.

Для выпуска определенных типов сертификатов РЦ может полагаться на сертификаты, выданные сторонними УЦ или другими сторонними базами данных и источниками информации, такими как государственные паспорта, eID и водительские права. Если РЦ полагается на сертификаты, выданные сторонним УЦ, то должен изучить практику проверки третьей стороны и обязательства полагающейся стороны, обратившись к его CPS.

1.3.2.1 Органы регистрации предприятий

GlobalSign может назначить Enterprise РЦ для проверки запросов сертификатов от собственной организации Enterprise РЦ, и в этом случае организация Абонента проверяется, предварительно определяется и ограничивается конфигурацией системы.

GlobalSign может разрешить использование Enterprise РЦ при условии соглашения Enterprise РЦ с GlobalSign и требований, изложенных в Приложении A настоящего CPS.

GlobalSign налагает ограничения, применимые к органам регистрации предприятий, в качестве договорного требования к РА предприятия и контролирует соблюдение РА предприятия в соответствии с разделом 8.8.

1.3.2.1.1 Сертификаты TLS

Что касается сертификатов TLS, GlobalSign не будет принимать запросы на сертификаты, авторизованные центром сертификации предприятия, если не выполнены следующие требования:

1. GlobalSign подтверждает, что запрошенные полные доменные имена находятся в проверенном пространстве доменных имен Enterprise РЦ.
2. Если запрос сертификата включает имя субъекта типа, отличного от полного доменного имени, GlobalSign подтверждает, что это имя принадлежит либо делегированному предприятию, либо аффилированному лицу делегированного предприятия, либо что делегированное предприятие является агент названного Субъекта.

1.3.2.1.2 Сертификаты расширенной проверки

Для TLS расширенной проверки или сертификатов подписи кода расширенной проверки:

1. Абонент должен быть организацией, проверенной УЦ в соответствии с Руководством EV.
2. GlobalSign не делегирует выполнение окончательных требований к взаимной корреляции и комплексной проверке, предусмотренных разделом 11.12 Руководства EV.

1.3.2.1.3 Сертификаты S/MIME BR

Для сертификатов S/MIME BR GlobalSign не будет принимать запросы на сертификаты, авторизованные РЦ предприятия, если не выполнены следующие требования:
1. Если запрос на сертификат относится к профилю, проверенному почтовым ящиком, организацией или спонсором, GlobalSign подтверждает, что Enterprise РЦ имеет авторизацию или контроль над запрошенным доменом(ами) электронной почты в соответствии с разделом 3.2.2.1 или разделом 3.2.2.3.
2. GlobalSign подтверждает, что имя субъекта: имя организации принадлежит либо делегированному предприятию, либо аффилированному лицу делегированного предприятия, либо что делегированное предприятие является агентом указанного Субъекта.
Представитель РЦ предприятия также может отправлять запросы на сертификаты с использованием профиля, проверенного почтовым ящиком, для пользователей, чьи домены электронной почты не находятся под авторизацией или контролем делегированной организации. В этом случае GlobalSign подтверждает, что владелец почтового ящика контролирует запрошенный адрес(а) почтового ящика в соответствии с разделом 3.2.2.2.

Сертификаты расширенной проверки
Для TLS расширенной проверки или сертификатов подписи кода расширенной проверки:

1. Абонент должен быть организацией, проверенной УЦ в соответствии с Руководством EV.
2. GlobalSign не делегирует выполнение окончательных требований к взаимной корреляции и комплексной проверке, предусмотренных разделом 11.12 Руководства EV.

1.3.2.2 Квалифицированные сертификаты

GlobalSign может делегировать местному или внешнему РЦ проверку личности и управление жизненным циклом сертификата. В этом случае GlobalSign обеспечивает соблюдение РЦ применимых норм, законов, отраслевых стандартов и политик.

Местный или внешний РЦ заключает с GlobalSign договор о делегированной деятельности, включающий, по крайней мере, следующее:

- Обязательство РЦ соблюдать соответствующие нормативные акты, законы, отраслевые стандарты и политику.
- Распределение ответственности между GlobalSign и РЦ.

- Возможность GlobalSign отозвать делегирование.
- Возможность GlobalSign контролировать соблюдение РЦ соответствующих нормативных актов, законов, отраслевых стандартов и политик через аудиторские проверки.

1.3.2.2.1 Местные РЦ

Субъекты

Проверка личности доступна только для сотрудников (физических лиц) местного РЦ, его родительских, дочерних или аффилированных организаций.

Делегированные полномочия
Делегирование полномочий местному РЦ ограничивается подтверждением личности и аутентификацией отдельных субъектов, а также событиями жизненного цикла сертификата, включая запрос и отзыв сертификата.

Соответствие требованиям
GlobalSign применяет соответствующие меры для обеспечения соблюдения местным РЦ применимых норм, законов, отраслевых стандартов и политик.

1.3.2.2.2 Внешние РЦ

Субъекты
Субъектами могут быть физические и/или юридические лица.

Делегированные полномочия
Делегирование может включать подтверждение личности Абонента (и/или субъекта), аутентификацию запроса и события жизненного цикла сертификата, включая запрос и отзыв.

Аудиты
Для обеспечения соблюдения соответствующих нормативных актов, законов, отраслевых стандартов и политик, внешний РЦ должен:

- Проходить аудиторские проверки в рамках аудитов GlobalSign; или
- Предоставить отчет об аудите от органа по оценке соответствия или эквивалентного органа.

1.3.3 Абоненты

Абоненты — это юридические или физические лица, которые успешно подают заявку и получают Сертификат для использования в транзакциях, коммуникациях и применении Цифровых подписей.

Под *Абонентом* в настоящем документе понимается как субъект сертификата, так и организация, заключившая контракт с GlobalSign на выдачу сертификата. До проверки личности и выдачи сертификата Абонент является *Заявителем*.

Юридические лица идентифицируются на основе изучения опубликованных внутренних документов организации и назначения директора (директоров), а также последующего правительственного вестника или аналогичной официальной правительственной публикации, или других баз данных третьих сторон квалифицированного независимого источника информации (QIIS) или квалифицированного правительственного источника информации (QGIS). Самозанятые субъекты идентифицируются на основании подтверждения профессиональной регистрации, предоставленного компетентным органом страны, в которой они проживают.

Для всех категорий Абонентов требуются дополнительные полномочия, как объясняется в онлайн-процессе подачи заявки на получение сертификата.

В число Абонентов сертификатов конечных субъектов включаются сотрудники и агенты GlobalSign, деятельность которых требует каждодневного доступа к сетевым ресурсам GlobalSign. В число Абонентов также иногда заносят операционных или юридических владельцев устройств для создания подписей, которые выпускаются с целью генерации пар ключей и хранения сертификатов.

Предполагается, что организация-Абонент заключила соглашение об обслуживании или другие договорные отношения с GlobalSign, уполномочивающие ее выполнять конкретную функцию в рамках приложения, использующего услуги сертификата GlobalSign. Выдача сертификата организации-Абоненту разрешается только в соответствии с таким соглашением между GlobalSign и конечной организацией-Абонентом.

1.3.4 Доверяющие стороны

Чтобы проверить действительность сертификата, доверяющие стороны должны всегда обращаться к информации от GlobalSign либо из точки распространения COC, либо в виде ответа OCSP.

1.3.5 Другие участники

Среди других участников — мостовые УЦ, а также УЦ, осуществляющие перекрестную сертификацию подчиненных УЦ для обеспечения доверия между разными сообществами PKI.

1.4 Использование сертификатов

Сертификат позволяет субъекту, участвующему в электронной транзакции, подтвердить свою личность перед другими участниками этой транзакции. В коммерческой среде сертификаты используются в качестве цифрового эквивалента идентификационной карты.

1.4.1 Правильное использование сертификата

Использование сертификата конечным субъектом ограничено значениями использования ключа и расширенного ключа.

Сертификаты GlobalSign можно использовать для публичных транзакций со следующими свойствами:

- **Фиксация авторства и обязательства по содержанию.** Сторона не может отрицать факт участия в транзакции или отправки электронного сообщения.
- **Аутентификация.** Один субъект получает гарантию, что другой субъект является тем, за кого себя выдает.
- **Конфиденциальность.** Гарантия, что никто не сможет прочитать определенный фрагмент данных, кроме получателя (получателей), которому явно адресовано сообщение.
- **Целостность.** Гарантия того, что данные не изменялись (намеренно или нет) на пути от отправителя к получателю и от момента передачи до момента получения.

Цифровая подпись: Цифровая (электронная) подпись может использоваться только для определенных операций, которые поддерживают цифровую подпись форм, документов или электронной почты. Сертификат используется для проверки цифровой подписи, сделанной закрытым ключом, который соответствует открытому ключу в сертификате. Поэтому он используется только в контексте приложений, поддерживающих сертификаты. Для цифровых подписей подходят следующие типы сертификатов:

- **PersonalSign 2.** Фиксация авторства и обязательства по содержанию транзакций (средний уровень заверения)
- **PersonalSign 2 Pro.** Фиксация авторства и обязательства по содержанию транзакций стороной, которая действует в контексте организации (средний уровень заверения)
- **AATL.** Фиксация авторства и обязательства по содержанию транзакций стороной, которая действует в контексте организации (средний уровень заверения с

аппаратной поддержкой). (Не рекомендуется использовать данный сертификат для шифрования из-за его необычности)
- **Квалифицированные сертификаты.** Фиксация авторства и обязательства по содержанию для подписи физического лица (квалифицированные сертификаты электронных подписей) и юридического лица persons (квалифицированные сертификаты электронных печатей)

Аутентификация (пользователи): Сертификаты аутентификации пользователей используются для аутентификации при доступе к веб-сайтам и другому онлайн-контенту, электронной почте и т.д. Функция аутентификации часто является результатом комбинации проверок определенных свойств сертификата, таких как проверка личности Абонента, связанного с открытым ключом. Для описания функции аутентификации часто используется термин «цифровая подпись», поскольку таким методом предоставляет доказательство владения закрытым ключом, который соответствует открытому ключу в сертификате.

- **PersonalSign 2.** Аутентификация физического лица (средний уровень надежности) и подтверждение адреса электронной почты.
- **PersonalSign 2 Pro.** Аутентификация физического лица, машины, устройства, отдела или роли (должности) в контексте организации (средний уровень надежности) и, по желанию, адреса электронной почты.
- **PersonalSign 3 Pro.** Аутентификация физического лица в контексте организации (высокий уровень надежности).
- **Рудиментарная аутентификация NAESB**, как предписано в «Руководстве NIST SP800-63A Digital Identity: Регистрация и подтверждение личности», раздел 4.3 «Уровень заверения I для подтверждения идентичности».
- **Базовая аутентификация NAESB,** как предписано в Базовых требованиях, раздел 3.2.3 «Проверка подлинности личности». Работодатели, которые проверяют личность своих кандидатов средствами, сравнимыми с указанными выше для Базового уровня, могут выбрать стать локальный УЦ и проводить проверку личности кандидатов либо лично, проверяя корпоративный пропуск с фотографией, либо через безопасный онлайн-процесс локального УЦ. Корпоративный пропуск или онлайн-процесс должны основываться на удостоверении личности государственного образца с фотографией.
- **Средняя аутентификация NAESB,** как предписано в Руководстве EV, глава 11.2.2: «Приемлемый метод верификации (4) Основное лицо».

Аутентификация (устройства и объекты): Сертификаты аутентификации устройств используются для электронных операций аутентификации, которые поддерживают идентификацию веб-сайтов и других онлайн-ресурсов, таких как программные объекты. Функция аутентификации сертификата часто является результатом комбинации проверок определенных свойств сертификата. Например, проверка веб-сервера, связанного с открытым ключом. Для описания функции аутентификации часто используется термин «цифровая подпись», поскольку таким методом, например, веб-сервер доказывает факт владения закрытым ключом, соответствующим открытому ключу в сертификате. Таким способом проверяется доменное имя в сертификате.

- **DomainSSL.** Аутентификация удаленного доменного имени или веб-сервиса и шифрование канала связи.
- **AlphaSSL.** Аутентификация удаленного доменного имени или веб-сервиса и шифрование канала связи.
- **OrganizationSSL.** Аутентификация удаленного доменного имени и связанного контекста организации, веб-сервиса, шифрование канала связи.
- **Расширенная проверка SSL.** Аутентификация удаленного доменного имени и связанного контекста организации, веб-сервиса, шифрование канала связи.
- **Подпись кода.** Аутентификация объекта данных у юридического лица или самого юридического лица.
- **Подпись кода EV.** Аутентификация объекта данных у юридического лица или самого юридического лица.

- **Метки времени.** Аутентификация времени и даты, связанных с услугой в контексте организации.
- **PersonalSign (все).** Аутентификация устройства или машины, связанной с организацией.
- **Рудиментарная аутентификация NAESB**, как предписано в «Руководстве NIST SP800-63A Digital Identity: Регистрация и подтверждение идентичности», раздел 4.3 «Уровень заверения I для подтверждения идентичности».
- **Базовая аутентификация NAESB,** как предписано в «Базовых требованиях», раздел 3.2.3 «Проверка подлинности личности».
- **Средняя аутентификация NAESB,** как предписано в Руководстве EV, глава 11.2.2: «Приемлемый метод верификации (4) Основное лицо».

Уровни заверения: При проверке Абонент выбирает соответствующую степень заверения, которую хочет предоставить доверяющим сторонам. Например, Абоненту с неизвестным брендом нужен сертификат с расширенной проверкой (EV), в то время как узкому сообществу с известным URL или специфическими транзакциями можно выбрать низкий уровень заверения.

- **Сертификаты с низким уровнем заверения** (класс 1) не подходят для проверки идентичности, поскольку в сертификате нет соответствующей информации. Эти сертификаты не поддерживают функцию безотзывности и ответственности за содержание документов.
- **Сертификаты со средним уровнем заверения** (класс 2) — индивидуальные и организационные сертификаты, которые подходят для обеспечения умеренно рискованных межорганизационных, внутриорганизационных и коммерческих транзакций.
- **Сертификаты с высоким уровнем заверения** (класс 3) — индивидуальные и организационные сертификаты, которые обеспечивают высокий уровень уверенности в идентичности субъекта по сравнению с классами 1 и 2.
- **Сертификаты с высоким уровнем заверения (EV)** — сертификаты класса 3, выпущенные компанией GlobalSign в соответствии с Руководством по расширенной проверке (Руководство EV).
- **Рудиментарный уровень NAESB** обеспечивает самую низку степень заверения. Одной из основных функций является обеспечение целостности данных, а не личности. Этот уровень подходит для сред, в которых риск вредоносной деятельности считается низким. Он не подходит для операций, требующих аутентификации, и обычно недостаточен для операций, требующих конфиденциальности, но может быть использован для последних, если недоступны сертификаты с более высоким уровнем заверения.
- **Базовый уровень NAESB** подходит для сред, где существуют риски и последствия компрометации данных, но они не считаются серьезными. Это может включать доступ к частной информации, где вероятность злоумышленного доступа невелика. На этом уровне заверения предполагается, что пользователи не склонны к злоупотреблениям.
- **Средний уровень NAESB** подходит для среды с умеренными рисками и последствиями компрометации данных. Сюда могут входить крупные коммерческие операции или риск мошенничества, или защита приватной информации со значительным риском атаки со стороны злоумышленников.

Конфиденциальность: Все типы сертификатов, за исключением сертификатов с временной меткой и подписи кода, могут быть использованы для обеспечения конфиденциальности коммуникаций. Конфиденциальность может относиться к деловым и личным коммуникациям, а также к защите персональных данных и приватности.

Сертификаты, выпущенные в рамках NAESB PKI, могут использоваться для транзакций в соответствии со стандартами деловой практики WEQ-001, WEQ002, WEQ-003, WEQ-004 и WEQ-005. Они могут быть использованы также для других операций по взаимному соглашению сторон. Сертификаты, выданные в соответствии с WEQ-012 («Стандарты WEQ

NAESB»), никогда не должны использоваться для выполнения какой-либо из следующих функций:

- Транзакция или передача данных, которая может привести к тюремному заключению в случае компрометации или фальсификации.
- Транзакция или передача данных, которая считается незаконной в соответствии с федеральным законодательством.

Любое другое использование сертификата не поддерживается данным CPS: В рамках одного сертификата допускаются функции электронной подписи (фиксация авторства и обязательства по содержанию) и аутентификации (цифровая подпись). Различные термины относятся к разным терминологиям. Одна терминология принята Инженерным советом Интернета (IETF), другая — в правовых рамках директивы Европейского союза 1999/93/EC (общественный фреймворк по электронным подписям), Регламента eIDAS (Regulation (EU)N910/2014) ("eIDAS"), eIDAS (Великобритания) и Положения об электронной идентификации и доверительных услугах для электронных транзакций 2016 года ("UK eIDAS").

1.4.2 Запрещенное использование Сертификата

Сфера действия сертификата ограничена с помощью соответствующих расширений сертификата и функции расширенного использования ключей. Запрещается любое использование сертификата, не соответствующее этим расширениям. Сертификаты не разрешено использовать для транзакций, превышающих установленные лимиты доверия, указанные в Гарантийной политике GlobalSign.

Сертификаты по данному CPS не гарантируют, что субъект заслуживает доверия, ведет надежный бизнес или что оборудование, на котором установлен сертификат, не пострадает от дефектов, вредоносных программ или вирусов. Сертификат подписи кода не гарантирует, что подписанный код не содержит ошибок или уязвимостей.

Сертификаты по данному CPS не могут быть использованы:

- Для любого применения, требующего безотказной работы
- Для любого применения или механизма, где проблемы с сертификатом могут вызвать риск для безопасности (например, риск для людей или окружающей среды)
- В случаях, когда это запрещено законом.
- Квалифицированные сертификаты для электронных подписей должны использоваться только физическими лицами, а сертификаты для электронных печатей — только юридическими лицами.
- Сертификаты, выданные в соответствии с NAESB WEQ PKI, никогда не должны использоваться для выполнения какой-либо из следующих функций:
    - Транзакция или передача данных, которая может привести к тюремному заключению в случае компрометации или фальсификации.
    - Транзакция или передача данных, которые считаются незаконными в соответствии с федеральным законодательством.

1.5 Управление политикой

1.5.1 Организация, администрирующая документ

Запросы на информацию о соответствии подчиненных УЦ схемам аккредитации, а также любые другие запросы по данному CPS следует направлять по адресу:

PACOM1 – CA Governance GlobalSign
Diestsevest 14,
3000 Leuven, Belgium
Тел.: + 32 (0)16 891900
Факс: + 32 (0) 16 891909
Электронная почта: policy-authority@globalsign.com

1.5.2 Контактное лицо

Общие запросы

GlobalSign NV/SA attn.
Legal Practices,
Diestsevest 14,
3000 Leuven, Belgium
Тел.: + 32 (0)16 891900
Факс: + 32 (0) 16 891909
Электронная почта: legal@globalsign.com
URL: www.globalsign.com

Сообщения о проблемах с сертификатами

Организации по борьбе с вредоносным ПО, Абоненты, доверяющие стороны, поставщики прикладного ПО и другие третьи стороны могут сообщать о подозрениях в компрометации закрытого ключа, неправомерном использовании сертификатов, подписи подозрительного кода, похищении аккаунтов или других видах мошенничества, компрометации, неправомерного использования, ненадлежащего поведения или любых других вопросах, связанных с сертификатами, по электронному адресу:

report-abuse@globalsign.com

GlobalSign может отозвать или не отозвать сертификат в ответ на этот запрос. См. раздел 4.9.5, где подробно описаны действия, выполняемые GlobalSign для принятия такого решения.

1.5.3 Лицо, определяющее применимость CPS

Применимость CP и соответствие данной CPS определяет PACOM1 - CA Governance на основании результатов и рекомендаций, полученных от квалифицированного аудитора.

В целях поддержания авторитета и доверия к данной CPS и лучшего соответствия требованиям аккредитации и законодательства, руководство PACOM1 - CA пересматривает данную CPS не реже одного раза в год и может вносить изменения и обновления в правила по своему усмотрению или по требованию других обстоятельств. Любые обновления становятся обязательными для всех выданных и будущих сертификатов с момента публикации обновленной версии данного CPS.

1.5.4 Процедуры утверждения CPS

PACOM1 - CA Governance рассматривает и утверждает любые изменения в CPS. Обновленный документ проверяется на соответствие CP. Изменения в CP добавляются по мере необходимости. После утверждения обновления руководством PACOM1 - CA Governance, новое CPS публикуется в репозитории GlobalSign по адресу https://www.globalsign.com/repository.

Обновленная версия является обязательной для всех Абонентов, включая Абонентов и стороны, полагающиеся на сертификаты, выданные в соответствии с предыдущей версией CPS.

1.6 Определения и аббревиатуры

Любые термины, используемые, но не определенные в настоящем документе, имеют значение, присвоенное им в Требованиях форума CA/браузера и правилах eIDAS.

Adobe Approved Trust List (AATL): Хранилище удостоверяющего центра для подписи документов, созданное органом Adobe Root CA и внедренное в Adobe PDF Reader версии 9.0.

Certificate Authority Authorization (CAA): Запись CAA используется для указания удостоверяющих центров, которым разрешено выдавать сертификаты для домена.

DCF77: Немецкий длинноволновый передатчик точного времени и частоты.

GlobalSign Certificate Center (GCC): Центр сертификации GlobalSign (GCC): Облачная система управления сертификатами, с помощью которой клиенты и партнеры могут приобретать и управлять сертификатами GlobalSign.

IP-адрес: 32-битный или 128-битный номер, присвоенный устройству, которое использует для связи Интернет-протокол (IP).

Online Certificate Status Protocol: Протокол онлайн-проверки сертификатов, который позволяет прикладному программному обеспечению доверяющей стороны определять статус идентифицированного сертификата. См. также Ответчик OCSP.

Сертификат S/MIME: сертификат, предназначенный для использования для подписи, проверки, шифрования и расшифровки электронной почты. Сертификат с расширенным использованием ключа (EKU) для id-kp-emailProtection (OID: 1.3.6.1.5.5.7.3.4) и включением rfc822Name или другого имени типа id-on-SmtpUTF8Mailbox в расширение subjectAltName.

Сертификат S/MIME BR: Сертификат S/MIME, соответствующий базовым требованиям для политики S/MIME.

SSL-сертификат: Сертификаты для аутентификации серверов в интернете.

UK eIDAS ("UK eIDAS"): eIDAS (UK Legislation) и Положения об электронной идентификации и доверенных услугах для электронных транзакций 2016 года.

X.400: Стандарт Международного союза электросвязи-Т (МСЭ-Т) для электронной почты.

X.500: Стандарт МСЭ-Т для служб каталогов.

X.509: Стандарт МСЭ-Т для сертификатов

Абонентский договор: Соглашение между УЦ и заявителем/Абонент
ом, определяющее права и обязанности сторон.

Авторизованный центр сертификации: Центр сертификации, который соответствует всем положениям Стандарта деловой практики Североамериканского совета по энергетическим стандартам (NAESB) для инфраструктуры открытых ключей (PKI) — WEQ-012.

Аппаратный модуль безопасности (HSM): Тип защищенного криптопроцессора, предназначенный для управления цифровыми ключами, ускорения криптопроцессов с точки зрения количества цифровых подписей в секунду и обеспечения надежной аутентификации для доступа к критическим ключам для серверных приложений.

Аттестационное письмо: Письмо, подтверждающее правильность информации об идентификации субъекта.

Аффилированное лицо: Корпорация, партнерство, совместное предприятие или другая организация, контролирующая, управляемая или находящаяся под общим контролем с другой организацией, или агентство, департамент, политическое подразделение или любая организация, работающая под прямым контролем правительственной организации.

Бенефициары сертификата: Абонент (абонент) как сторона Абонентского договора или Условий использования сертификата, все поставщики прикладного программного обеспечения, с которыми компания GlobalSign заключила договор о включении своего корневого сертификата, и все доверяющие стороны, которые обоснованно полагаются на действительный сертификат.

Включение путем ссылки: Сделать один документ частью другого путем идентификации документа, который должен быть включен, с информацией, позволяющей получателю получить доступ и получить включенное сообщение в полном объеме, и выражением намерения, чтобы оно стало частью включающего сообщения. Такое инкорпорированное сообщение имеет такое же действие, как если бы оно было полностью изложено в сообщении.

Внутреннее имя: Строка символов (не IP-адрес) в общем имени или альтернативном имени субъекта (SAN) сертификата, которое нельзя проверить на уникальность в публичной системе DNS на момент выпуска сертификата, поскольку оно не заканчивается суффиксом домена верхнего уровня из базы IANA (Root Zone Database).

Выпускающий УЦ: В отношении конкретного сертификата это УЦ, выпустивший сертификат. Им может быть как корневой, так и подчиненный УЦ.

Глобальная система позиционирования (GPS): Американская система, предоставляющая пользователям услуги по определению местоположения, сервисы навигации и времени (PNT).

Государственная организация: Управляемое правительством юридическое лицо, агентство, департамент, министерство, филиал или аналогичный элемент правительства страны или политическое подразделение в этой стране (например, регион, область, город, округ и т. д.).

Данные сертификата: Запросы на сертификат и относящиеся к ним данные (полученные от заявителя или иным образом), находящиеся во владении или под контролем УЦ или к которым УЦ имеет доступ.

Дата истечения срока действия: Дата «Не после» в сертификате, определяющая окончание срока действия сертификата.

Действительный сертификат: Сертификат, который проходит проверку, как описано в RFC 5280.

Деловое предприятие: Любая организация, которая не является частной, государственной или некоммерческой организацией, как определено в Руководстве по расширенной проверке. Среди примеров: полные товарищества, некорпорированные ассоциации, индивидуальные предприниматели и т. д.

Директива о платежных сервисах (PSD2): Директива Европейского союза (EU) 2015/2366, регулирующая платежные услуги и поставщиков платежных сервисов на территории Европейского союза и Европейской экономической зоны.

Доверенная третья сторона: Поставщик услуг с безопасным процессом проверки личности человека на основе удостоверения личности государственного образца. Или его услуга сама генерирует разновидность такого удостоверения личности.

Доверяющая сторона: Любое физическое или юридическое лицо, которое полагается на действительный сертификат. Поставщик прикладного ПО не считается доверяющей стороной, если его программное обеспечение просто отображает информацию о сертификате.

Доменная метка: Как указано в RFC 8499 (http://tools.ietf.org/html/rfc8499): «Упорядоченный список из нуля или более октетов, составляющий часть доменного имени. Используя теорию графов, метка идентифицирует один узел в части графа всех возможных доменных имен».

Доменное имя: Упорядоченный список из одной или нескольких доменных меток, присвоенных узлу в системе доменных имен.

Доменное имя Wildcard: Строка, начинающаяся с символа "*". (U+002A ASTERISK, U+002E FULL STOP), за которой сразу следует полностью квалифицированное доменное имя.

Доменное имя авторизации: Имя FQDN, которое используется для получения разрешения на включение данного FQDN в сертификат. Для проверки домена УЦ может взять FQDN из поиска DNS CNAME. Если в сертификат следует включить имя из маски wildcard, то УЦ ДОЛЖЕН удалить символы "*." из самой левой части доменного имени с символами wildcard, чтобы получить соответствующее FQDN. УЦ может обрезать несколько доменных меток FQDN слева направо, пока не встретит основное доменное имя, и может использовать для проверки домена любое из значений, полученных в результате обрезки (включая само основное доменное имя).

Закрытый ключ: Ключ пары ключей, который хранится владельцем в секрете и используется для создания цифровых подписей и/или расшифровки электронных записей и файлов, зашифрованных соответствующим открытым ключом.

Зарегистрированное доменное имя: Доменное имя, которое было зарегистрировано у регистратора доменных имен.

Зарезервированный IP-адрес: Адрес IPv4 или IPv6 в адресном блоке любой записи в одном из следующих реестров IANA:

https://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtml
https://www.iana.org/assignments/iana-ipv6-special-registry/iana-ipv6-special-registry.xhtml

Захват секретного ключа (takeover attack): Атака, при которой служба подписи или закрытый ключ, связанный с сертификатом подписи кода, были скомпрометированы в результате мошенничества, кражи, преднамеренных злонамеренных действий агента субъекта или других незаконных действий.

Заявитель: Физическое или юридическое лицо, подающее заявку на получение (или требующее продления) сертификата. После выдачи сертификата заявитель именуется Абонентом. Для сертификатов, выпущенных для устройств, заявителем является организация, которая контролирует или управляет устройством, указанным в сертификате, даже если фактический запрос на сертификат отправляет устройство.

Заявление о практике сертификации: Один из нескольких документов, формирующих структуру управления, в которой создаются, выпускаются, управляются и используются сертификаты.

Идентификатор объекта (OID): Уникальный буквенно-цифровой или цифровой идентификатор, зарегистрированный по соответствующему стандарту Международной организации по стандартизации для конкретного объекта или класса объектов.

Интернационализированное доменное имя (IDN): Интернет-доменное имя, содержащее по крайней мере один языковой или алфавитный символ, который затем переводится в кодировку ASCII методом punycode для использования в международной системе DNS, которая принимает только ASCII.

Информация об идентификации Субъекта: Информация, идентифицирующая субъект сертификата. Информация об идентификации субъекта не включает доменное имя, указанное в расширении subjectAltName или в поле commonName.

Инфраструктура открытых ключей (PKI): Набор аппаратных средств, программного обеспечения, людей, процедур, правил, политик и обязательств, используемых для

обеспечения надежного создания, выпуска, управления и использования сертификатов и ключей на основе криптографии с открытым ключом.

Квалифицированная временная маркировка (QTS): Проставление временных меток, соответствующих статье 42 Регламента eIDAS/UK eIDAS.

Квалифицированная электронная печать: Усовершенствованная электронная печать, созданная устройством для создания квалифицированных электронных печатей на основе квалифицированного сертификата электронной печати.

Квалифицированная электронная подпись: Усовершенствованная электронная подпись, созданная устройством для создания квалифицированных подписей и основанная на квалифицированном сертификате для электронных подписей.

Квалифицированное устройство создания электронной подписи/печати (QSCD): Устройство создания электронной подписи/печати, отвечающее требованиям, установленным в Приложении II к Регламенту eIDAS.

Квалифицированные сертификаты веб-аутентификации (QWAC): Квалифицированный SSL-сертификат, отвечающий требованиям статьи 45 Регламента eIDAS/UK eIDAS.

Квалифицированный аудитор: Физическое или юридическое лицо, отвечающее требованиям раздела 8.2 (Идентификация/квалификация аудитора).

Квалифицированный государственный источник информации: База данных, которую ведет государственная организация.

Квалифицированный государственный источник налоговой информации: Квалифицированный государственный источник информации. В частности, содержит налоговую информацию, относящуюся к частным организациям, деловым предприятиям или физическим лицам.

Квалифицированный независимый источник информации: Регулярно обновляемая и актуальная, общедоступная база данных, созданная с целью точного предоставления информации, для которой она используется, и общепризнанная как надежный источник такой информации.

Квалифицированный поставщик доверенных услуг (QTSP): Физическое или юридическое лицо, предоставляющее одну или несколько доверенных услуг и получившее квалифицированный статус от надзорного органа, как определено в регламенте eIDAS/UK eIDAS.

Квалифицированный сертификат: Сертификат, отвечающий квалификационным требованиям, определенным Положением об eIDAS/UK eIDAS.

Квалифицированный сертификат для электронных печатей: Сертификат, отвечающий квалификационным требованиям, определенным Положением об eIDAS/UK eIDAS.

Квалифицированный сертификат электронной подписи: Сертификат электронной подписи, выданный квалифицированным поставщиком доверенных услуг и отвечающий требованиям, изложенным в Приложении I к Регламенту eIDAS/UK eIDAS.

Компрометация: Нарушение политики безопасности, которое приводит к потере контроля над конфиденциальной информацией.

Компрометация ключа: Закрытый ключ считается скомпрометированным, если его значение было раскрыто неуполномоченному лицу, неуполномоченное лицо получило к нему доступ или существует практический метод, с помощью которого неуполномоченное лицо может узнать его значение.

Контакт IP-адреса: Лицо(-а) или организация(-и), зарегистрированные в органе регистрации IP-адресов как имеющие право контролировать использование одного или нескольких IP-адресов.

Контакт домена: Регистрант доменного имени, технический контакт или административный контракт (или эквивалент в ccTLD), указанный в записи WHOIS основного доменного имени или в записи DNS SOA, или полученный при непосредственном контакте с регистратором доменного имени.

Контактный адрес электронной почты DNS CAA: Адрес электронной почты, определенный в Приложении B.1.1. Базовых требований для TLS.

Контактный адрес электронной почты в записи DNS TXT: Адрес электронной почты, определенный в Приложении B.2.1. Базовых требований для TLS.

Контактный номер телефона в записи DNS TXT: Номер телефона, определенный в Приложении B.2.2. Базовых требований для TLS.

Контролирующий орган: Орган, выполняющий надзор за квалифицированными поставщиками доверенных услуг на территории определенного государства, а в случае необходимости принимающий меры в отношении неквалифицированных поставщиков доверенных услуг. Подробности описаны в статье 17 eIDAS.

Корневой сертификат: Самоподписанный сертификат, выданный корневым УЦ для самоидентификации и упрощения проверки сертификатов, выданных подчиненным УЦ.

Корневой УЦ: Удостоверяющий центр высшего уровня. Он выдает сертификаты подчиненных УЦ, а его корневой сертификат распространяется поставщиками прикладного ПО.

Корпоративная PKI (EPKI): Продукт GlobalSign для организаций, позволяющий управлять полным жизненным циклом доверенных цифровых идентификаторов Microsoft Windows, Adobe Approved Trust List, включая выпуск, перевыпуск, обновление и аннулирование.

Корпоративный РЦ: Сотрудник или агент организации, не связанной с УЦ, который разрешает выпуск сертификатов для этой организации или ее дочерних компаний. Корпоративный РЦ может также разрешить выдачу клиентских сертификатов для аутентификации партнерам, клиентам или филиалам, желающим взаимодействовать с этой организацией.

Место ведения бизнеса: Местонахождение любого объекта (например, завода, розничного магазина, склада и т. д.), где ведется бизнес заявителя.

Модуль доверенной платформы (TPM): Аппаратное криптографическое устройство, определенное Группой доверенных вычислений (Trusted Computing Group): https://www.trustedcomputinggroup.org/specs/TPM.

Надежная система: Компьютерное оборудование, программное обеспечение и процедуры, которые достаточно защищены от вторжения и неправомерного использования; обеспечивают разумный уровень доступности, надежности и корректной работы; разумно подходят для выполнения своих предполагаемых функций; обеспечивают соблюдение применимой политики безопасности.

Общая база данных центров сертификации (CCADB): Управляемое Mozilla хранилище сертификатов, в котором перечислены все публичные доверенные корни и выпускающие сертификаты.

Орган по оценке соответствия: Орган, определенный в пункте 13 статьи 2 Регламента (ЕС) № 765/2008, который аккредитован в соответствии с этим Регламентом как компетентный для проведения оценки соответствия квалифицированного поставщика услуг доверия и предоставляемых им квалифицированных услуг доверия.

Орган регистрации IP-адресов: Администрация адресного пространства Интернет (IANA) или региональный регистратор (RIPE, APNIC, ARIN, AfriNIC, LACNIC).

Организация по борьбе с вредоносным ПО: Организация, которая хранит информацию о подозрительном коде и/или разрабатывает программное обеспечение, используемое для предотвращения, обнаружения или удаления вредоносных программ.

Печать WebTrust: Подтверждение соответствия, полученное в результате реализации программы WebTrust для УЦ.

Программа WebTrust для УЦ: Действующая в соответствующий момент времени или сейчас версия Программы AICPA/CICA WebTrust для удостоверяющих центров.

Псевдоним: вымышленная личность, которую человек принимает на себя для определенной цели. В отличие от анонимной личности, псевдоним может быть связан с реальной личностью человека.

Поиск WHOIS: Информация, полученная непосредственно от регистратора доменных имен или оператора реестра по протоколу WHOIS, определенному в RFC 3912, протоколу доступа к данным реестра, определенному в RFC 7482, или через веб-сайт HTTPS.

Основное доменное имя: Часть заявленного FQDN, которая является первым узлом доменного имени слева от контролируемого реестром или общедоступного суффикса, плюс сам суффикс (например, "example.co.uk" или "example.com"). Для FQDN, в которых крайний правый узел доменного имени представляет доменную зону верхнего уровня (gTLD) со Спецификацией 13 от ICANN в соглашении о реестре, сама gTLD может использоваться в качестве базового доменного имени.

Ответчик OCSP: Онлайн-сервер, работающий под управлением УЦ и подключенный к его хранилищу для обработки запросов о статусе сертификата. См. также Протокол состояния сетевого сертификата.

Открытый ключ: Ключ из пары ключей, который может быть публично раскрыт держателем соответствующего закрытого ключа. Открытый ключ используется доверяющей стороной для проверки цифровых подписей, созданных с помощью соответствующего закрытого ключа держателя, и/или для шифрования сообщений таким образом, что они могут быть расшифрованы только с помощью соответствующего закрытого ключа держателя.

Перекрестный сертификат: Сертификат, который используется для установления доверительных отношений между двумя корневыми УЦ.

Абонент: Физическое или юридическое лицо, которому выдан сертификат и которое юридически связано Абонентским договором или Условиями использования.

Подчиненный УЦ: Удостоверяющий центр, чей сертификат подписан корневым УЦ или другим подчиненным УЦ.

Политика сертификатов: Набор правил, указывающий на применимость названного сертификата к определенному сообществу и/или реализации PKI с общими требованиями безопасности.

Полностью определенное доменное имя (FQDN): Доменное имя, включающее доменные метки всех вышестоящих узлов в системе доменных имен Интернета.

Поставщик прикладного ПО: Поставщик программного обеспечения интернет-браузера или другого прикладного программного обеспечения доверяющей стороны, которое отображает или использует сертификаты и включает корневые сертификаты.

Пространство доменных имен: Набор всех возможных доменных имен, подчиненных одному узлу в системе доменных имен.

Протокол сетевого времени (NTP): Сетевой протокол для синхронизации времени между компьютерными системами в сетях передачи данных с пакетной коммутацией и переменной задержкой.

Процесс управления сертификатами: Процессы, практики и процедуры, связанные с использованием ключей, программного и аппаратного обеспечения, с помощью которых УЦ проверяет данные сертификата, выпускает сертификаты, ведет репозиторий и отзывает сертификаты.

Регистрант доменного имени: Иногда упоминается как «владелец» доменного имени, но более правильно — лицо (лица) или организация (организации), зарегистрированные у регистратора доменных имен как имеющие право контролировать использование доменного имени, например, физическое или юридическое лицо, указанное как «регистрант» в WHOIS или у регистратора доменных имен.

Регистратор доменных имен: Физическое или юридическое лицо, которое регистрирует Доменные имена под эгидой или по соглашению с: (i) Корпорацией по присвоению имен и номеров в Интернете (ICANN), (ii) национальным органом/реестром доменных имен или (iii) Сетевым информационным центром (NIC), включая его филиалы, подрядчиков, делегатов, преемников или правопреемников.

Регистрационный центр (РЦ): Любое юридическое лицо, которое отвечает за идентификацию и аутентификацию субъектов сертификатов, но не является УЦ и, следовательно, не подписывает и не выдает сертификаты. РЦ может помогать в процессе подачи заявки на сертификат или в процессе отзыва сертификата, или в обоих случаях. Когда «РЦ» используется в качестве прилагательного для описания должности или функции, это не обязательно отдельный орган, а может быть частью УЦ.

Регламент eIDAS ("eIDAS"): РЕГУЛИРОВАНИЕ (ЕС) № 910/2014 ЕВРОПЕЙСКОГО ПАРЛАМЕНТА И СОВЕТА от 23 июля 2014 года об электронной идентификации и доверительных услугах для электронных сделок на внутреннем рынке и отмене Директивы 1999/93/ЕС.

Репозиторий: Онлайновая база данных, содержащая публично раскрытые документы управления PKI (такие как политики сертификации и заявления о практике сертификации) и информацию о статусе сертификата, либо в форме COC, либо в форме ответа OCSP.

Сертификат: Электронный документ, в котором используется цифровая подпись для связывания открытого ключа и идентификатора.

Сертификат Open Banking: Квалифицированный сертификат со специфическими атрибутами Open Banking.

Сертификат Wildcard: Сертификат, содержащий по крайней мере одно доменное имя Wildcard в поле SAN.

Сертификат с открытым ключом: Сертификат, которому доверяют в силу того, что соответствующий корневой сертификат распространяется в качестве якоря доверия в широко доступном прикладном программном обеспечении.

Система доменных имен (DNS): Интернет-сервис, который переводит доменные имена в IP-адреса.

Сообщение о проблеме с сертификатом: Жалоба на подозрение в компрометации ключа, неправильное использовании сертификата или другие виды мошенничества, компрометации, неправильного использования или ненадлежащего поведения, связанного с сертификатами.

Специалист по проверке достоверности информации: Лицо, выполняющее обязанности по проверке информации, указанные в настоящем CPS.

Специфические атрибуты Open Banking: Атрибуты, которые являются специфическими для сертификатов **Open Banking**:

- номер авторизации NCA или регистрационный номер, признанный на национальном или европейском уровне, или идентификатор юрлица, включенный в реестр кредитных организаций.
- должность или должности PSP.
- имя NCA (NCAName) и уникальный идентификатор (NCAId).

Список отзыва сертификатов (COC): Регулярно обновляемый список отозванных сертификатов с временной меткой, который создается и подписывается цифровой подписью УЦ, выдавшего сертификаты.

Срок действия: Период от даты выпуска до даты истечения срока действия сертификата.

Стандарты деловой практики NAESB для инфраструктуры открытых ключей (PKI) — WEQ-012 («Стандарты деловой практики NAESB»): Минимальные требования для удостоверяющих центров, выданных ими сертификатов и конечных организаций, которые используют эти сертификаты.

Сторонний валидатор: Физическое или юридическое лицо, которое компетентно и уполномочено выполнять любое из следующих действий в соответствии с национальным законодательством: 1. дать заключение по фактическим утверждениям о заявителе, включая проверку конкретных атрибутов физического или юридического лица; 2. удостоверить подлинность подписи на документе. Примеры: госслужащие, нотариусы, дипломированные профессиональные бухгалтеры или адвокаты.

Страна: Член Организации Объединенных Наций ИЛИ географический регион, признанный в качестве суверенного государства не менее чем двумя странами-членами ООН.

Субъект: Физическое лицо, устройство, система, подразделение или юридическое лицо, указанное в сертификате в качестве субъекта. Если субъектом является устройство или система, оно должно находиться под контролем и управлением Абонента.

Технически ограниченный сертификат подчиненного УЦ: Сертификат подчиненного УЦ, в котором используется комбинация настроек использования расширенного ключа и настроек ограничения имени для общего ограничения области, в которой подчиненный УЦ может выпускать сертификаты Абонента или сертификаты дополнительных подчиненных УЦ.

Требования CA/Browser Forum: Следующий набор документов, опубликованный CA/Browser Forum, охватывающий требования к выдаче и управлению сертификатами: Базовые требования CA/Browser Forum к выдаче и управлению публично доверенными сертификатами, Рекомендации CA/Browser Forum по выдаче и управлению расширенной проверкой. Сертификаты, Требования к безопасности сети и системы сертификатов CA/Browser Forum, Базовые требования CA/Browser Forum для подписи кода, Базовые требования CA/Browser Forum для выдачи и управления публично доверенными сертификатами S/MIME

Требования Североамериканского совета по энергетическим стандартам (NAESB) по аккредитации для уполномоченных удостоверяющих центров («Спецификация аккредитации NAESB»): Технические и управленческие требования, которым должен соответствовать УЦ для аккредитации в качестве уполномоченного удостоверяющего центра NAESB.

Удостоверение личности государственного образца: Физическое или электронное удостоверение личности, выданное государственными органами, или форма удостоверения личности, которую государство принимает для подтверждения личности человека в своих официальных целях.

Удостоверящий центр (центр сертификации): Организация, которая отвечает за создание, выдачу, отзыв и управление сертификатами. Термин одинаково применим как к корневым, так и к подчиненным УЦ.

Условия использования: Положения о хранении и допустимом использовании сертификата, выданного в соответствии с Базовыми требованиями, когда заявитель/Абонент является аффилированным лицом УЦ.

Учредительное агентство: В контексте частной организации, государственное учреждение, под чьим руководством оформлено юридическое существование организации (например, государственное учреждение, которое выдает сертификаты о создании или регистрации). В контексте государственной организации — орган, принимающий законы, постановления или указы, устанавливающие юридическое существование государственных организаций.

Физическое лицо: Человек как субъект права.

Хэш (например, SHA1 или SHA256): Алгоритм, который отображает или переводит один набор битов в другой (обычно меньший) набор таким образом, что:

- Когда алгоритм обрабатывает одно и то же сообщение, каждый раз получается одинаковый результат.
- Восстановить исходное сообщение из хэша с помощью вычислений невозможно.
- С помощью вычислений невозможно найти два разных сообщения, которые дают одинаковый результат хэширования, используя один и тот же алгоритм.

Цифровая подпись: Кодирование сообщения с помощью асимметричной криптосистемы и хэш-функции таким образом, чтобы человек, имеющий исходное сообщение и открытый ключ подписанта, мог точно определить, что преобразование сделано с помощью закрытого ключа, соответствующего открытому ключу подписанта, а исходное сообщение не изменено после преобразования.

Частная организация: Негосударственное юридическое лицо (независимо от формы собственности), созданное путем подачи заявки (или акта) в учредительное агентство или эквивалентное учреждение по адресу регистрации.

Электронная печать: Данные в электронной форме, которые прикреплены к другим данным в электронной форме или логически связаны с ними для обеспечения происхождения и целостности последних.

Электронная подпись: Данные в электронной форме, которые присоединены к другим данным в электронной форме или логически связаны с ними, и которые используются для подписи.

Юридическое лицо: Ассоциация, корпорация, партнерство, собственник, траст, правительственная организация или другая организация, имеющая юридическую силу в правовой системе страны.

Юрисдикция инкорпорации: В контексте частной организации — страна и (если применимо) регион, область или населенный пункт, где юридическое существование

организации было установлено путем подачи заявки или взаимодействия с соответствующим государственным учреждением или органом (например, по месту регистрации). В контексте правительственной организации — страна и (если применимо) регион или область, где началось законное существование юридического лица.

AATL	Доверенный список, утвержденный Adobe
AICPA	Американский институт сертифицированных бухгалтеров
API	Программный интерфейс приложения
ARL	Список отзыва УЦ (также ведется список CRL (COC) для подчиненных УЦ, а не конечных организаций)
CAA	Авторизация удостоверяющего центра
CCADB	Общая база данных УЦ
ccTLD	Домен верхнего уровня, выделенный для конкретной страны
CICA	Канадский институт дипломированных бухгалтеров
DBA	Doing Business As (Ведение бизнеса как)
DNS	Система доменных имен
EIR	Реестр предприятий электропромышленности
EKU	Расширенное использование ключей
EPKI	Корпоративный PKI
ETSI	Европейский институт телекоммуникационных стандартов
EV	Расширенная проверка
FIPS	(правительство США) Федеральный стандарт обработки информации
FQDN	Полностью определенное доменное имя
GCC	Центр сертификации GlobalSign
GPS	Глобальная система позиционирования
IANA	Администрация адресного пространства Интернет
ICANN	Корпорация по управлению доменными именами и IP-адресами
IETF	Инженерный совет Интернета
ISO	Международная организация по стандартизации
LRA	Местный регистрационный центр (местный РЦ)
NAESB	Североамериканский совет по энергетическим стандартам
NCA	Компетентный национальный орган
NIST	(правительство США) Национальный институт стандартов и технологий
NTP	Протокол сетевого времени
OCSP	Протокол состояния сетевого сертификата
OID	Идентификатор объекта
PKI	Инфраструктура открытых ключей
PSP	Поставщик платежных услуг
QGIS	Квалифицированный источник государственной информации
QGTIS	Квалифицированный государственный источник налоговой информации
QIIS	Квалифицированный независимый источник информации
РЦ	Регистрационный центр
RFC	Request for Comments («Запрос на комментарии», серия официальных документов)
S/MIME	Безопасный MIME (Многоцелевые расширения интернет-почты)
SSCD	Устройство создания защищенной подписи
SSL	Уровень защищенных сокетов
TLD	Домен верхнего уровня
TLS	Безопасность транспортного уровня
НДС	Налог на добавленную стоимость
WEQ	Wholesale Electric Quadrant (серия официальных документов NAESB)
CP	Политика сертификации
CPS	Положение о сертификационной практике

СОС	Список отзыва сертификатов
МСЭ	Международный союз электросвязи
УЦ	Удостоверяющий центр

2.0 Ответственность за публикацию и репозитории

2.1 Репозитории

GlobalSign публикует в репозиториях все сертификаты УЦ и перекрестные сертификаты, данные об отзыве выпущенных сертификатов, CP, CPS и соглашения доверяющей стороны, а также соглашения с Абонентами. GlobalSign гарантирует, что данные об отзыве выпущенных сертификатов и ее корневых сертификатов доступны через репозиторий 24 часа в сутки, 7 дней в неделю с общей доступностью не менее 99% в год с запланированным временем простоя, не превышающим 0,5% в год.

GlobalSign может публиковать предоставленную информацию в общедоступных каталогах для предоставления информации о статусе сертификата.

GlobalSign воздерживается от публикации в открытом доступе конфиденциальной и/или секретной документации, включая средства контроля безопасности, операционные процедуры и внутренние политики безопасности. Однако эти документы предоставляются по мере необходимости квалифицированным аудиторам в ходе любого аудита WebTrust или ETSI в компании GlobalSign.

Веб-сайты и переводы данного CPS и другой общедоступной документации могут предоставляться компанией GlobalSign и/или компаниями группы в маркетинговых целях, однако репозитории всей общедоступной документации GlobalSign находятся по адресам www.globalsign.com/repository и www.globalsign.com/en/company/corporatepolicies, и в случае любого несоответствия преимущественную силу имеет версия на английском языке.

2.2 Публикация информации о сертификатах

GlobalSign публикует свои CP, CPS, соглашения с Абонентами и соглашения с доверяющими сторонами на сайте https://www.globalsign.com/repository. CP и CPS включают все материалы, требуемые RFC 3647, и структурированы в соответствии с RFC 3647. Списки СОС публикуются в онлайн-репозиториях. Они содержат записи обо всех отозванных непросроченных сертификатах с указанием их сроков действия, которые зависят от типа сертификата и/или положения сертификата в цепочке сертификатов.

GlobalSign размещает тестовые веб-страницы, чтобы поставщики прикладного ПО могли тестировать свои приложения с сертификатами Абонентов, которые подключаются ко всем публично доверенным корневым сертификатам. Ниже приведены тестовые веб-страницы для (i) действующих, (ii) отозванных и (iii) просроченных сертификатов.

Корень R1:

https://valid.r1.roots.globalsign.com
https://revoked.r1.roots.globalsign.com
https://expired.r1.roots.globalsign.com

Корень R3:

https://valid.r3.roots.globalsign.com
https://revoked.r3.roots.globalsign.com
https://expired.r3.roots.globalsign.com

Корень R5:

https://valid.r5.roots.globalsign.com
https://revoked.r5.roots.globalsign.com
https://expired.r5.roots.globalsign.com

Корень R6

https://valid.r6.roots.globalsign.com
https://revoked.r6.roots.globalsign.com
https://expired.r6.roots.globalsign.com

Корень R46

https://valid.r46.roots.globalsign.com
https://revoked.r46.roots.globalsign.com
https://expired.r46.roots.globalsign.com

Корень E46

https://valid.e46.roots.globalsign.com
https://revoked.e46.roots.globalsign.com
https://expired.e46.roots.globalsign.com

2.3 Время или частота публикации

Сертификаты УЦ публикуются в репозитории на страницах поддержки как можно скорее после выпуска.

GlobalSign пересматривает CP и CPS и вносит соответствующие изменения каждые 365 дней, чтобы работа GlobalSign оставалась точной, прозрачной и соответствовала внешним требованиям. GlobalSign внимательно следит за голосованиями CA/Browser Forum и обновлениями их Требований, своевременно внедряя обновления в свою работу. Новые или измененные версии CP, настоящего CPS, соглашений с Абонентами или соглашений с доверяющими сторонами публикуются в течение семи дней после цифровой подписи.

2.4 Контроль доступа к репозиториям

Репозиторий GlobalSign общедоступен только для чтения.

Для предотвращения добавления, удаления или изменения записей репозитория неавторизованными лицами применяются логические и физические меры безопасности.

3.0 Идентификация и аутентификация

GlobalSign выступает в качестве РЦ, проверяет и удостоверяет личность и другие атрибуты заявителя перед включением этих атрибутов в сертификат.

Заявителям запрещается использовать в сертификате имена, нарушающие права интеллектуальной собственности других лиц. GlobalSign не проверяет наличие у заявителя прав интеллектуальной собственности на имя, указанное в заявке на получение сертификата, а также не занимается арбитражем, посредничеством или иным разрешением споров, касающихся прав собственности на любое доменное имя, товарный знак, фирменное наименование или знак обслуживания. GlobalSign оставляет за собой право отклонить заявку из-за такого спора, не неся ответственности перед заявителем.

Регистрационные центры GlobalSign проверяют подлинность запросов сторон, желающих отозвать сертификаты.

3.1 Имена

3.1.1 Типы имен

Сертификаты GlobalSign выпускаются на отличительные имена (DN) субъекта, которые отвечают требованиям именования X.500, именования RFC-822 и именования X.400. Эти DN соблюдают уникальность пространства имен и не вводят в заблуждение. Некоторые сертификаты, такие как DV TLS, OV TLS и IntranetSSL SSL Common Names, могут также включать адреса RFC2460 (IP версии 6) или RFC791 (IP версии 4).

SSL-сертификаты Wildcard в качестве первого символа поля CN или SAN включают подстановочный знак, символ звездочки (*). Перед выдачей такого сертификата компания

GlobalSign, следуя передовому опыту, определяет, встречается ли символ подстановочного знака в первой позиции слева от «контролируемой реестром» метки или «публичного суффикса». (например, "*.com", "*.co.uk", для более подробного объяснения см. раздел 8.2 RFC 6454). Если это так и пространство доменных имен не принадлежит Абоненту или не контролируется им, то запрос отклоняется.

Для сертификатов S/MIME BR, если субъект:commonName сертификата, выданного физическому лицу, не содержит адрес почтового ящика, он указывается как личное имя или псевдоним, как описано в разделе 7.1.4.2.2(a). Допускаются имена, состоящие из нескольких слов. Имена, соединенные через дефис, считаются одним именем. Субъекты, имеющие более одного имени, могут выбрать одно или несколько своих имен в любой последовательности. Субъекты могут выбирать порядок расположения своих имен и фамилий в соответствии с национальными предпочтениями. GlobalSign допускает общепринятые варианты или сокращения личных имен в соответствии с локальной практикой.

3.1.2 Необходимость осмысленности имен

В случаях, когда продукт GlobalSign позволяет использовать ролевое или ведомственное имя, и если DN включает поле OU, то в DN можно добавить дополнительные уникальные элементы в поле OU, чтобы доверяющие стороны могли различать сертификаты с общими элементами.

Для сертификатов S/MIME BR личные имена должны представлять собой значимое представление имени Субъекта, подтвержденное идентификационной документацией или записями Enterprise РЦ.

3.1.3 Анонимность или псевдонимность Абонентов

Если это не запрещено соответствующими нормами и, по возможности, сохраняется уникальность пространства имен, GlobalSign может выпускать анонимные или псевдонимные сертификаты конечных субъектов. GlobalSign оставляет за собой право раскрывать личность Абонента, если это требуется по закону. Запросы на интернационализированные доменные имена (IDN) в сертификатах будут помечены для дополнительной ручной проверки. Расшифрованное имя хоста подвергнут дополнительной проверке, чтобы снизить риск фишинга и других мошеннических действий, и оно может быть сопоставлено с ранее отклоненными запросами на сертификат или отозванными сертификатами. GlobalSign может отклонять заявки на основании критериев снижения риска, например, имена с риском фишинга или другое мошенническое использование, включенные в списки Google Safe Browsing или включенные в базу данных, которую ведет Рабочая группа по борьбе с фишингом.

GlobalSign разрешает использование псевдонимов для сертификатов S/MIME в соответствии с разделом 3.1.3 GlobalSign CP.

3.1.4 Правила интерпретации различных форм имен

Отличительные имена в сертификатах интерпретируются с использованием стандартов X.500 и синтаксиса ASN.1. См. RFC 2253 и RFC 2616 для дополнительной информации о том, как отличительные имена X.500 в сертификатах интерпретируются в качестве унифицированных идентификаторов ресурсов и HTTP-ссылок.

GlobalSign не выполняет замену символов, отличных от ascii, в сертификатах S/MIME BR.

3.1.5 Уникальность имен

GlobalSign включает в сертификат различные атрибуты субъекта для обеспечения уникальности субъекта

3.1.6 Признание, аутентификация и значение товарных знаков

Абоненты не могут запрашивать сертификаты с содержанием, нарушающим права интеллектуальной собственности третьей стороны. GlobalSign не требует проверки права заявителя на использование товарного знака. GlobalSign оставляет за собой право отозвать любой сертификат, вовлеченный в спор.

3.2 Первоначальная проверка

GlobalSign может проводить идентификацию заявителя или проверку для сервисов, включая услуги цепочки УЦ, используя любые законные средства связи или расследования, необходимые для идентификации юридического или физического лица.

GlobalSign использует результаты первоначальной проверки для альтернативных предложений продуктов путем комбинирования элементов ранее проверенной информации с новой проверенной информацией. Учетная запись клиента используется для подтверждения подлинности использования любой ранее проверенной информации для повторных заявителей при условии соблюдения владельцем учетной записи требований повторной проверки, изложенных в разделе 3.3.1.

3.2.1 Метод доказательства владения закрытым ключом

Не предусмотрено.

3.2.2 Аутентификация организации

GlobalSign поддерживает внутреннюю политику и процедуры, которые регулярно пересматриваются с целью соблюдения требований различных корневых программ, участником которых является GlobalSign, а также Базовых требований CA/Browser.

Для всех сертификатов, включающих идентификатор организации, заявители должны предоставить название организации и ее зарегистрированный или торговый адрес. Для всех сертификатов, включающих идентификатор организации, GlobalSign проверяет факт юридического существования, юридическое название, вымышленное название (если применимо), организационно-правовую форму (если она включена в запрос или является частью юридического названия в юрисдикции регистрации), запрашиваемый адрес организации и надежный метод связи. При расширенной проверке GlobalSign дополнительно проверяет физическое существование, ведение деятельности и, если это требуется для выполнения дополнительных шагов проверки, надежные средства связи.

Эта информация может быть проверена с помощью одного из следующих методов:

- Государственный орган (QTIS или QGIS, включая учредительное или регистрационное агентство) в юрисдикции заявителя или вышестоящий руководящий государственный орган, если сам заявитель является государственной организацией.
- QIIS.
- Заверенное юридическое заключение или заверенное письмо бухгалтера.
- Независимое подтверждение от заявителя.

Кроме того, для сертификатов без расширенной проверки компания GlobalSign может проверить информацию, используя один из следующих надежных источников данных:

- Письмо, подтверждающее правильность информации от субъекта проверки, написанное бухгалтером, юристом, государственным чиновником или другой надежной третьей стороной, на которую обычно полагаются при получении такой информации.
- Счет за коммунальные услуги, выписка из банковского счета, выписка с кредитной карты, налоговый документ, выданный правительством, или другая форма идентификации, которая была определена GlobalSign как достаточно точная и надежная, если такие документы признаны надежными среди коммерческих предприятий, государством и созданы третьей стороной с целью, отличной от получения заявителем сертификата.
- База данных третьей стороны, созданная третьей стороной с целью, отличной от получения заявителем сертификата, признанная надежной среди коммерческих предприятий и государственных организаций, которая периодически обновляется. База данных третьей стороны оценивается компанией GlobalSign на предмет ее надежности, точности и устойчивости к изменениям или фальсификации.

Эти методы проверки используются в соответствии с отраслевыми стандартами. Не все методы будут приемлемы во всех обстоятельствах или доступны для использования для всех типов информации.

Список учредительных или регистрационных агентств опубликован в юридическом репозитории на веб-сайте GlobalSign (globalsign.com) в разделе «Ресурсы проверки».

Полномочия заявителя запрашивать сертификат от имени организации проверяются в соответствии с разделом 3.2.5 ниже.

3.2.2.1 Аутентификация местного регистрационного центра

Соответствующим образом аутентифицированные администраторы учетных записей, действующие в качестве местного регистрационного центра (LRA), аутентифицируют лиц, связанных с организацией и/или любыми поддоменами, принадлежащими или контролируемыми организацией. *(Хотя LRA по контракту имеют право аутентифицировать лиц, подлежащие аутентификации домены все равно должны быть предварительно проверены GlobalSign).*

3.2.2.2 Аутентификация сертификата на основе должностей (DepartmentSign)

GlobalSign обеспечивает проверку подлинности запросов на получение сертификатов на основе машин, устройств, отделов или должностей. Местные РЦ по договору обязаны обеспечить точность и правильность имен машин, устройств, отделов или должностей, относящихся к профилю организации и ее бизнесу.

3.2.2.3 Сертификаты S/MIME BR

Информация о заявителе включает в себя следующее:
• Официальное наименование юридического лица;
• Зарегистрированное предполагаемое имя юридического лица (необязательно).
• Организационное подразделение юридического лица (по желанию);
• Адрес юридического лица;
• Идентификатор организации, состоящий из соответствующего идентификатора схемы регистрации, двухзначного кода страны по ISO 3166 для страны, в которой действует схема («XG» должен использоваться, когда схема работает во всем мире), где это применимо, идентификатора ISO 3166-2 для подразделения страны, в которой действует Схема регистрации, и, где применимо, регистрационный номер, присвоенный в соответствии с установленной схемой регистрации.

GlobalSign проверяет информацию Заявителя, используя как минимум один из следующих методов:
• Государственный орган в юрисдикции места создания, существования или признания юридического лица;
• Ссылка на данные идентификатора юридического лица (LEI). В этом случае GlobalSign проверяет, что статус регистрации — ВЫДАНО, а статус EntityStatus — АКТИВЕН. GlobalSign разрешает использование LEI только в том случае, если запись ValidationSources имеет значение FULLY_CORROBORATED;
• Посещение объекта центром сертификации или третьей стороной, выступающей в качестве агента центра сертификации; или
• Аттестация, включающая копию подтверждающей документации, используемой для подтверждения юридического существования заявителя, такой как свидетельство о регистрации, учредительный договор, операционное соглашение, устав или нормативный акт.

GlobalSign использует следующие схемы регистрации:
• NTR: для идентификатора, присвоенного национальным или государственным торговым реестром юридическому лицу, указанному в теме:имя организации.
• НДС: для идентификатора, присвоенного национальными налоговыми органами юридическому лицу, указанному в теме:название организации.
• LEI: для идентификатора юридического лица, указанного в ISO 17442, для объекта, указанного в теме:имяорганизации. Двухзначный код страны по стандарту ISO 3166 должен быть установлен на «XG».

• Правительство: для государственных учреждений.
• INT: для некоммерческих организаций. Двухзначный код страны по стандарту ISO 3166 должен быть установлен на «XG».

GlobalSign проверяет предполагаемые Nnames, проверяя, что:
• Заявитель зарегистрировал использование предполагаемого имени в соответствующем государственном органе для подачи такой документации в юрисдикции его учреждения или регистрации; и
• Заявление о предполагаемом имени остается действительным.

GlobalSign может полагаться на подтверждение, в котором указано Предполагаемое имя, под которым Заявитель ведет бизнес, правительственный орган, в котором зарегистрировано Предполагаемое имя, и что такая регистрация остается действительной.

3.2.2.4 Квалифицированные сертификаты

GlobalSign выпускает три типа квалифицированных сертификатов, которые включают идентификационные данные организации:

- Квалифицированные сертификаты для электронных печатей, которые удостоверяют организацию.
- Квалифицированные сертификаты для электронных подписей, которые подтверждают принадлежность физического лица к организации.
- Квалифицированные сертификаты аутентификации веб-сайта.

Для всех квалифицированных сертификатов, включающих идентификацию организации, заявители должны указать полное юридическое название организации (включая организационно-правовую форму) и адрес физического местонахождения субъекта предпринимательской деятельности.

GlobalSign проверяет юридическое существование и адрес по следующим документам:

- официальные государственные записи в квалифицированных государственных источниках информации;
- документы, предоставленные или подтвержденные государственным органом в юрисдикции создания, существования или признания организации;
- записи, предоставленные квалифицированным независимым источником информации.

Кроме того, GlobalSign может проверить адрес по следующим документам:

- подтвержденное юридическое заключение или письмо бухгалтера; или подтверждение физического местонахождения, подписанное с использованием действительной квалифицированной электронной печати организации.

Информация в документе должна соответствовать содержанию квалифицированного сертификата.

В квалифицированный сертификат можно включить полное юридическое название организации, осуществляющей предпринимательскую деятельность (торговое наименование или торговое имя). GlobalSign проверит, что организация зарегистрировала в соответствующем государственном органе по своему местонахождению каждое из названий, включенных в сертификат, и что запись действительна в данный момент.

GlobalSign проверяет принадлежность физического лица к организации по одному из следующих документов:

- подтверждение от организации, полученное по проверенному методу связи;
- независимое подтверждение от организации;
- заверенное заключение или заверенное письмо бухгалтера-аудитора;
- заверение, подписанное с использованием действительной квалифицированной электронной печати организации;

- заверение от корректно аутентифицированного администратора учетной записи, действующего в качестве местного регистрационного центра.

Для квалифицированных сертификатов организации или веб-сайта компания GlobalSign проверяет личность и полномочия уполномоченного представителя (представителей) организации.

GlobalSign проверяет полномочия уполномоченного представителя (представителей) организации по одному из следующих документов:

- официальные государственные записи в квалифицированных государственных источниках информации;
- документы или подтверждение от государственного органа по месту регистрации или ведения бизнеса организации;
- записи из квалифицированного независимого источника информации;
- заверенное заключение или заверенное письмо бухгалтера-аудитора;
- заверение, подписанное действительной квалифицированной электронной печатью организации. Информация в документе должна соответствовать содержанию квалифицированного сертификата.

GlobalSign проверит личность уполномоченного представителя в соответствии с разделом 3.2.3.

GlobalSign может подписывать сертификаты своих аффилированных компаний и лиц, связанных с этими компаниями (в качестве субъекта). Аффилированные компании включают материнские и дочерние компании GlobalSign, а также другие компании, у которых общая материнская компания с GlobalSign.

Для всех специфичных атрибутов PSD2 проверяется информация из компетентных национальных органов, включая государственный реестр, реестры Европейского банковского ведомства и аутентифицированные сообщения от национального компетентного органа.

Когда GlobalSign получает уведомление, что в новом сертификате указан адрес электронной почты для информирования компетентных национальных органов, то направляет на этот адрес обычным текстом информацию о содержании сертификата, включая его серийный номер в шестнадцатеричном формате, отличительное имя субъекта, отличительное имя эмитента, срок действия сертификата, контактную информацию, инструкции для запросов об отзыве и копию файла сертификата.

3.2.3 Проверка физического лица

GlobalSign проверяет физических лиц в зависимости от класса сертификата, как указано ниже.

3.2.3.1 Класс 1

Заявитель должен продемонстрировать контроль над своим адресом электронной почты или доменным именем, к которому относится сертификат. GlobalSign не проверяет подлинность дополнительной информации/атрибутов, которые могут быть предоставлены заявителем в процессе подачи заявления и регистрации. Это относится к сертификатам DV.

Для домена SSL заявитель должен продемонстрировать контроль над всеми доменными именами, которые включаются в сертификат.

3.2.3.2 Класс 2

Заявитель должен подтвердить определенные атрибуты, включенные в запрос, такие как адрес электронной почты или доменное имя, к которому относится сертификат, если они включены в запрос на сертификат. Это относится к сертификатам OV.

Для сертификатов Organization Validation SSL заявитель должен продемонстрировать контроль над всеми доменными именами, которые включаются в сертификат.

От заявителя может потребоваться предоставить разборчивую копию паспорта или удостоверения личности с фотографией (водительские права, военный билет или эквивалент). Для дополнительного подтверждения может потребоваться дополнительный документ, выданный не государственными органами. GlobalSign до достаточной степени уверенности проверяет, что копия удостоверения личности соответствует запрашиваемому имени и что верно указаны другие данные субъекта, такие как страна, регион и населенный пункт.

GlobalSign также может проверить личность заявителя одним из следующих методов:

- Телефонный вызов/ответ с использованием телефонного номера из надежного источника.
- Вызов/ответ по факсу с использованием номера факса из надежного источника.
- Вызов/ответ по адресу электронной почты, полученному из надежного источника.
- Почтовый вызов по почтовому адресу, полученному из надежного источника.
- К любому заявлению в письменной форме прилагается оттиск печати заявителя (в юрисдикциях, допускающих их использование для подписи документов).

Документы для AATL указаны ниже. Обратите внимание, что они используются и для других продуктов класса 2:

- Заверение от соответствующего нотариуса или доверенной третьей стороны о том, что они проверили личность физического лица по удостоверению государственного образца.
- Для физических лиц, связанных с организацией, нужно предоставить заполненное заявление об удостоверении личности, включающее минимум один уникальный биометрический идентификатор (например, отпечаток пальца или собственноручную подпись). В этом оформленном заявлении уполномоченный представитель организации, указанной в сертификате, подтверждает, что видел физическое лицо, просмотрел его удостоверение личности с фотографией, а информация о личности физического лица в запросе на сертификат соответствует информации в удостоверении. GlobalSign подтверждает подлинность документа непосредственно у уполномоченного представителя организации, используя контактную информацию, подтвержденную с помощью квалифицированного независимого источника информации, квалифицированного государственного источника информации или любым другим способом в соответствии с Руководством EV. Полномочия уполномоченного представителя представлять организацию также подтверждаются в соответствии с Руководством EV.
- При проверке физических лиц, связанных с организацией, GlobalSign может полагаться на заверения утвержденного местного РЦ. Для запросов сертификатов класса 2 через EPKI или MSSL см. пункт 3.2.3.5.
- Заверение от организации, которая проверяет личность собственных клиентов по удостоверениям государственного образца и сохраняет защищенные записи таких проверок, доступные для аудита.
- Другие методы проверки по списку для квалифицированного сертификата.

Для сертификатов AATL компания GlobalSign может установить личность физического лица и провести проверку удостоверения личности государственного образца с помощью видеовстречи или метода аналогичной надежности.

GlobalSign может запросить у заявителя дополнительную информацию. Для достижения эквивалентного уровня надежности может использоваться другая информация и методы.

Если в запрос на сертификат включается адрес электронной почты, GlobalSign или местный РЦ должны проверить его действительность и принадлежность.

3.2.3.3 Класс 3

Для сертификатов подписи кода с расширенной проверкой (EV) заявитель должен продемонстрировать контроль над каждым адресом электронной почты, который включается в сертификат.

Для сертификатов SSL с расширенной проверкой заявитель должен продемонстрировать контроль над всеми доменными именами, которые включаются в сертификат.

Заявитель должен представить разборчивую копию действительного паспорта или другого удостоверения личности государственного образца с фотографией (водительские права, военный билет или эквивалент). Для дополнительного подтверждения может потребоваться соответствующий негосударственный документ или удостоверение личности с фотографией. GlobalSign или доверенная третья сторона с достаточной степенью уверенности сверяет по копии документа имя и другие данные субъекта, такие как страна, регион и населенный пункт.

Если местным законодательством или нормативными актами запрещено предоставлять копии паспорта или удостоверения личности с фотографией, то GlobalSign принимает подтверждение или документацию от доверенной третьей стороны, уполномоченной проводить проверку личности.

Уровень PersonalSign 3 требует личной встречи. Нотариус или доверенная третья сторона должны подтвердить, что они встретились с физическим лицом и проверили его паспорт с фотографией, и данные верны. GlobalSign может установить личность физического лица и проверить паспорт на видеовстрече или другим методом с эквивалентным уровнем надежности.

Заявитель также обязан продемонстрировать контроль над всеми адресами электронной почты, который включат в сертификат.

Также GlobalSign проверяет полномочия заявителя представлять организацию-субъекта в сертификате. Проверка производится через надежные средства связи в соответствии с Руководством по EV и Базовыми требованиями к подписи кода.

GlobalSign может запросить у заявителя или его организации дополнительную информацию. Для достижения эквивалентного уровня надежности может использоваться другая информация и методы.

3.2.3.4 Сертификаты S/MIME BR

Информация о заявителе включает в себя следующее:
1. Имя(а) и фамилия(я), которые должны быть настоящими именами;
2. Псевдоним (если используется);
3. Должность (если используется); и
4. Дополнительная информация, необходимая для однозначной идентификации заявителя.
GlobalSign должна проверить личность индивидуального заявителя и информацию об атрибутах личности, используя хотя бы один из следующих методов:

• Для сбора идентификационных данных и атрибутов личности заявителя:
o Использование для целей идентификации официального документа, удостоверяющего личность, выданного Заявителю соответствующим государственным органом в юрисдикции Заявителя, содержащего фотографию и/или другую (биометрическую) информацию, которую можно сравнить с внешним видом Заявителя. Примеры включают, помимо прочего, паспорта, удостоверения личности, водительские права и военные билеты. (S/MIME BR, раздел 3.2.4.1 (1)); или
o Использование цифрового или электронного документа, удостоверяющего личность, который считается документом, удостоверяющим личность электронного МСПД, согласно стандарту ICAO 9303, часть 10 (S/MIME BR, раздел 3.2.4.1 (2)); или

o Использование действующего eID, выданного в рамках «уведомленных» схем eID в соответствии со статьей 9 Регламента eIDAS, и eID должен соответствовать LoA eIDAS «Значительный» или «Высокий» (S/MIME BR, раздел 3.2.4.1 (3)); или
o Использование запроса на сертификат, подписанного действительной цифровой подписью, на основе действительного личного сертификата, выданного в соответствии с утвержденной структурой, описанной в S/MIME BR (раздел 3.2.4.1 (4) S/MIME BR) и 3.2.4.2 (4));; или
o Только для сертификатов, подтвержденных спонсором, с использованием записей Enterprise РЦ (S/MIME BR, раздел 3.2.4.1 (5)).
o Полномочия или принадлежность физического лица, представляющего организацию, должны быть включены в тему:название организации сертификата с использованием аттестации, предоставленной организацией (S/MIME BR, раздел 3.2.4.1 (6))

• Для проверки идентификационных данных заявителя:
o Все атрибуты личности: с использованием аттестации квалифицированного практикующего юриста или нотариуса в юрисдикции заявителя. GlobalSign подтверждает, что Аттестация была написана бухгалтером, юристом, государственным должностным лицом или другой надежной третьей стороной в юрисдикции заявителя, на которую обычно полагаются для получения такой информации. Аттестация включает копию документации, подтверждающей факт, подлежащий удостоверению. GlobalSign использует надежный метод связи для связи с отправителем и подтверждения подлинности подтверждения (S/MIME BR, раздел 3.2.4.1 (7))

GlobalSign обязуется проверять дополнительные доказательства, используя авторизованные источники, такие как дополнительные официальные документы, правительственные или нормативные реестры или национальные реестры населения (S/MIME BR, раздел 3.2.4.1 (8)). Прежде чем полагаться на источник проверочных данных, GlobalSign проверяет его пригодность в качестве надежного источника данных.

Что касается валидации, применяются следующие методы:

Любой документ, удостоверяющий личность, должен быть представлен в его оригинальной форме. GlobalSign использует процедуры, гарантирующие, что доказательства, представленные заявителем, являются подлинным документом, удостоверяющим личность, который не является поддельным или фальсифицированным/модифицированным. При использовании удаленного процесса этот процесс гарантирует, что заявитель имеет документ под рукой и представляет его в режиме реального времени перед камерой. GlobalSign поддерживает внутренний авторитетный источник информации, который охватывает документы, принятые GlobalSign, их внешний вид и способы проверки этих документов. (S/MIME BR, раздел 3.2.4.2 (1))

Для документов, удостоверяющих личность, GlobalSign проверяет, успешно ли подтверждена цифровая подпись эмитента на документе в соответствии со стандартом ICAO 9303, часть 11. (S/MIME BR, раздел 3.2.4.2 (2))

Как для физических, так и для цифровых документов, удостоверяющих личность, GlobalSign может использовать ручные (личные) или дистанционные процедуры или их комбинацию. GlobalSign записывает следующую информацию: эмитент, срок действия и уникальный идентификационный номер документа. Чтобы убедиться, что личность заявителя подтверждена, GlobalSign визуально сравнивает внешний вид заявителя и фотографию лица и/или другую информацию в физическом или цифровом документе, удостоверяющем личность. (S/MIME BR, раздел 3.2.4.2 (1) и 3.2.4.2 (2))

Для аутентификации с использованием eID проверка с помощью поставщика удостоверений eID (IdP) документируется и сохраняется. (S/MIME BR, раздел 3.2.4.2 (3))

3.2.3.5 Квалифицированные сертификаты

GlobalSign проверяет личность Абонентов в соответствии со статьей 24.1 Регламента eIDAS/UK eIDAS, в частности, используя следующие методы:

- Проверка при личном присутствии
- Использование электронных средств идентификации
- Использование квалифицированной электронной подписи

- Видеоверификация

3.2.3.5.1 Личная проверка

Личная проверка требует физического присутствия абонента и предъявления следующих документов:

- Удостоверение государственного образца с фотографией
- Подписанное заявление

Внешность физического лица сравнивается с фотографией на удостоверении личности, проверяются защитные элементы документа. Подпись на личном заявлении сравнивается с подписью на удостоверении личности с фотографией.

Данная проверка может быть выполнена сторонним специалистом.

Для проверки уникальности личности заявителя или для подтверждения другой информации, кроме имени и фамилии, могут потребоваться дополнительные доказательства.

3.2.3.5.2 Использование удаленных электронных средств идентификации

Для проверки личности GlobalSign может использовать электронные средства идентификации, имеющие уровень надежности «Существенный» или «Высокий», как указано в статье 8 Регламента eIDAS. Перед выдачей удостоверяется физическое присутствие человека.

1. Для нотифицированных электронных схем идентификации уровень заверения определяется уведомлением, направляемым государством-членом в Комиссию.
2. Для ненотифицированных электронных средств идентификации уровень заверения определяется в соответствии с факторами, описанными Европейской комиссией. После проверки органом по оценке соответствия компания GlobalSign представит результаты проверки надзорному органу, прежде чем принять это средство идентификации.

3.2.3.5.3 Квалифицированная электронная подпись

Для проверки личности заявителя и дополнительных атрибутов в сертификате GlobalSign принимает действительную квалифицированную электронную подпись Абонента на личном заявлении. Сертификат должен быть выдан в соответствии со статьей 24 (a) или (b) Регламента eIDAS/UK eIDAS.

3.2.3.5.4 Видеоверификация

GlobalSign может использовать видеоверификацию. Аналогично личной верификации, от Абонента потребуется предоставить следующие документы:

- Удостоверение государственного образца с фотографией
- Заявление с (электронной) подписью

Для проверки уникальности личности заявителя или для подтверждения другой информации, кроме имени, могут потребоваться дополнительные доказательства.

Внешность физического лица сравнивается с фотографией на удостоверении личности, проверяются защитные элементы документа. Подпись на личном заявлении сравнивается с подписью на удостоверении личности с фотографией. Этот метод требует, чтобы у абонента было устройство с выходом в интернет, веб-камера или другое видеооборудование, а также работающий микрофон и звуковая система.

3.2.3.6 Аутентификация местного регистрационного центра

Для организаций, допускающих концепцию местного РЦ, GlobalSign устанавливает профили. Сертификаты, выданные в рамках этих учетных записей, заполняются полями данных из профиля. Организация по договору обязана аутентифицировать лиц, связанных с организацией.

3.2.3.7 Сертификаты Североамериканского совета по энергетическим стандартам (NAESB)

Запросы на проверку личности организации для сертификатов NAESB на имя аффилированной организации должны включать название организации, адрес и документальное подтверждение существования организации. GlobalSign или РЦ проверят эту информацию, подлинность представителя запрашивающей организации и его полномочия действовать от ее имени. Конечные организации, использующие сертификаты для приложений WEQ-012, обязаны зарегистрировать свое юридическое название и получить «Код организации». Его опубликуют в NAESB EIR и будут использовать во всех заявках Абонентов, поданных этой организацией, и выданных ей сертификатах. При выдаче сертификатов для использования в энергетической отрасли для других приложений, кроме WEQ-012, уполномоченные удостоверяющие центры NAESB должны соблюдать положения стандартов и моделей деловой практики инфраструктуры открытого ключа NAESB WEQ-012, за исключением положений WEQ-012-1.9.1, WEQ-012-1.3.3 и WEQ-012-1.4.3, которые требуют регистрации конечной организации в NAESB EIR.

GlobalSign может самостоятельно выполнять некоторые/все функции РЦ или делегировать их отдельным юрлицам через одну из своих платформ управляемых услуг. В обоих случаях на РЦ распространяются все обязательства по проверке личности, аудиту, регистрации, защите информации абонента, хранению записей и другие аспекты, связанные с функцией РЦ, изложенные в настоящем CPS, Спецификации аккредитации NAESB и Стандартах деловой практики NAESB. Вся инфраструктура и операции УЦ должны соответствовать этим требованиям во время выполнения функций/операций РЦ. Уполномоченный центр сертификации и/или делегированная организация несут ответственность за обеспечение того, чтобы все стороны, выполняющие функции РЦ, понимали и соглашались соблюдать Спецификацию аккредитации NAESB.

Для своих абонентов компания GlobalSign и/или связанные с ней РЦ должны обеспечить проверку идентификационной информации заявителя в соответствии с процессом, установленным в CP и CPS. Процесс зависит от уровня заверения сертификата и рассматривается в Спецификации аккредитации NAESB. Требования к документам и проверке варьируются в зависимости от уровня заверения.

Требования к проверке личности по уровням заверения NIST и NAESB соответствуют следующим образом:

Уровень заверения NIST	Уровень заверения NAESB
Уровень 1	Рудиментарный
Уровень 2	Базовый
Уровень 3	Средний

GlobalSign или назначенный им РЦ (в случае EPKI) должен проверить всю предоставленную заявителем идентификационную информацию в соответствии с требованиями к аутентификации, определенными с Процессом подтверждения личности, описанным в разделе 2.2.2 «Аутентификация Абонентов» Требований NAESB к аккредитации уполномоченных центров сертификации.

3.2.4 Непроверенная информация абонента

GlobalSign не проверяет содержимое поля Subject:OrganizationalUnitName, за исключением публично доверенных сертификатов SSL и сертификатов подписи кода, в которых поле Subject:OrganizationalUnitName содержит имя, DBA, торговую марку, товарный знак, адрес, местоположение или другой текст, относящийся к конкретному физическому или юридическому лицу.

Если это допускается отраслевыми стандартами, GlobalSign может разрешить размещение непроверенной информации Абонента в поле Subject:SerialNumber.

Для сертификатов IntranetSSL компания GlobalSign принимает у заявителя без проверки информацию для включения в поле subjectAlternativeName, в том числе внутренние или непубличные имена DNS, имена хостов и IP-адреса RFC 1918.

Для сертификатов S/MIME BR информация об Абоненте, которая не была проверена в соответствии с базовыми требованиями для S/MIME, не будет включена в сертификат.

3.2.5 Проверка полномочий

Сертификаты PersonalSign1	Проверка, что заявитель контролирует адрес электронной почты, указанный в сертификате, путем ответа на вызов.
Сертификаты PersonalSignDemo	Проверка, что заявитель контролирует адрес электронной почты, указанный в сертификате.
Сертификаты PersonalSign2	Проверка через надежное средство связи вместе с заявителем, что он контролирует адрес электронной почты, указанный в сертификате.
Сертификаты NAESB	Проверка через надежное средство связи вместе с организацией или отдельным заявителем, что он контролирует все адреса электронной почты, указанные в сертификате (см. раздел 3.2.3.5).
PersonalSign2 Pro	Проверка отдельного заявителя вместе с подтверждением того, что заявитель контролирует указанный адрес электронной почты, если это необходимо. Кроме того, проверка того, что Представитель заявителя имеет полномочия и разрешение на выполнение одного или нескольких из следующих действий: запросить выдачу или отзыв сертификатов; или возлагать ответственность на других, чтобы те выполняли эти роли. Для сертификатов, выданных через учетную запись EPKI, полномочия представителя заявителя действовать в качестве РЦ предприятия будут проверены во время настройки профиля.
Сертификаты PersonalSign2 Department	Проверка через надежное средство связи вместе с заявителем, что он контролирует адрес электронной почты, если тот включается в сертификат. Для сертификатов, выданных через учетную запись EPKI, полномочия представителя заявителя действовать в качестве РЦ предприятия будут проверены во время настройки профиля.
Сертификаты PersonalSign3	Проверка через надежное средство связи, что заявитель представляет данную организацию. Обязательна явка в соответствующий орган регистрации для личного подтверждения полномочий заявителя вместе с проверкой, что заявитель контролирует адрес электронной почты, указанный в сертификате.
Сертификаты S/MIME	Проверка с помощью надежных средств связи с организацией или отдельным заявителем, а также проверка того, что заявитель контролирует любой указанный адрес электронной почты. Кроме того, проверка того, что Представитель заявителя имеет полномочия и разрешение на выполнение одного или нескольких из следующих действий: запросить выдачу или отзыв сертификатов; или возлагать ответственность на других, чтобы те выполняли эти роли. Для сертификатов, выданных через учетную запись EPKI, полномочия представителя заявителя действовать в качестве РЦ предприятия будут проверены во время настройки профиля.
Сертификаты S/MIME BR	Проверка в соответствии с базовыми требованиями для S/MIME.

Сертификаты подписи кода	Проверка через надежное средство связи вместе с организацией или отдельным заявителем, что он контролирует все адреса электронной почты, которые могут быть по желанию указаны в сертификате.
Сертификаты подписи кода EV	Проверка полномочий лица, подписавшего договор, и лица, утвердившего сертификат, в соответствии с Руководством EV и Базовыми требованиями к подписи кода.
Сертификаты DV/AlphaSSL	Проверка прав собственности или контроля над доменным именем осуществляется одним из методов, определенных в разделе 3.2.7.
Сертификаты OV SSL	Проверка через надежное средство связи вместе с организацией или отдельным заявителем, что он контролирует доменное имя, с помощью методов, перечисленных в разделе 3.2.7. Для сертификатов, выпущенных через учетную запись MSSL, во время настройки профиля проверяются полномочия местного регистрационного центра.
Сертификаты EV SSL	Проверка полномочий лица, подписавшего контракт, и лица, утвердившего сертификат, в соответствии с Руководством EV, а также проверка наличия у заявителя права собственности или контроля над доменным именем с помощью методов, перечисленных в разделе 3.2.7. Для сертификатов, выпущенных через учетную запись MSSL, во время настройки профиля проверяются полномочия местного регистрационного центра.
Сертификаты меток времени	Верификация через надежное средство связи вместе с заявителем организации.
AATL	Верификация через надежные средства связи вместе с организацией или отдельным заявителем с проверкой, что заявитель контролирует адрес электронной почты, если тот включается в сертификат. Для сертификатов, выпущенных через учетную запись EPKI, во время настройки профиля проверяются полномочия местного регистрационного центра.
Квалифицированные сертификаты для аутентификации веб-сайтов	Проверка полномочий лица, подписавшего договор или подтвердившего сертификат, и уполномоченного представителя в соответствии с методами в разделе 3.2.2.3, а также проверка того, что заявитель владеет или контролирует доменное имя, с помощью методов в разделе 3.2.7.
Квалифицированные сертификаты для электронных печатей	Проверка полномочий лица, подписавшего договор или подтвердившего сертификат, и уполномоченного представителя в соответствии с методами в разделе 3.2.2.3.
Квалифицированные сертификаты для электронных подписей	Проверка подлинности запроса заявителя в соответствии с методами в разделе 3.2.3.4.

Кроме любого надежного средства связи, полномочия организации могут быть подтверждены с помощью:

- усовершенствованной (или выше) электронной печати, включающей название организации, ее материнской, дочерней или аффилированной компании;
- усовершенствованной (или выше) электронной подписи, включающей наименование организации, ее материнской, дочерней или аффилированной компании. В этом случае GlobalSign проверит, что подписавшее лицо надлежащим образом проверено как сотрудник или агент организации, указанной в сертификате;

- усовершенствованной (или выше) электронной подписи подтвержденного сотрудника или агента организации.

3.2.6 Критерии взаимодействия

Кросс-сертификаты публикуются в репозитории GlobalSign.

3.2.7 Проверка доменных имен

Для всех SSL-сертификатов GlobalSign проверяет владение или контроль заявителем (или материнской компанией заявителя, дочерней компании, филиала, именуемых «заявителями» для целей данного раздела) всех запрашиваемых FQDN одним из следующих методов:

1. Отправка контакту домена по электронной почте случайного значения, а затем получение подтверждающего ответ с использованием этого случайного значения. (Базовые требования TLS, раздел 3.2.2.4.2).
2. Отправка случайного значение на адрес электронной почты, созданный путем добавления 'admin', 'administrator', 'webmaster', 'admin', 'administrator', 'hostmaster' или 'postmaster' в локальной части, за которым следует знак "at" ("@"), а затем авторизационное доменное имя, и получение ответа с использованием случайного значения (BR, раздел 3.2.2.4.4).
3. Подтверждение наличия случайного значения в записи DNS CNAME или TXT авторизационного доменного имени (TLS BR, раздел 3.2.2.4.7).
4. Отправка случайного значения на адрес электронной почты контактного лица, указанному в поле DNS CAA. Соответствующий набор записей CAA ДОЛЖЕН быть доступен для алгоритма поиска, определенного в разделе 3 RFC 8659 (TLS BR, раздел 3.2.2.4.13).
5. Отправка по электронной почте случайного значения на адрес электронной почты, указанный в записи DNS TXT Record Email Contact, а затем получение подтверждения с использованием этого случайного значения (TLS BR, раздел 3.2.2.4.14).
6. Звонок на номер телефона контактного лица домена и получение ответа, подтверждающего запрос (TLS BR, раздел 3.2.2.4.15).
7. Звонок на номер телефона, указанный в поле DNS TXT Record Phone Contact и получение ответа для подтверждения ADN (BR, раздел 3.2.2.4.16).
8. Наличие случайного значения в файле в каталоге "/.well-known/pki-validation" на авторизованном доменном имени, доступном УЦ по HTTP/HTTPS через авторизованный порт (TLS BR, раздел 3.2.2.4.18).
9. Заявитель демонстрирует контроль над FQDN с помощью метода ACME HTTP Challenge, определенного в разделе 8.3 RFC 8555 (TLS BR, раздел 3.2.2.4.19).

Для проверки FQDN с подстановочным символом (wildcard) GlobalSign использует вышеуказанные методы, за исключением метода 9 (TLS BR, 3.2.2.4.18) и метода 10 (TLS BR, 3.2.2.2.4.19). Редиректы поддерживаются методами 9 (TLS BR, 3.2.2.4.18 и 10 (TLS BR, 3.2.2.4.19).

3.2.7.1 Записи CAA

В публично доверенных SSL-сертификатах GlobalSign проверяет FQDN каждого сервера по CAA-записям домена. Доменом эмитента CAA компании GlobalSign является "globalsign.com". Если существует запись CAA, в которой globalsign.com не указан как авторизованный УЦ, GlobalSign не будет выдавать сертификат. GlobalSign:

- кэширует записи CAA для повторного использования на срок до 8 часов
- поддерживает метки CAA issue и issuewild
- обрабатывает, но не действует по тегу свойства iodef, т.е. GlobalSign не отправляет сообщения о таких запросах на выдачу сертификата контакту(ам), указанному(ым) в записи(ях) CAA iodef
- не поддерживает никаких дополнительных тегов свойств

3.2.8 Проверка IP-адресов

Для проверки контроля IP-адресов или права на их использование GlobalSign использует следующие методы:

1. Подтверждение наличия случайного значения в файле в каталоге "/.well-known/pki-validation", который доступен УЦ по HTTP/HTTPS на авторизованном порту (TLS BR, раздел 3.2.2.5.1).
2. Отправка случайного значения по электронной почте контактному лицу для IP-адреса и получение подтверждающего ответа с использованием этого случайного значения (TLS BR, раздел 3.2.2.5.2).
3. Обратный поиск IP-адреса, а затем проверка контроля над полученным доменным именем с помощью одного из вариантов, перечисленных в разделе 3.2.7.1 (TLS BR, раздел 3.2.2.5.3).
4. Звонок на телефонный номер контактного лица для IP-адреса и получение ответа, подтверждающего запрос заявителя на проверку (TLS BR, раздел 3.2.2.5.5).

3.2.9 Проверка адресов электронной почты

Для проверки контроля над адресами электронной почты или права на их использование GlobalSign использует следующие методы:

1. Проверка контроля объекта над доменной частью адреса почтового ящика, который будет использоваться в сертификате (раздел 3.2.2.1 S/MIME BR); или
2. Подтверждение контроля заявителя над каждым полем почтового ящика, которое должно быть включено в сертификат, путем отправки случайного значения по электронной почте и последующего получения подтверждающего ответа с использованием случайного значения (S/MIME BR, раздел 3.2.2.2).

3.3 Идентификация и аутентификация для запросов на повторный ключ

GlobalSign поддерживает запросы на повторный ключ от Абонентов до истечения срока действия существующего сертификата.

3.3.1 Идентификация и аутентификация для обычного повторного ключа

Для продуктов, поддерживающих повторный ключ, проверка запроса на повторный ключ основывается на механизме, предусмотренном при первоначальном выпуске сертификата, или эквивалентном ему.

Проверка запроса осуществляется в соответствии с условиями повторного использования, указанными в разделе 4.2.1. Если в какой-то момент времени любая информация в сертификате изменяется, необходимо провести дополнительную проверку.

3.3.2 Идентификация и аутентификация для повторного ключа после отзыва

После отзыва ключа не поддерживается выдача обычного повторного ключа. В данном случае требуется повторно пройти процесс первоначальной проверки, который был завершен ранее, чтобы разрешить первоначальный выпуск сертификата.

3.4 Идентификация и аутентификация для запроса на отзыв сертификата

Все запросы на отзыв сертификата удостоверяются компанией GlobalSign или ОР (РЦ). Запросы на отзыв могут быть удовлетворены после выполнения заданного действия, например, входа в учетную запись с именем пользователя и паролем, подтверждения владения уникальными элементами, включенными в сертификат (например, доменным именем или адресом электронной почты), или подтверждения конкретной информации из учетной записи, которая проверяется за ее пределами.

GlobalSign может осуществлять отзыв сертификата от имени Абонента в соответствии с CPS и/или Абонентским договором.

4.0 Операционные требования к жизненному циклу сертификата

4.1 Заявка на сертификат

4.1.1 Кто может подать заявку на сертификат

GlobalSign ведет собственные списки лиц и организаций, от которых заявки на сертификат не принимаются. Кроме того, для отсеивания нежелательных заявителей используются другие внешние источники, такие как государственные списки отказников или международно признанные списки отказников в юрисдикциях, где работает GlobalSign.

GlobalSign не выдает сертификаты субъектам в странах, где законы из юрисдикции GlobalSign запрещают ведение бизнеса.

Руководство EV указывает конкретные правила для получения SSL-сертификата с расширенной проверкой или сертификата подписи кода с расширенной проверкой. Заявитель должен подать запрос на сертификат и подписать Абонентский договор. Это может быть электронный или предварительно одобренный договор в зависимости от характера услуг, требуемых от GlobalSign.

4.1.2 Процесс регистрации и обязанности

Перед выдачей Сертификата GlobalSign получает запрос на Сертификат и подписанное Абонентское соглашение и/или Условия использования в соответствии с применимыми требованиями CA/Browser Forum.

Компания GlobalSign поддерживает системы и процессы, обеспечивающие достаточную проверку заявителя для всех типов публичных сертификатов. Заявители должны предоставить достаточную информацию, чтобы GlobalSign и любой РЦ GlobalSign могли успешно выполнить требуемую проверку. В соответствии со своей Политикой конфиденциальности, GlobalSign и РЦ защищают каналы связи и надежно хранят информацию, предоставленную заявителем в процессе подачи заявки.

Обычно процесс подачи заявки включает следующие шаги (не обязательно в таком порядке, поскольку некоторые рабочие процессы генерируют ключевые пары после завершения проверки):

- Генерация подходящей пары ключей с использованием соответствующей безопасной платформы.
- Генерация запроса на подписание сертификата (CSR) с помощью соответствующего безопасного инструмента.
- Подача запроса на тип сертификата и информации о заявке.
- Согласие с Абонентским договором или другими применимыми положениями и условиями.
- Оплата соответствующих сборов.

4.2 Обработка заявки на сертификат

4.2.1 Выполнение функций идентификации и аутентификации

GlobalSign поддерживает системы и процессы для достаточной проверки заявителя в соответствии с настоящим CPS.

Первоначальная проверка может осуществляться группой проверки GlobalSign, как указано в разделе 3.2, или регистрационным центром по контракту. Все сообщения, отправленные по факсу/электронной почте, надежно хранятся вместе со всей информацией, предоставленной заявителем напрямую через веб-интерфейс или API GlobalSign. Будущие заявки на получение сертификатов аутентифицируются с использованием однофакторной (имя пользователя и пароль) или многофакторной (сертификат в сочетании с именем пользователя/паролем) аутентификации.

Для проверки информации о сертификате GlobalSign может запросить документы и данные, перечисленные в разделе 3.2, или повторно использовать результаты предыдущих проверок, при условии, что:

• GlobalSign получила данные или документ из источника, указанного в разделе 3.2, или завершила проверку не более чем за 825 дней до выдачи Сертификата;
• Для сертификатов S/MIME BR для проверки авторизации или контроля почтового ящика: любые повторно используемые данные, документы или завершенная проверка были получены не более чем за 398 дней до выдачи Сертификата;
• Для сертификатов SSL для проверки доменных имен и IP-адресов в соответствии с разделами 3.2.2.4 и 3.2.2.5 «Базовых требований к TLS» любые повторно используемые данные, документы или завершенная проверка были получены не более чем за 398 дней до выдачи. сертификат; и
• Для сертификатов EV SSL и EV Code Signing компания GlobalSign получила данные или документ из источника, указанного в разделе 3.2, или завершила проверку не более чем за 398 дней до выдачи сертификата. За исключением повторного выпуска сертификата EV в соответствии с разделом 11.14.2 и за исключением случаев, когда иное разрешено в разделе 11.14.1 Руководства по EV.

В некоторых случаях GlobalSign может полагаться на договор с Заявителем, в котором указан другой срок подтверждения полномочий, проверенный в соответствии с разделом 3.2.5. Например, контракт может включать бессрочное распределение ролей до тех пор, пока он не будет аннулирован Кандидатом или УЦ либо пока не истечет срок действия контракта или он не будет расторгнут. GlobalSign может установить процесс, позволяющий заявителю указать лиц, которые могут запрашивать сертификаты. В случае местных регистрационных органов полномочия местного регистрационного органа будут проверены во время настройки профиля. Это полномочие может оставаться в силе до тех пор, пока оно не будет аннулировано.

Клиенты могут запросить перевыпуск сертификата, что соответствует процессу выдачи нового сертификата. Там, где это применимо, информация о сертификате может быть использована повторно.

Если в какой-то момент информация об имени субъекта в сертификате каким-либо образом изменяется, необходимо повторно выполнить процедуры, описанные в настоящем документе.

4.2.2 Утверждение или отклонение заявок на сертификат

GlobalSign отклоняет запросы на сертификаты, если не может успешно завершить проверку всех элементов.

Если все этапы проверки успешно завершены в соответствии с процедурами данного CPS, то GlobalSign обычно утверждает заявку. Заявки могут отклоняться по следующим причинам:

- На основании потенциального ущерба бренду GlobalSign при принятии заявки.
- GlobalSign может отклонить заявки от заявителей, которым ранее было отказано или которые ранее нарушили какое-либо положение Абонентского договора.

GlobalSign не обязана сообщать заявителю причину отклонения запроса на сертификат.

Для сертификатов с расширенной проверкой, квалифицированных сертификатов и сертификатов с подписью кода разделение обязанностей требует, чтобы запрос утверждали два члена команды по проверке. GlobalSign работает во многих юрисдикциях; однако компания может принять решение передать функцию предварительной проверки обученным и опытным внешним партнерам РЦ, которые обладают углубленными знаниями языка и юридических тонкостей, чтобы обрабатывать и/или переводить документацию.

GlobalSign не выдает публично доверенные SSL-сертификаты на внутренние имена или зарезервированные IP-адреса.

4.2.3 Время обработки заявок на сертификат

GlobalSign использует все разумные методы для оценки и обработки заявок на сертификаты. В случае возникновения не зависящих от нее проблем, GlobalSign стремится должным образом информировать заявителя.

Для сертификатов с расширенной проверкой GlobalSign проверяет правильность всей информации, предоставленной заявителем, прежде чем отправлять на утверждение Абонентский договор.

Ниже приведены приблизительные сроки обработки и выдачи.

- **Сертификаты PersonalSign1**. Примерно 1 минута
- **Сертификаты PersonalSign2.** Примерно 24-48 рабочих часов
- **Сертификаты PersonalSign2 Pro.** Примерно 36-72 рабочих часов
- **Сертификаты NAESB.** Примерно 24-48 рабочих часов
- **Сертификаты PersonalSign3 Pro.** Примерно 48-72 рабочих часов
- **Сертификаты подписи кода.** Примерно 24-48 рабочих часов
- **Сертификаты подписи кода EV.** Примерно 48-96 рабочих часов
- **Сертификаты DV SSL.** Примерно 1-5 минут[4]
- **Сертификаты AlphaSSL.** Примерно 1-5 минут[3]
- **Сертификаты OV SSL.** Примерно 24-48 рабочих часов
- **Сертификаты EV SSL.** Примерно 48-96 рабочих часов
- **Квалифицированные сертификаты.** Примерно 48-96 рабочих часов
- **Сертификаты меток времени.** Примерно 5-10 рабочих дней
- **Сертификаты AATL.** Примерно 24-48 рабочих часов
- **Сертификаты S/MIME.** Примерно 48-72 рабочих часов

4.3 Выдача сертификатов

4.3.1 Действия УЦ во время выпуска сертификата

Выпуск сертификата корневым УЦ GlobalSign требует, чтобы уполномоченный член GlobalSign выдал корневому УЦ прямую команду на подпись сертификата.

GlobalSign должна обеспечить связь со всеми аккаунтами РЦ, которые могут выпустить сертификат с использованием многофакторной аутентификации. Сюда входят РЦ, непосредственно управляемые GlobalSign, или нанятые GlobalSign по контракту. РЦ должны проверять всю информацию, отправляемую в УЦ, и гарантировать, что любая база данных для хранения любой информации, надлежащим образом защищена от несанкционированной модификации или фальсификации.

4.3.2 Уведомление Абонента о выдаче сертификата

GlobalSign или ОР (РЦ) уведомляет Абонента о выдаче сертификата по адресу электронной почты, указанному в процессе регистрации или любым другим эквивалентным способом. Письмо может содержать сам сертификат или ссылку для загрузки, в зависимости от процедуры выдачи сертификата.

4.4 Принятие сертификата

4.4.1 Действия, составляющие принятие сертификата

GlobalSign информирует Абонента о запрете использовать сертификат до тех пор, пока Абонент не проверит точность данных в сертификате. В отсутствии уведомления GlobalSign от Абонента в течение семи (7) дней с момента получения, сертификат считается принятым.

4.4.2 Публикация сертификата удостоверяющим центром

GlobalSign публикует сертификат путем передачи Абоненту, а также может опубликовать в одном или нескольких публичных списках Certificate Transparency Logs. Кроме того, для

---

[4] Если проверяемое доменное имя для SSL-сертификата DV/Alpha считается высокорискованным, процесс обработки по времени близок к OV SSL.

корпоративных клиентов PKI GlobalSign может опубликовать сертификат в каталоге, таком как LDAP.

4.4.3 Уведомление удостоверяющим центром других организаций о выдаче сертификата

Если РЦ, местные РЦ, партнеры/реселлеры, GlobalSign и другие организации участвовали в первоначальной регистрации, то они могут быть проинформированы о выпуске сертификата.

4.5 Использование пары ключей и сертификата

4.5.1 Использование закрытого ключа и сертификата

Абонент должен защищать свой секретный ключ, стараясь не раскрывать его третьим лицам. В Абонентском договоре GlobalSign определены обязательства Абонента в отношении защиты закрытого ключа. Закрытые ключи должны использоваться только так, как указано в полях использования и расширенного использования ключа в соответствующем сертификате.

Для квалифицированных сертификатов ключи Абонента должны генерироваться и храниться в признанном устройстве создания квалифицированной подписи (QSCD).

Для сертификатов подписи кода без EV, выпущенных до 24 апреля 2023 г. закрытый ключ Абонента должен генерироваться, храниться и использоваться в криптомодуле, отвечающем требованиям FIPS 140-2 уровня 2 или Common Criteria EAL 4+, или в модуле доверенной платформы (TPM), который генерирует и защищает пару ключей и может документировать защиту закрытого ключа Абонента посредством сертификации ключа TPM.

Для сертификатов подписи кода EV, выпущенных до 24 апреля 2023 г. закрытый ключ Абонента должен генерироваться, храниться и использоваться в криптомодуле, который соответствует или превосходит требования FIPS 140-2 уровень 2 или Common Criteria EAL 4+.
С 24 апреля 2023 г. закрытые ключи абонента для сертификатов подписи кода EV и без EV должны создаваться и защищаться в аппаратном криптомодуле с форм-фактором устройства, сертифицированным как соответствующий как минимум FIPS 140-2 уровня 2 или Общими Критериями EAL. 4+.

Резервную копию закрытого ключа следует защищать с той же осторожностью, что и оригинал. По окончании срока службы закрытого ключа Абонент должен безопасно удалить ключ и все фрагменты, на которые он был разделен для резервного копирования.

В Службе цифровой подписи GlobalSign с согласия Абонента GlobalSign размещает, защищает и управляет краткосрочными сертификатами и соответствующими закрытыми ключами в соответствующем HSM/QSCD.

См. раздел 9.6.3, положения 2. и 4.

4.5.2 Использование доверяющей стороной открытого ключа и сертификата

В рамках данного CPS компания GlobalSign предоставляет условия, при которых сертификаты могут использоваться доверяющими сторонами, включая соответствующие службы сертификатов, доступные для проверки действительности сертификата, такие как COC (CRL) и OCSP. GlobalSign предоставляет Абонентам соглашение для доверяющей стороны, содержание которого должно быть ей представлено. До того, как полагаться на сертификат от GlobalSign, доверяющая сторона должна принять и действовать в соответствии с этим соглашением. Доверяющие стороны проводят самостоятельную оценку рисков перед тем, как полагаться на сертификат или любые предоставленные гарантии, поэтому несут полную ответственность за свою оценку рисков.

Программное обеспечение, используемое доверяющими сторонами, должно полностью соответствовать стандартам X.509, включая передовую практику принятия решений о цепочке политик и использовании ключей.

4.6 Продление сертификата

Продление сертификата означает выдачу сертификата с новым сроком действия, заканчивающимся после срока действия старого сертификата, но без изменения открытого ключа Абонента или другого участника или любой другой информации в сертификате.

Если открытый ключ или любая информация в сертификате отличается, то запрос на продление обрабатывается как запрос на новый сертификат.

4.6.1 Обстоятельства для продления сертификата

Если такое поддерживается продуктом, продление сертификата может выполняться по запросу Абонента, его уполномоченного представителя или компанией GlobalSign по своему усмотрению.

Продление сертификата выполняется только если оригинальный сертификат не отозван.

4.6.2 Кто может запросить продление

Запрос на продление подается Абонентом или его уполномоченным представителем.

4.6.3 Обработка запросов на продление сертификата

Для обработки запроса на продление сертификата компания GlobalSign подтверждает запрос у Абонента или его уполномоченного представителя.

Запросы на продление обрабатываются как запросы на новый сертификат.

4.6.4 Уведомление Абонента о выдаче нового сертификата

В соответствии с пунктом 4.3.2.

4.6.5 Поведение, означающее принятие продленного сертификата

В соответствии с пунктом 4.4.1.

4.6.6 Публикация продленного сертификата удостоверяющим центром

В соответствии с пунктом 4.4.2.

4.6.7 Уведомление удостоверяющим центром других организаций о выдаче сертификата

Не предусмотрено.

4.7 Перевыпуск ключа для сертификата

Перевыпуск ключа означает выдачу нового сертификата с другим открытым ключом, но без изменения срока действия или любой другой информации в сертификате.

Если изменяется срок действия или любая другая информация в сертификате, то запросы на перевыпуск ключа обрабатываются как запросы на новый сертификат.

4.7.1 Обстоятельства для перевыпуска ключа сертификата

Если такое поддерживается продуктом, перевыпуск ключа сертификата выполняется по запросу Абонента, его уполномоченного представителя или компанией GlobalSign по своему усмотрению.

Перевыпуск ключа возможен при компрометации закрытого ключа сертификата.

4.7.2 Кто может запросить перевыпуск открытого ключа

Запрос на перевыпуск подает Абонент сертификата или его уполномоченный представитель.

4.7.3 Обработка запросов на перевыпуск ключа сертификата

Перед выполнением запроса на перевыпуск ключа GlobalSign получает подтверждение у Абонента или его уполномоченного представителя.

Запросы на перевыпуск ключа сертификата обрабатываются как запросы на новый сертификат.

4.7.4 Уведомление Абонента о выдаче нового сертификата

В соответствии с пунктом 4.3.2.

4.7.5 Действия, означающие принятие перевыпущенного ключа сертификата

В соответствии с пунктом 4.4.1.

4.7.6 Публикация удостоверяющим центром сертификата с перевыпущенный ключом

В соответствии с пунктом 4.4.2.

4.7.7 Уведомление удостоверяющим центром других организаций о выпуске сертификата

Не предусмотрено.

4.8 Изменение сертификата

Изменение сертификата означает выдачу нового сертификата в связи с изменением какой-либо информации в сертификате, кроме открытого ключа.

Запросы на изменение сертификата обрабатываются как запросы на новый сертификат, если изменен срок действия или отличается открытый ключ Абонента.

4.8.1 Обстоятельства для изменения сертификата

Если такое поддерживается продуктом, изменение сертификата может быть выполнено по запросу Абонента, его уполномоченного представителя или компанией GlobalSign по своему усмотрению.

4.8.2 Кто может запросить изменение сертификата

Запрос на изменение подает Абонент сертификата или его уполномоченный представитель.

4.8.3 Обработка запросов на изменение сертификата

Перед выполнением запроса на изменение сертификата GlobalSign проверяет запрос у Абонента или его уполномоченного представителя.

Запросы на изменение сертификата обрабатываются как запросы на новый сертификат.

4.8.4 Уведомление Абонента о выдаче нового сертификата

В соответствии с пунктом 4.3.2.

4.8.5 Действия, означающие принятие измененного сертификата

В соответствии с пунктом 4.4.1.

4.8.6 Публикация удостоверяющим центром измененного сертификата

В соответствии с пунктом 4.4.2.

4.8.7 Уведомление удостоверяющим центром других организаций о выпуске сертификата

Не предусмотрено.

4.9 Отзыв и приостановление действия сертификата

4.9.1 Обстоятельства для отзыва

Перед отзывом сертификата GlobalSign проверит подлинность запроса на отзыв.

GlobalSign может отозвать любой сертификат по своему собственному усмотрению.

В следующих обстоятельствах сертификат Абонента отзывается в течение двадцати четырех (24) часов:

1. Абонент подает письменный запрос о своем желании отозвать сертификат в компанию GlobalSign.
2. Абонент уведомляет GlobalSign о том, что первоначальный запрос на сертификат был не авторизован, и не производит авторизацию задним числом.
3. GlobalSign получила обоснованные доказательства компрометации закрытого ключа, который соответствует открытому ключу в сертификате Абонента.
4. GlobalSign стало известно о продемонстрированном или проверенном методе, который позволяет легко вычислить закрытый ключ на основе открытого ключа в сертификате Абонента (см. слабые ключи Debian, https://wiki.debian.org/SSLkeys);
5. GlobalSign больше не может полагаться на подтверждение авторизации или контроля над каким-либо доменным именем или IP-адресом в сертификате.
6. GlobalSign получает доказательства того, что не следует полагаться на проверку авторизации домена или контроля почтового ящика для любого адреса почтового ящика в сертификате.
7. GlobalSign становится известно о неожиданном прекращении действия соглашения или деловых функций Абонента или субъекта.
8. В случае PSD2-сертификатов GlobalSign получает аутентифицированный запрос на отзыв (или аутентифицирует запрос на отзыв) от NCA, авторизовавшего или зарегистрировавшего поставщика платежных услуг, и который содержит действительную причину для отзыва. Уважительные причины для отзыва включают отзыв авторизации PSP или отзыв любой должности PSP, включенной в сертификат.

В следующих обстоятельствах сертификат Абонента, который должен быть отозван в течение двадцати четырех (24) часов, отзывается в течение 5 дней:

1. Сертификат более не соответствует требованиям к типу алгоритма и размеру ключа, как указано в разделах 6.1.5 и 6.1.6 Базовых требований CA/Browser Forum.
2. GlobalSign получает доказательства, что сертификат использован не по назначению.
3. GlobalSign получает информацию, что Абонент нарушил один из существенных пунктов Абонентского договора или Условий использования.
4. GlobalSign становится известно о любых обстоятельствах, указывающих на юридический запрет дальнейшего использования полностью квалифицированного доменного имени или IP-адреса в сертификате (например, суд или арбитраж отозвал право регистранта на использование доменного имени или прекратило действие лицензионное соглашение между регистрантом и заявителем, или регистрант не продлил срок действия доменного имени).
5. GlobalSign уведомляется о любых обстоятельствах, указывающих на то, что использование адреса электронной почты или полного доменного имени в Сертификате больше не разрешено законом (например, суд или арбитр отменил право на использование адреса электронной почты или доменного имени, соответствующее лицензионное соглашение или соглашение об оказании услуг между Абонентом расторгнуто, либо владелец учетной записи не смог поддерживать активный статус адреса электронной почты или Доменного имени);
6. GlobalSign определяет неточность какой-либо информации в сертификате.
7. GlobalSign потеряла право выдавать сертификаты в соответствии с Базовыми требованиями, если не договорилась о продолжении ведения репозитория COC/OCSP.
8. Отзыв требуется в соответствии с CP или CPS GlobalSign.
9. GlobalSign узнает о продемонстрированном или доказанном методе, который подвергает риску компрометации закрытый ключ Абонента или есть четкие доказательства слабости конкретного метода, который использовался для генерации закрытого ключа.
10. Техническое содержание или формат сертификата представляют неприемлемый риск для поставщиков прикладного программного обеспечения или доверяющих сторон (например, CA/B Forum может заявить, что устаревший криптоалгоритм или размер ключа представляют неприемлемый риск и УЦ должен за определенный срок отозвать и заменить такие сертификаты).
11. GlobalSign узнала о каких-то обстоятельствах, что использование адреса электронной почты в сертификате связано с нарушением закона.

12. GlobalSign становится известно, что сертификат выдан в нарушение Базовых требований, CP или CPS GlobalSign.
13. Есть подозрения компрометации закрытого ключа УЦ, использованного при выдаче сертификата.
14. GlobalSign по какой-либо причине прекращает деятельность, не договорившись с другим УЦ о поддержке отзыва сертификатов.
15. Сертификат выдан в нарушение действующей на тот момент версии Политики корневого хранилища Mozilla (Root Store Policy).

В следующих обстоятельствах отзыв сертификата Абонента может быть осуществлен в течение коммерчески обоснованного периода времени:

1. Абонент или администратор организации запросил отзыв сертификата через учетную запись клиента, которая контролирует жизненный цикл сертификата.
2. Абонент отправил аутентифицированный запрос в службу поддержки GlobalSign или регистрационный центр GlobalSign.
3. GlobalSign узнает, что Абонент добавлен в блок-лист как запрещенная сторона или лицо, или по месту его деятельности запрещено вести бизнес в соответствии с законодательством юрисдикции, в которой работает GlobalSign.
4. Абонент был добавлен в качестве стороны, которой запрещено, или иным образом обозначен, или на него наложены экономические санкции или другие ограничения в соответствии с применимым законодательством.
5. Абонентом просрочена оплата соответствующих сборов.
6. После запроса на аннулирование сертификата.
7. Если сертификат выпущен повторно, GlobalSign может отозвать ранее выпущенный.
8. В соответствии с некоторыми лицензионными соглашениями GlobalSign может отозвать сертификаты после истечения срока действия или прекращения действия лицензионного соглашения.
9. GlobalSign определяет, что дальнейшее использование сертификата наносит ущерб бизнесу GlobalSign или третьих лиц. При рассмотрении вопроса о вреде для бизнеса или репутации GlobalSign учитывает, среди прочего, характер и количество полученных жалоб, личность заявителя (заявителей), соответствующее законодательство и действия Абонента в связи с предполагаемым вредом.
10. Если компания Microsoft самостоятельно выявит сертификат, использование или атрибуты которого противоречат Программе доверенных корней (Trusted Root Program), она уведомит об этом GlobalSign и попросит отозвать сертификат. GlobalSign либо отзовет сертификат, либо в течение 24 часов после получения уведомления запросит у Microsoft исключение. Microsoft рассмотрит представленные материалы и сообщит GlobalSign свое окончательное решение о предоставлении исключения или отказе в нем. В случае, если Microsoft не предоставит исключение, GlobalSign отзовет сертификат в течение 24 часов с момента отказа в предоставлении исключения.
11. Смерть Абонента.

В следующих обстоятельствах отзыв сертификата подчиненного УЦ осуществляется в течение семи (7) дней:

1. Подчиненный УЦ в письменной форме обращается с просьбой об отзыве сертификата к организации GlobalSign, выдавшей сертификат, или к органу, указанному в разделе 1.5.2 настоящего CPS.
2. Абонент уведомляет GlobalSign о том, что первоначальный запрос на сертификат был не авторизован, и не производит авторизацию задним числом.
3. GlobalSign получила обоснованные доказательства компрометации закрытого ключа, который соответствует открытому ключу в сертификате Абонента, или закрытый ключ более не соответствует требованиям к типу алгоритма и размеру ключа применяемых требований CA/B Forum, как указано в Разделах 6.1.5 и 6.1.6.
4. GlobalSign получает доказательства, что сертификат использован не по назначению.
5. GlobalSign становится известно, что сертификат выдан в нарушение требований CA/B Forum или подчиненный УЦ нарушил условия CP или CPS GlobalSign.

6. GlobalSign определяет, что информация в сертификате является неточной или вводящей в заблуждение.
7. GlobalSign или подчиненный УЦ по какой-либо причине прекращает свою деятельность и не договорился с другим УЦ о поддержке отзывов сертификатов.
8. Право GlobalSign или подчиненного УЦ на выпуск сертификатов в соответствии с требованиями CA/B Forum истекает, аннулируется или прекращается, если только выпускающий УЦ не принял меры для продолжения ведения репозитория COC/OCSP.
9. Отзыв требуется в соответствии с CP или CPS GlobalSign.
10. Техническое содержание или формат сертификата представляют неприемлемый риск для поставщиков прикладного программного обеспечения или доверяющих сторон (например, CA/B Forum может заявить, что устаревший криптоалгоритм или размер ключа представляют неприемлемый риск и УЦ должен за определенный срок отозвать и заменить такие сертификаты).

Если отзыва требует Абонент, он может указать причину:

- Unspecified: Если приведенные ниже коды причин не применимы к запросу на отзыв, Абонент не должен указывать код причины, отличный от Unspecified.
- keyCompromise: Когда есть основания полагать, что закрытый ключ сертификата скомпрометирован, например, к нему получило доступ неавторизованное лицо.
- cessationOfOperation: Когда Абонент больше не владеет всеми доменными именами в сертификате или прекращает работу веб-сайта.
- affiliationChanged: Когда изменилось название организации или другая информация в сертификате.
- Superseded: Когда отправлен запрос на новый сертификат для замены существующего.

Если причина отзыва не указана, используется код Unspecified.

Для краткосрочных Сертификатов, выданных через Облачный сервис цифровой подписи (DSS) GlobalSign и Сервис квалифицированной подписи (QSS), отзыв Абонентом не поддерживается.

4.9.2 Кто может запросить отзыв

GlobalSign, OP (РЦ) или Абонент могут инициировать отзыв. Принимаются только аутентифицированные запросы на отзыв. Разрешение на отзыв дается в том случае, если запрос получен от Абонента либо аффилированной организации, указанной в сертификате. Абоненты, доверяющие стороны, поставщики прикладного программного обеспечения и другие третьи стороны могут подавать отчеты о проблемах с сертификатами, чтобы уведомить GlobalSign о предполагаемой разумной причине для отзыва сертификата. Кроме того, для сертификатов Open Baniking запрос на отзыв может исходить от NCA, которая уполномочила или зарегистрировала поставщика платежных услуг. GlobalSign также может по собственному усмотрению отзывать сертификаты, включая сертификаты, выданные другим УЦ с перекрестной подписью.

4.9.3 Процедура запроса на отзыв

В связи с характером запросов на отзыв и ради эффективности GlobalSign предоставляет автоматизированные механизмы для подачи и аутентификации запросов. Основной метод – через клиентскую учетную запись r, которая использовалась для выпуска отзываемого сертификата. Можно использованать альтернативные офлайновые методы, такие как факс, письмо и телефонный звонок. Их следует заверять с помощью общих секретов клиентской учетной записи. В случае отсутствия учетных записей клиента можно использовать методы, основанные на демонстрации контроля над одним или несколькими элементами поля Subject DN в сертификате. Для сертификатов S/MIME это может включать демонстрацию контроля над адресом электронной почты. GlobalSign и ее РЦ регистрируют все запросы, проверяют их подлинность и запускают процедуру отзыва сертификата, если запрос одобрен.

Абоненты, доверяющие стороны, поставщики прикладного программного обеспечения и другие третьи лица могут направлять сообщения о проблемах с сертификатами по адресу report-abuse@globalsign.com. GlobalSign может удовлетворить или не удовлетворить этот

запрос. Подробности действий, выполняемых GlobalSign для принятия решения, см. в разделе 4.9.5.

В случае отзыва сертификата его серийный номер, дата и время добавляют в соответствующий список COC. Могут быть добавлены и коды причин COC. Списки COC публикуются в соответствии с настоящим CPS.

4.9.4 Отсрочка отзыва

GlobalSign не поддерживает отсрочку отзыва сертификатов SSL и подписи кода.

Для всех остальных сертификатов отсрочка отзыва (grace period) — это время, в течение которого Абонент может предпринять все необходимые действия, чтобы запросить отзыв потенциально скомпрометированного ключа, слабого ключа или сообщить о неточной информации в выданном сертификате. Анализ рисков должен быть завершен и записан для всех случаев отзыва, которые по какой-либо причине не могут быть обработаны ни одной из сторон по какой-либо причине.

У Абонентов есть 48 часов, чтобы сообщить GlobalSign о компрометации ключа.

4.9.5 Время, за которое УЦ должен обработать запрос на отзыв

Все запросы на отзыв сертификатов конечных субъектов, как автоматически генерируемые через учетные записи пользователей, так и инициируемые самой компанией GlobalSign, должны быть обработаны в течение 24 часов с момента получения.

В GlobalSign работает служба круглосуточного реагирования на высокоприоритетные сообщения о проблемах с сертификатами. При необходимости жалобы перенаправляются в правоохранительные органы с мгновенным отзывом сертификата, ставшего предметом жалобы. По подозрению в компрометации ключа или неправомерном использовании сертификата GlobalSign инициирует расследование в течение 24 часов после получения сообщения.

GlobalSign принимает решение о целесообразности отзыва или других действий, основываясь, по крайней мере, на следующих критериях:

- Характер предполагаемой проблемы.
- Количество полученных сообщений о конкретном сертификате или Абоненте.
- Организация, подавшая жалобу.
- Соответствующее законодательство.

4.9.6 Требования для доверяющих сторон проверять информацию об отзывах сертификатов

Прежде чем полагаться на сертификат, доверяющие стороны должны проверить соответствие сертификата поставленной цели и убедиться в его действительности, иначе все гарантии теряют силу.

Для каждого сертификата в цепочке доверяющие стороны должны проверить информацию COC или OCSP, а также убедиться, что цепочка сертификатов полная. Это может включать проверку идентификатора ключа центра (AKI) и идентификатора ключа субъекта (SKI). Для квалифицированных сертификатов проверка цепочки сертификатов должна быть успешно проведена вплоть до якоря доверия GlobalSign в доверенном списке EC и UK eIDAS.

Доверяющие стороны должны учитывать, что COC выпускаются в определенные временные рамки. Может быть период непосредственно после отзыва и до следующей генерации COC, когда OCSP и COC возвращают разный статус. В случаях таких различий приоритетным источником информации следует считать OCSP.

GlobalSign включает в сертификат соответствующие URL-адреса для проверки списков отзывов, чтобы помочь доверяющим сторонам.

4.9.7 Частота выпуска COC

Каждый список COC включает монотонно возрастающий порядковый номер для нумерации.

Если компания GlobalSign по своей инициативе или по требованию должна прекратить действие COC или отозвать издающий УЦ, она выпускает и публикует в соответствующей точке распространения последний COC со значением поля nextUpdate "99991231235959Z". GlobalSign не выпускает последний COC до тех пор, пока все сертификаты в области действия COC не будут либо просрочены, либо отозваны. Последний COC становится доступным до истечения срока действия сертификата издающего УЦ, и целостность COC сохраняется в течение этого периода.

Для статуса сертификатов Абонентов:
Для УЦ, публикующих COC, список обновляется обновляется и перевыпускается не реже одного раза в семь дней (для квалифицированных сертификатов каждые 24 часа), а значение поля nextUpdate не превышает значение поля thisUpdate более чем на десять дней.

Для статуса сертификатов подчиненных УЦ:
Если подчиненный УЦ содержит CDP, то COC обновляется и перевыпускается не реже (i) одного раза в 3 месяца и (ii) в течение 24 часов после отзыва сертификата подчиненного УЦ, а значение поля nextUpdate не превышает значение поля thisUpdate более чем на двенадцать месяцев.

4.9.8 Максимальная задержка для списков COC

COC публикуются в хранилище в течение коммерчески обоснованного времени после генерации.

4.9.9 Онлайновая доступность проверки статуса/отмены

Там, где GlobalSign в дополнение к COC поддерживает ответы OCSP, время ответа OCSP обычно не превышает 10 секунд при нормальных условиях работы сети.

Ответы OCSP от GlobalSign соответствуют RFC6960 и/или RFC5019. Ответы OCSP подписываются ответчиком OCSP с подписью того УЦ, который выдал сертификат, подвергаемый проверке. Сертификат подписи OCSP содержит расширение типа id-pkixocsp-nocheck, как определено RFC6960.

4.9.10 Требования к проверке отзыва онлайн

Ответчики OCSP, управляемые GlobalSign, поддерживают метод HTTP GET, как описано в RFC 6960 и/или RFC 5019.
Интервал действия ответа OCSP — это разница во времени между thisUpdate и
поле nextUpdate включительно. Для целей расчета различий учитывается разница в 3600 секунд и будет равна одному часу, а разница в 86 400 секунд будет равна одним суткам, без учета дополнительные секунды.

Для статуса сертификатов Абонентов:

1. Период действия ответов OCSP составляет восемь или более часов.
2. Период действия ответов OCSP не превышает десять дней.
3. Для ответов OCSP с периодом действия менее шестнадцати часов компания GlobalSign обновляет информацию, предоставленную с помощью протокола Online Certificate Status Protocol, до наступления середины срока действия перед следующим обновлением (nextUpdate).
4. Для ответов OCSP с периодом действия 16 и более часов GlobalSign обновляет информацию, предоставляемую с помощью протокола Online Certificate Status Protocol, не менее чем за восемь часов до следующего обновления и не позднее чем через четыре дня после этого обновления.

Для статуса сертификатов подчиненных УЦ:

- GlobalSign обновляет информацию, предоставляемую через OCSP Responder (i) не реже раза в двенадцать месяцев и (ii) в течение 24 часов после отзыва сертификата подчиненного УЦ.

Для невыданных сертификатов ответчики OCSP не должны возвращать "good" в ответ на запрос о статусе таких сертификатов.

Для УЦ, которые не являются технически ограниченными, в соответствии с разделом 7.1.5, OCSP не должны возвращать "good" в ответ на запрос о статусе таких сертификатов.

GlobalSign требует, чтобы запросы OCSP содержали следующие данные:

- Версия протокола
- Запрос службы
- Идентификатор целевого сертификата

Серийный номер сертификата в запросе OCSP может быть одним из трех следующих вариантов:

1. «назначается», если сертификат с таким серийным номером был выдан выдающим центром сертификации с использованием

любой текущий или предыдущий ключ, связанный с этим субъектом CA; или

2. «зарезервировано», если предварительный сертификат [RFC6962] с этим серийным номером был выдан

а. УЦ-эмитент; или

б. сертификат подписи предварительного сертификата, связанный с выдающим центром сертификации; или

3. «не используется», если ни одно из предыдущих условий не выполнено.

4.9.11 Другие доступные формы объявлений об отзыве сертификатов

Не предусмотрено.

4.9.12 Специальные требования, связанные с компрометацией ключей

GlobalSign и все ее регистрационные центры должны использовать коммерчески обоснованные методы для информирования Абонента о потенциальной компрометации закрытого ключа, включая обнаружение новых уязвимостей или когда GlobalSign по собственному усмотрению решает, что имеются доказательства возможной компрометации. Если компрометация ключа не оспаривается, GlobalSign в течение 24 часов отзывает сертификаты выпускающего УЦ или сертификаты конечных субъектов Абонента, выкладывая в интернете COC в течение 30 минут после его создания, а ARL в течение 12 часов.

Для демонстрации факта компрометации ключей стороны могут использовать следующие методы:

- Предоставить файл COC, созданный и подписанный закрытым ключом. Файл содержит одно из следующего:
  - Конкретную строку, которую GlobalSign отправила ответчику.
  - Строку текста, которая явно указывает на компрометацию.

- Предоставить ссылки на источники информации об уязвимостях и/или инцидентах безопасности, на основании которых можно проверить факт компрометации.
- Предоставить двоичные файлы, содержащие скомпрометированный закрытый ключ, включая метод его извлечения.

Если новый метод компрометации будет доказан, GlobalSign проанализирует другие запросы и соответствующим образом обновит CPS.

4.9.13 Обстоятельства для приостановки действия сертификата

Приостановка сертификата применяется, когда администратор EPKI хочет временно отключить клиентские сертификаты. Такие ситуации включают временную потерю сертификатов, временный отъезд пользователей из организации и т.д. В отличие от отзыва, отключающего сертификат навсегда, администратор может отменить статус приостановки сертификата и повторно его активировать.

Не поддерживается приостановка сертификатов SSL, подписи кода, временных меток и квалифицированных сертификатов.

4.9.14 Кто может запросить приостановку

Приостановку и ее отмену могут запросить администраторы EPKI через учетную запись GCC. GlobalSign не обрабатывает запросы на приостановку, поступившие по другим каналам.

4.9.15 Процедура запроса на приостановку действия сертификата

Администраторы EPKI запрашивают приостановку сертификата в GCC. После подачи запроса информация синхронизируется с РЦ и УЦ для обработки запроса.

Приостановка действия сертификата указывается в COC с кодом причины "certificateHold".

4.9.16 Ограничения на период приостановки

Приостановка сертификата может длиться столько, сколько длится срок действия сертификата.

4.10 Службы статуса сертификата

4.10.1 Операционные характеристики

GlobalSign указывает в сертификатах службу статуса сертификата в виде точки распространения COC либо в виде ответчика OCSP, либо и то, и другое. Для уменьшения размера файла COC записи об отзыве могут быть удалены по истечении срока действия сертификата, за исключением сертификатов подписи кода (их можно удалить только через 10 лет после истечения срока действия).

Для других типов сертификатов GlobalSign не удаляет записи об отзыве в COC или OCSP до истечения срока действия отозванного сертификата.

За месяц (обычно за 30 и 7 дней) до истечения срока действия сертификата GlobalSign отправляет уведомления по электронной почте, информируя Абонентов о предстоящем истечении их сертификатов.

За исключением случаев приостановки, статус отзыва никогда не будет восстановлен.

Если того требуют корневые программы или требования CA/B Forum, GlobalSign может осуществлять отзыв сертификатов задним числом с помощью поля revocationDate, в виде исключения из правил RFC 5280 по использованию поля invalidityDate.

GlobalSign может отозвать задним числом сертификат подписи кода. Если В таком случае GlobalSign в качестве исключения из правил RFC 5280 следует рекомендации CSBR использовать поле revocationDate вместо invalidityDate в своем COC.

4.10.2 Доступность услуги

GlobalSign поддерживает ресурсы для сервисов COC и OCSP, достаточные для обеспечения времени ответа не более 10 секунд в нормальных условиях работы. GlobalSign круглосуточно поддерживает онлайн-репозиторий, который могут использовать сторонние программы для автоматической проверки текущего состояния всех неистекших сертификатов, выданных GlobalSign.

GlobalSign поддерживает круглосуточную возможность внутреннего реагирования на высокоприоритетные сообщения о проблемах с сертификатами. При необходимости такие

жалобы направляются в правоохранительные органы с отзывом сертификата, ставшего предметом жалобы.

В случае сбоя системы, обслуживания или других неподконтрольных факторов GlobalSign стремится к тому, чтобы доступность информационной услуга восстановилась в течение 48 часов.

4.10.3 Особенности эксплуатации

Не предусмотрено.

4.11 Окончание подписки

Абоненты могут прекратить подписку на услуги сертификата путем отзыва сертификата или естественного истечения срока его действия.

4.12 Хранение и восстановление ключей

4.12.1 Политика и практики депонирования и восстановления ключей

Закрытые ключи УЦ никогда не депонируются. GlobalSign не предлагает Абонентам такие услуги.

4.12.2 Политика и практика инкапсуляции и восстановления сеансовых ключей

Не предусмотрено.

5.0 Безопасность здания, управление и операционный контроль

Процесс управления сертификатами GlobalSign включает:

1. Физическая безопасность и контроль окружающей среды.
2. Контроль целостности системы, включая управление конфигурацией, поддержание целостности доверенного кода и обнаружение/предотвращение вредоносных программ.
3. Сетевая безопасность и управление файрволом, включая ограничения портов и фильтрацию IP-адресов.
4. Управление пользователями, назначение отдельных доверенных сотрудников, обучение, информирование и тренинги.
5. Контроль логического доступа, регистрация действий и таймауты бездействия для обеспечения подотчетности каждого физического лица.

Ежегодная оценка рисков в рамках программы безопасности GlobalSign включает в себя:

1. Определение потенциальных внутренних и внешних угроз, которые могут привести к несанкционированному доступу, раскрытию, неправильному использованию, изменению или уничтожению любых данных сертификата или процессов управления сертификатами.
2. Оценка вероятности и потенциального ущерба от этих угроз, принимая во внимание чувствительность данных сертификата и процессов управления сертификатами.
3. Оценка достаточность политик, процедур, информационных систем, технологий и других мер, которые GlobalSign применяет для противодействия таким угрозам.

На основе оценки рисков GlobalSign разрабатывает, внедряет и поддерживает план безопасности. Он включает процедуры, меры и продукты безопасности, предназначенных для достижения изложенных выше целей, а также для управления и контроля рисков, выявленных в ходе оценки рисков, соразмерно чувствительности данных сертификата и процессов управления сертификатами.

План безопасности включает административные, организационные, технические и физические меры защиты, соответствующие чувствительности данных в сертификатах, и процессы управления сертификатами. План безопасности также учитывает доступные технологии и стоимость внедрения конкретных мер и реализует разумный уровень безопасности, соответствующий ущербу, который может возникнуть в результате нарушения безопасности, и характеру защищаемых данных.

5.1 Физические средства контроля

GlobalSign поддерживает политику физической и экологической безопасности систем, используемых для выпуска и управления сертификатами, которая охватывает контроль физического доступа, защиту от стихийных бедствий, факторы пожарной безопасности, отказ вспомогательных коммуникаций (например, электропитания, телекоммуникаций), разрушение структуры, протечку водопровода, защиту от кражи, взлома и проникновения, а также аварийное восстановление. Средства контроля применяются для того, чтобы избежать потери, повреждения или компрометации активов и прерывания деловой активности, а также кражи информации и средств обработки информации.

5.1.1 Расположение и строительство объекта

УЦ компании GlobalSign расположены в защищенном центре обработки данных. Центр обработки данных представляет собой специально построенный объект из бетона и стальных конструкций.

5.1.2 Физический доступ

УЦ GlobalSign работают в защищенном центре обработки данных с контролем доступа на базе биометрических сканеров и систем карточного доступа. Обеспечивается круглосуточное видеонаблюдение, а также цифровая запись. Помещения охраняются квалифицированными охранниками, а на территорию допускается только персонал, прошедший проверку безопасности и получивший разрешение.

5.1.3 Электропитание и кондиционирование

УЦ компании GlobalSign работают в защищенном центре обработки данных, оснащенном резервной системой электропитания и охлаждения. В маловероятном случае отключения электричества имеются ИБП и генератор электроэнергии.

5.1.4 Воздействие воды

УЦ компании GlobalSign защищен от воды. Он расположен над поверхностью земли на высоком этаже с фальшполом. Кроме того, имеется система сигнализации обнаружения воды, а оперативный персонал центра обработки данных на месте готов отреагировать на любое маловероятное воздействие воды.

5.1.5 Профилактика и защита от пожаров

УЦ компании GlobalSign работают в защищенном центре обработки данных, оборудованном системой обнаружения и тушения пожара.

5.1.6 Хранение носителей

Хранение резервных накопителей осуществляется за пределами площадки. Это место физически изолировано, защищено от пожара и повреждения водой.

5.1.7 Утилизация отходов

GlobalSign гарантирует, что все накопители информации перед утилизацией рассекречиваются или уничтожаются общепринятым.

5.1.8 Резервное копирование за пределами дата-центра

Как указано в разделе 5.5.

5.2 Процедурные средства контроля

5.2.1 Доверенные должности

GlobalSign гарантирует, что все операторы и администраторы, включая специалистов по проверке, действуют в рамках доверенных должностей, где конфликт интересов невозможен. Должности распределены таким образом, что никто не может обойти систему безопасности УЦ.

Доверенные должности включают, но не ограничиваются следующими:

- **Разработчик:** Отвечает за разработку систем УЦ.

- **Сотрудник службы безопасности/руководитель службы информационной безопасности:** Общая ответственность за управление практиками безопасности УЦ.
- **Специалист по валидации:** Отвечает за проверку подлинности и целостности данных, включаемых в сертификаты, с помощью соответствующей системы РЦ, утверждает генерацию/отмену/приостановку сертификатов.
- **Инфрасистемный инженер:** Уполномочен устанавливать, настраивать и обслуживать системы УЦ для управления жизненным циклом сертификатов.
- **Инфрасистемный: оператор:** Отвечает за ежедневную эксплуатацию систем УЦ. Уполномочен выполнять резервное копирование/восстановление системы, просмотр/обслуживание архивов систем УЦ и журналов аудита.
- **Аудитор:** Уполномочен просматривать архивы и журналы аудита.
- **Владелец данных активации УЦ:** Уполномоченное лицо, владеющее данными активации УЦ, которые необходимы для работы аппаратного модуля безопасности УЦ.

5.2.2 Количество лиц, необходимых для выполнения задачи

Резервное копирование, хранение и восстановление закрытых ключей УЦ осуществляется в физически защищенной среде только доверенных персоналом, как минимум, с двойным контролем.

5.2.3 Идентификация и аутентификация для каждой должности

Прежде чем назначить человека на доверенную должность, GlobalSign проводит проверку его биографии. Каждая должность, описанная выше, идентифицируется и аутентифицируется специальным образом для гарантии, что у соответствующего человека соответствующая должность.

5.2.4 Должности, требующие разделения обязанностей

GlobalSign обеспечивает разделение должностей с помощью оборудования УЦ (логически), процедурно либо сочетанием обоих способов.

Отдельные сотрудники УЦ специально назначаются на должности, определенные в разделе 5.2.1 выше.

Должности, требующие разделения обязанностей:

- Те, кто выполняет утверждение генерации, аннулирования и приостановления сертификатов (специалисты по валидации).
- Лица, выполняющие установку, конфигурирование и обслуживание систем УЦ (инфрасистемные инженеры).
- Лица, несущие общую ответственность за управление безопасностью УЦ. (сотрудники службы безопасности).
- Лица, выполняющие обязанности, связанные с управлением жизненным циклом криптографических ключей, например, хранители ключевых компонентов (владельцы данных активации УЦ).
- Лица, выполняющие разработку систем УЦ (разработчики).
- Лица, выполняющие аудит систем УЦ (инфрасистемные операторы, аудиторы).

5.3 Контроль персонала

5.3.1 Требования к квалификации, опыту и допускам

Перед привлечением любого лица к процессу управления сертификатами в качестве сотрудника, агента или независимого подрядчика компания GlobalSign проверяет его личность и благонадежность.

GlobalSign нанимает персонал с экспертными знаниями, опытом и квалификацией для предлагаемых услуг, в соответствии с должностными обязанностями.

Персонал GlobalSign выполняет это требование благодаря экспертным знаниям, опыту и квалификации, полученным в результате формального обучения и образования,

фактического опыта или их сочетания. Как указано в разделе 5.2.1, доверенные должности и обязанности документируются в должностных инструкциях. Должностные инструкции персонала GlobalSign (как временного, так и постоянного) определяются с точки зрения разделения обязанностей и наименьших привилегий, определения чувствительности должности на основе обязанностей и уровней доступа, проверки биографических данных, обучения и информирования сотрудников. Персонал GlobalSign назначается на доверенные должности официально.

5.3.2 Процедуры проверки биографических данных

У доверенных сотрудников GlobalSign нет конфликта интересов, способного нанести ущерб беспристрастности деятельности УЦ. GlobalSign не назначает на такие должности лиц, ранее осужденных за совершение тяжкого преступления или иного правонарушения, если это влияет на соответствие занимаемой должности. До завершения всех необходимых проверок и анализа результатов персонал не имеет доступа к доверенным функциям (если подобные проверки законны в конкретной юрисдикции). Все доверенные сотрудники отбираются на основе лояльности, благонадежности, добросовестности и проходят проверку биографических данных, если это разрешено законом.

Любое использование информации, выявленной в ходе проверки биографических данных гражданина, должно соответствовать действующему законодательству в его юрисдикции.

5.3.3 Требования к обучению

GlobalSign проводит обучение для всех сотрудников, выполняющих работу по проверке (валидации) информации. Обучение охватывает базовые знания инфраструктуры открытых ключей, политики и процедуры аутентификации и валидации, включая Политику сертификации и/или Положение о сертификационной практике GlobalSign), общие угрозы в процессе проверки информации (включая фишинг и другие тактики социальной инженерии), а также Базовые требования CA/Browser Forum.

GlobalSign ведет учет обучения и гарантирует, что специалисты по проверке обладают соответствующим уровнем квалификации. Прежде чем допустить их к работе, GlobalSign официально фиксирует их навыки, необходимые для выполнения задачи.

Все специалисты по проверке обязаны сдать экзамен УЦ по требованиям к проверке информации, изложенным в Базовых требованиях CA/Browser Forum.

5.3.4 Частота и требования к курсам переподготовки

Доверенные сотрудники поддерживают уровень квалификации в соответствии с ежегодными программами обучения и аттестации GlobalSign.

При любом значительном изменении операций составляется план обучения (информирования), а выполнение плана документируется.

GlobalSign проводит обучение по информационной безопасности и конфиденциальности для всех сотрудников не реже раза в год.

5.3.5 Частота и последовательность ротации рабочих мест

GlobalSign гарантирует, что никакое кадровое изменение не повлияет на операционную эффективность услуги или безопасность системы.

5.3.6 Санкции за несанкционированные действия

К персоналу, нарушающему положения и политику CP, настоящего CPS или операционных процедур, связанных с УЦ, применяются соответствующие дисциплинарные санкции.

5.3.7 Требования к независимым подрядчикам

Делегированная третья сторона и персонал подрядчика, нанятый для выполнения операций GlobalSign, проходит те же процессы, процедуры, оценку, контроль безопасности и обучение, что и постоянный персонал УЦ.

5.3.8 Документация для персонала

GlobalSign предоставляет своим сотрудникам данное CPS, все соответствующие CP, а также любые необходимые уставы, политики и контракты. Другие технические, эксплуатационные и административные документы (например, руководства администратора, руководства пользователя и т. д.) предоставляются для того, чтобы доверенный персонал мог выполнять свои обязанности.

Ведутся записи, кто прошел обучение, и какие материалы усвоил.

5.4 Процедуры ведения журнала аудита

5.4.1 Типы регистрируемых событий

GlobalSign записывает события, связанные с безопасностью их систем сертификатов, систем управления сертификатами и корневых систем CA. GlobalSign записывает события, связанные с действиями, предпринятыми для обработки запроса на сертификат и выдачи Сертификата, включая всю сгенерированную информацию и документацию, полученную в связи с запросом на сертификат; время и дата; и привлеченный персонал.

GlobalSign предоставляет эти записи своему Квалифицированному аудитору в качестве доказательства соблюдения УЦ этих требований.

GlobalSign записывает как минимум следующие события:

События жизненного цикла сертификата УЦ и ключей, включая:

- Генерация ключей, резервное копирование, хранение, восстановление, архивирование и уничтожение.
- Запросы на сертификат, его продление, запросы на перевыпуск и аннулирование ключа.
- Утверждение и отклонение запросов на сертификаты.
- События управления жизненным циклом криптографического устройства.Создание списков отозванных сертификатов;
- Подписание ответов OCSP; и
- Введение новых профилей сертификатов и удаление существующих профилей.

События управления жизненным циклом сертификата, включая:

- Запросы на сертификат, на продление, перевыпуск ключа, приостановку и отзыв.
- Все действия по проверке, предусмотренные настоящим CPS.
- Утверждение и отклонение запросов на сертификаты.
- Выдача сертификатов.
- Генерация списков отзыва сертификатов.
- Подписание ответов OCSP.

События безопасности, включая:

- Успешные и неуспешные попытки доступа к системе PKI.
- Выполненные действия PKI и системы безопасности.
- Изменения профиля безопасности.
- Установка, обновление и удаление программного обеспечения в системе сертификации.
- Системные сбои, аппаратные сбои и другие аномалии.
- Действия брандмауэра и маршрутизатора.
- Входы и выходы из центрального офиса.

5.4.2 Периодичность обработки журнала

Журналы аудита периодически просматриваются.

5.4.3 Срок хранения журнала аудита

GlobalSign и каждая делегированная третья сторона сохраняют соответствующие журналы аудита, по крайней мере, в течение срока хранения, определенного WebTrust и/или требованиями eIDAS или UK eIDAS к типу сертификата.

Срок хранения составляет не менее:

• 10 лет для сертификатов Абонента; или

• через 7 лет после того, как сертификат CA, основанный на журналах, перестает быть действительным.

Если иное не оговорено в соглашении с GlobalSign.

5.4.4 Защита журнала аудита

События регистрируются таким образом, что не могут быть удалены или уничтожены (за исключением переноса на долговременный носитель) в течение всего периода хранения.

Записи о событиях защищены для предотвращения изменений и обнаружения несанкционированного доступа, а также для обеспечения того, чтобы только доверенные роли могли выполнять операции без изменения целостности, подлинности и конфиденциальности данных.

На записи событий проставляется датировка для создания надежной связи между событием и моментом его реализации от создания записи до конца архивного периода.

5.4.5 Процедуры резервного копирования журналов аудита

Журналы аудита хранятся в безопасном месте (например, в несгораемом сейфе), под контролем доверенного лица и отдельно от источника их создания. Резервные копии защищаются в той же степени, что и оригиналы.

5.4.6 Система сбора данных аудита

Процессы аудита начинаются при запуске системы и завершаются только при ее выключении. Система обеспечивает целостность и доступность собранных данных. При необходимости система защищает конфиденциальность данных. В случае возникновения проблемы в процессе сбора данных аудита GlobalSign определяет, следует ли приостановить работу GlobalSign до устранения проблемы.

5.4.7 Уведомление субъекта, вызвавшего событие

Не предусмотрено.

5.4.8 Оценки уязвимостей

GlobalSign ежегодно проводит оценку рисков, которая:

1. Определяет прогнозируемые внутренние и внешние угрозы, которые могут привести к несанкционированному доступу, раскрытию, неправильному использованию, изменению или уничтожению любых данных сертификата или процесса управления сертификатами.
2. Оценивает вероятность и потенциальный ущерб от этих угроз, принимая во внимание чувствительность данных сертификата и процессов управления сертификатами.
3. Оценивает достаточность политики, процедур, информационных систем, технологий и других мер, которые GlobalSign применяет для противодействия таким угрозам.

GlobalSign регулярно проводит оценку уязвимостей и тестирование на проникновение, охватывающее все активы GlobalSign, связанные с выпуском сертификатов, продуктами и услугами. Оценки сосредоточены на внутренних и внешних угрозах, которые могут привести к несанкционированному доступу, фальсификации, модификации, изменению или уничтожению процесса выдачи сертификатов.

5.5 Архивирование записей

5.5.1 Типы архивируемых записей

GlobalSign и каждая делегированная третья сторона архивируют все журналы аудита, как указано в разделе 5.4.1, и:

Документация, относящаяся к безопасности их систем сертификатов, систем управления сертификатами, систем корневого центра сертификации и делегированных сторонних систем; и
Документация, связанная с их проверкой, выдачей и отзывом запросов на получение сертификатов.

5.5.2 Период хранения архива

GlobalSign и каждая делегированная третья сторона сохраняют журналы аудита (как указано в разделе 5.4.1) и записи (как указано в разделе 5.5.1) по крайней мере в течение срока хранения, определенного WebTrust и/или eIDAS или британскими требованиями eIDAS к типу сертификата.

Срок хранения составляет не менее:
10 лет для сертификатов Абонента; или
через 7 лет после того, как сертификат CA, основанный на журналах, перестает быть действительным.

Если иное не указано в соглашении с GlobalSign.
.

5.5.3 Защита архива

Архивы создаются таким образом, что не могут быть удалены или уничтожены (за исключением переноса на долговременные носители) в течение периода хранения. Защита архивов гарантирует, что только авторизованные роли с доверенным доступом могут выполнять операции без изменения целостности, подлинности и конфиденциальности данных. Если исходный носитель не может сохранить данные на оговоренный период, то определяется механизм периодического переноса архивных данных на новый носитель.

5.5.4 Процедуры резервного копирования архива

Онлайновые копии дублируются на регулярной основе, и каждая хранится в месте, отличном от исходной системы. Одна резервная копия хранится в пожаробезопасном сейфе. В конце любой церемонии с ключами (за исключением зашифрованных материалов, которые хранятся отдельно по соответствующим процедурам) создается автономная резервная копия, которая хранится в другом месте в течение 30 дней после церемонии.

5.5.5 Требования к временным меткам записей

Если для датирования записей используется служба временных меток, то она должна соответствовать требованиям в разделе 6.8. Независимо от методов датирования событий, метки времени должны присутствовать во всех журналах.

5.5.6 Система сбора данных для архива (внутренняя или внешняя)

Система сбора данных для архива соответствует требованиям безопасности в разделе 5.

5.5.7 Процедуры получения и проверки архивной информации

Никаких условий.

5.6 Смена ключей

В соответствии с разделом 6.3.2, GlobalSign может периодически менять материал ключей для издающих УЦ. Также в может измениться информация о субъекте сертификата и профили сертификатов для соответствия новым рекомендациям и лучшим практикам. Закрытые ключи, которыми были подписаны предыдущие сертификаты Абонентов, сохраняются до истечения срока действия всех таких сертификатов.

5.7 Компрометация и аварийное восстановление

5.7.1 Порядок реагирования на инциденты и компрометацию

GlobalSign действует в соответствии с Планом реагирования на инциденты и Планом аварийного восстановления. Процедуры для обеспечения бесперебойности операций и аварийного восстановления предусматривают уведомление и разумную защиту поставщиков прикладного программного обеспечения, Абонентов и доверяющих сторон в случае аварии, нарушения безопасности или сбоя в работе.

GlobalSign не раскрывает упомянутые процедуры Абонентам, доверяющим сторонам и разработчикам стороннего ПО, но предоставит их по запросу аудиторам УЦ GlobalSign.

GlobalSign ежегодно тестирует, проверяет и обновляет эти процедуры. План обеспечения бесперебойности операций включает в себя:

1. Условия активации плана.
2. Процедуры действий в чрезвычайных ситуациях.
3. Процедуры резервного копирования.
4. Процедуры возобновления работы.
5. График обслуживания плана.
6. Требования по осведомленности и обучению сотрудников.
7. Обязанности отдельных лиц.
8. План по времени восстановления (RTO).
9. Регулярное тестирование плана действий в чрезвычайных ситуациях.
10. План GlobalSign по поддержанию или своевременному восстановлению бизнес-операций УЦ после сбоя критически важных бизнес-процессов.
11. Требование хранить критические криптографические материалы (т.е. защищенное криптографическое устройство и материалы активации) в альтернативном месте.
12. Что представляет собой приемлемый перерыв в работе системы и время восстановления.
13. Как часто делаются резервные копии важной деловой информации и программного обеспечения.
14. Удаленность объектов восстановления от основного места УЦ.
15. Процедуры обеспечения безопасности объекта в максимально возможной степени в течение периода времени после инцидента и до восстановления безопасной среды на исходном или удаленном объекте.

5.7.2 Повреждение вычислительной техники, программного обеспечения и/или данных

Если какое-то оборудование повреждено, но закрытые ключи не уничтожены, то следует как можно быстрее восстановить работу. В соответствии с планом аварийного восстановления GlobalSign, в первую очередь восстанавливается функция генерации ответов о состоянии сертификатов.

5.7.3 Процедура действий в случае компрометации закрытого ключа организации

В случае компрометации, потери, уничтожения или подозрения на компрометацию закрытого ключа УЦ GlobalSign действует следующая процедура:

- После расследования проблемы GlobalSign решает, следует ли отозвать сертификат GlobalSign. Если да, то:
    - Все Абоненты уведомляются при первой же возможности.
    - Генерируется новая пара ключей GlobalSign или для создания новых сертификатов используется альтернативная иерархия существующих УЦ.

5.7.4 Доступность информации о статусе отзыва

В случае компрометации ключа УЦ информация о статусе отзыва предоставляется и хранится в общедоступном месте. Если это требуется, услуги по предоставлению статусов сертификатов предоставляет другая организация GMO Internet Group.

5.7.5 Обеспечение непрерывности бизнеса после катастрофы

План восстановления после катастрофы касается непрерывности бизнеса, как описано в разделе 5.7.1. Системы выдачи статуса сертификатов должны быть развернуты таким образом, чтобы обеспечить доступность 24 часа в сутки, 365 дней в году.

5.8 Прекращение деятельности УЦ или РЦ

Если необходимо прекратить деятельность выпускающего УЦ или РЦ, последствия такого прекращения сводятся к возможному минимуму в свете сложившихся обстоятельств и регулируются соответствующими соглашениями с выпускающим УЦ и/или регистрационным центром. Выпускающие УЦ GlobalSign определяют процедуры, которым будут следовать при полном или частичном прекращении деятельности по выпуску и управлению цифровыми сертификатами. Эти процедуры должны, как минимум:

- минимизировать любые сбои, вызванные прекращением деятельности выпускающего УЦ;
- сохранить архивные записи выпускающего УЦ;
- своевременно уведомить о прекращении действия сертификата всех Абонентов, уполномоченных доверяющих сторон, поставщиков прикладного программного обеспечения и другие заинтересованные стороны, участвующие в жизненном цикле сертификата GlobalSign;
- поддерживать информационный сервис о статусе сертификатов в течение соответствующего периода после прекращения действия сертификата, включая, при необходимости, передачу информационного сервиса о статусе сертификатов другой организации GMO Internet Group;
- обеспечить процесс отзыва всех цифровых сертификатов, выданных УЦ-эмитентом на момент прекращения действия сертификата;
- уведомить всех аудиторов, включая органы по оценке соответствия eIDAS/UK eIDAS;
- уведомить надзорный орган eIDAS Бельгии (FPS Economy, отдел Quality and Safety); уведомить надзорный орган eIDAS Великобритании (Управление комиссара по информации);
- уведомить другие соответствующие государственные и сертификационные органы в соответствии с законодательством и нормативными актами.

5.8.1 Преемник выпускающего сертификационного центра

В рамках разумной практичности преемник выпускающего УЦ принимает те же права и обязательства, что и прекративший свою деятельность выпускающий УЦ. Преемник выпускающего УЦ должен выдать новые ключи и сертификаты всем Абонентам, чьи ключи и сертификаты отозваны прекратившим свою деятельность выпускающим УЦ, при условии, что индивидуальный поставщик услуг или пользователь подаст заявку на новый сертификат и выполнит требования по первоначальной регистрации, идентификации и аутентификации, включая заключение нового соглашения с поставщиком услуг или владельцем сертификата.

6.0 Технические средства контроля безопасности

6.1 Генерация и установка пары ключей

6.1.1 Генерация пары ключей

6.1.1.1 Генерация пары ключей УЦ

For Root CA Key Pairs, GlobalSign performs the following controls.

1. Подготавливает сценарий генерации ключей и следует ему.
2. Приглашает квалифицированного аудитора, который наблюдает за процессом генерации пары ключей корневого УЦ или записывает видео всего процесса генерации пары ключей корневого УЦ.
3. Квалифицированный аудитор выдает заключение о том, что GlobalSign следовала своему сценарию церемонии генерации ключей в процессе генерации ключей и сертификатов, а также о средствах контроля, используемых для обеспечения целостности и конфиденциальности пары ключей.

В других парах ключей УЦ GlobalSign выполняет следующие меры контроля:

1. Генерирует ключи УЦ с помощью доверенных лиц из числа сотрудников, в соответствии с принципами контроля нескольких лиц и разделения знаний.
2. Генерирует ключи УЦ с помощью доверенных лиц из числа сотрудников в соответствии с принципами разделения полномочий и разделения знаний.
3. Генерирует ключи УЦ в рамках криптографических модулей, отвечающих применимым техническим и бизнес-требованиям, как раскрыто в Политике сертификации УЦ и/или Положении о сертификационной практике.
4. Ведет журнал своей деятельности по генерации ключей УЦ.
5. Поддерживает эффективный контроль для обеспечения разумной уверенности в том, что закрытый ключ сгенерирован и защищен в соответствии с процедурами, описанными в Политике сертификации и/или Положении о сертификационной практике и (если применимо) в сценарии генерации ключей.

6.1.1.2 Генерация пары ключей Абонента

Для ключей Абонента, сгенерированных GlobalSign, генерация ключей выполняется в соответствии с требованиями CA/Browser Forum на безопасном криптографическом устройстве, соответствующем FIPS 140-2 (или эквивалентному), с использованием алгоритма генерации ключей и размера ключа, как указано в разделе 6.1.5. и 6.1.6.

GlobalSign отклоняет запрос на сертификат, если он содержит заведомо слабый закрытый ключ.

Ключи, используемые для сертификатов подписи кода, должны быть сгенерированы на аппаратном криптомодуле форм-фактора устройства, сертифицированном как соответствующий как минимум FIPS 140-2 уровня 2 или общим критериям EAL 4+.

Для квалифицированных сертификатов, в которых закрытый ключ генерируется GlobalSign или третьей стороной от имени субъекта, закрытый ключ должен генерироваться и надежно храниться, пока он находится у GlobalSign или третьей стороны. Если устройство управляется третьей стороной от имени субъекта, GlobalSign должна проверить, что эта третья сторона отвечает соответствующим требованиям в отношении квалификации.

Защищенное криптографическое устройство необязательно для квалифицированных сертификатов, выданных в соответствии с политикой QCP-n или QCP-l.

Для квалифицированных сертификатов если закрытый ключ, связанный с сертифицированным открытым ключом, находится в признанном устройстве создания квалифицированной подписи (QSCD), ключи Абонентов генерируются и хранятся в QSCD. Статус сертификации QSCD контролируется, и в случае изменения статуса сертификации QSCD будут приняты соответствующие меры, включая аннулирование.

6.1.2 Доставка закрытого ключа Абоненту

GlobalSign не генерирует закрытые ключи для публично доверенных сертификатов SSL или сертификатов подписи кода.

Удостоверяющие центры GlobalSign создают личные ключи от имени Абонентов только если имеют такое право и только в том случае, если в процессе создания ключей и их последующей выдачи Абоненту поддерживается достаточный уровень безопасности.

Для непублично доверенных SSL-сертификатов это достигается путем использования файлов PKCS#12 (.pfx) с личными ключи и сертификатами, зашифрованными паролем как минимум из шестнадцати (16) символов. Не менее восьми (8) символов генерируются системой и предоставляются Абоненту в процессе регистрации, а Абонент выбирает не менее восьми (8) своих символов. Для сертификатов SMIME это достигается за счет использования файлов PCKS#12 (.pfx), содержащих личные ключи и сертификаты, зашифрованные минимальным паролем из семнадцати (17) буквенно-цифровых символов, выбранных Абонентом.

Для квалифицированных сертификатов управление закрытыми ключами может осуществляться GlobalSign или третьей стороной от имени субъекта. Если управление закрытым ключом осуществляется от имени субъекта, GlobalSign должна обеспечить субъекту единоличный контроль (или, если субъект является юридическим лицом, «контроль») над его закрытым ключом. GlobalSign подтверждает, что третья сторона является квалифицированным поставщиком доверительных услуг и обеспечивает единоличный контроль.

Для квалифицированных сертификатов, в которых закрытый ключ находится на QSCD, если GlobalSign или третья сторона управляет QSCD для субъекта, закрытый ключ не должен использоваться для подписи, кроме как в пределах QSCD. Пара закрытых ключей субъекта используется только для электронных подписей или печатей соответственно.

Для квалифицированных сертификатов GlobalSign генерирует закрытые ключи только в том случае, если управляет закрытым ключом от имени Абонента.

GlobalSign обеспечивает целостность любых открытых/закрытых ключей и случайность материала ключа с помощью подходящего ГСЧ или ГПСЧ. Если GlobalSign обнаруживает или подозревает, что закрытый ключ передан неуполномоченному лицу или организации, не связанной с Абонентом, то отзывает все сертификаты, включающие открытый ключ, соответствующий переданному закрытому ключу.

6.1.3 Доставка открытого ключа эмитенту сертификата

УЦ GlobalSign принимают от РЦ только те открытые ключи, которые были защищены во время транспортировки и подлинность и целостность происхождения которых от РЦ соответствующим образом проверена.

6.1.4 Передача открытых ключей УЦ доверяющим сторонам

GlobalSign гарантирует, что ее открытые ключи доставляются доверяющим сторонам таким образом, чтобы предотвратить подмену. Коммерческим веб-браузерам и операторам платформ рекомендуется встраивать открытые ключи корневых сертификатов в свои корневые хранилища и операционные системы. Открытые ключи выпускающих УЦ предоставляются Абонентом в виде цепочки сертификатов или через репозиторий, управляемый GlobalSign, и ссылаются на профиль выданного сертификата через AIA (Authority Information Access).

6.1.5 Размеры ключей

GlobalSign следует специальной публикации NIST 800-133, редакция 2 (2020 г.) — «Рекомендации по генерации криптографических ключей» — в отношении рекомендуемых сроков и передового опыта в выборе пар ключей для корневых центров сертификации, выпускающих центров сертификации и сертификатов конечных объектов, доставляемых Абонентам.

GlobalSign выбирает следующие размеры ключей/хэши для корневых сертификатов, сертификатов выдачи сертификатов CA и сертификатов конечного объекта, а также ответчиков статуса сертификатов CRL/OCSP. Эти варианты соответствуют требованиям форума CA/браузера.

Сертификаты должны соответствовать следующим требованиям к типу алгоритма и размеру ключа.

Сертификаты корневого центра сертификации

	Срок действия начинается до 31 декабря 2010 года включительно	Срок действия начинается после 31 декабря 2010 года
Алгоритм дайджеста	SHA-1, SHA-256, SHA-384 или SHA- 512	SHA-256, SHA-384 или SHA-512

Минимальный размер модуля RSA (бит)	2048 [5]	2048
Кривая ECC	NIST P-256, P-384 или P-521	NIST P-256, P-384 или P-521

Подчиненные сертификаты

	Срок действия начинается до 31 декабря 2010 года включительно и заканчивается до 31 декабря 2013 года включительно	Срок действия начинается после 31 декабря 2010 года или заканчивается после 31 декабря 2013 года
Алгоритм дайджеста	SHA-1, SHA-256, SHA-384 или SHA- 512	SHA-1[6], SHA-256, SHA-384 или SHA-512
Минимальный размер модуля RSA (бит)	1024	2048
Кривая ECC	NIST P-256, P-384 или P-521	NIST P-256, P-384 или P-521

Сертификаты Абонентов

Алгоритм дайджеста	SHA-1[7], SHA-256, SHA-384 или SHA- 512
Минимальный размер модуля RSA (бит)	2048
Кривая ECC	NIST P-256, P-384 или P-521
RSASSA-PSS[8]	

С 1 июля 2017 года минимальный размер ключа для новых сертификатов корневых УЦ, создающих подчиненные УЦ для AATL, составляет RSA 3072-бит или ECC NIST P-384.

С 1 января 2021 года минимальный размер ключа для новых сертификатов корневых и подчиненных УЦ, выдающих сертификаты подписи кода и временных меток, составляет RSA 3072-бит или ECC NIST P-256.

С 1 июня 2021 года минимальный размер ключа для новых пользовательских сертификатов подписи кода и временных меток составляет RSA 3072-бит или ECC NIST P-256.

6.1.6 Генерация параметров открытого ключа и проверка качества

GlobalSign генерирует пары ключей в соответствии со стандартом FIPS 186 и использует разумные методы проверки пригодности открытых ключей Абонентов. Известные слабые ключи проверяются и отклоняются в момент представления. GlobalSign следует применимым требованиям CA/Browser Forum в отношении создания пары ключей и проверки качества.

---

[5] *Размер модуля ключа RSA кратен 8 бит. Сертификат корневого УЦ, выпущенный до 31 декабря 2010 года с размером ключа RSA менее 2048 бит, МОЖЕТ все еще служить якорем доверия для сертификатов Абонентов, выпущенных в соответствии с этими Требованиями.*

[6] *SHA-1 может использоваться для сертификатов подчиненных УЦ IntranetSSL, но они не подключаются в цепочку к публично доверенным корням.*

[7] *SHA-1 может использоваться для сертификатов Абонентов УЦ IntranetSSL, но они не подключаются в цепочку к публично доверенным корням.*

[8] *RSASSA-PSS может использоваться с ключами RSA для сертификатов PersonalSign в соответствии с критериями, определенными в разделе 7.1.3.*

6.1.7 Цели использования ключей (в соответствии с полем Key Usage X.509 v3)

GlobalSign устанавливает область использования ключей сертификатов с помощью специального поля Key Usage для X.509 v3 (см. раздел 7.1).

Закрытые ключи от корневых сертификатов не используются для подписи сертификатов, за исключением следующих случаев:

1. Самоподписанные сертификаты для представления самого корневого УЦ.
2. Сертификаты для подчиненных УЦ и перекрестные сертификаты.
3. Сертификаты для проверки ответов OCSP.

6.2 Защита секретного ключа и инженерный контроль криптографического модуля

6.2.1 Стандарты и управление криптографическим модулем

GlobalSign защищает свои закрытые ключи CA в системе или устройстве, которое было проверено на соответствие как минимум FIPS 140-2 уровень 3, FIPS 140-3 уровень 3 или соответствующему профилю защиты общих критериев или целевому показателю безопасности, EAL 4 (или выше), который включает требования по защите закрытого ключа и других активов от известных угроз.
GlobalSign шифрует свой закрытый ключ с помощью алгоритма и длины ключа, которые, в соответствии с современным уровнем техники, способны противостоять криптоаналитическим атакам в течение остаточного срока службы зашифрованного ключа или части ключа.
Для сертификатов, к которым применяются особые требования к защите личного ключа Абонента, GlobalSign по контракту обяжет Абонента использовать такую систему или предоставить подходящий механизм, гарантирующий защиту.

6.2.2 Управление закрытым ключом несколькими лицами (n из m)

Для криптографических операций GlobalSign может активировать закрытые ключи под контролем нескольких доверенных лиц (с данными активации УЦ). Для доступа к такому управлению доверенные лица проходят строгую аутентификацию (например, токен с PIN-кодом).

6.2.3 Депонирование закрытого ключа

GlobalSign никогда не осуществляет депонирование закрытых ключей.

6.2.4 Резервное копирование закрытых ключей

GlobalSign создает резервные копии закрытых ключей УЦ под таким же контролем нескольких лиц, как и оригинальный закрытый ключ.

GlobalSign выполняет резервное копирование личных ключей Абонентов только для квалифицированных сертификатов, где личный ключ находится на QSCD, управляемом GlobalSign от имени субъекта. Личные ключи копируются в резервные копии с таким же контролем безопасности, что и оригинальная копия.

6.2.5 Архивирование закрытых ключей

GlobalSign не архивирует личные ключи Абонентов

6.2.6 Передача закрытого ключа в криптографический модуль или из него

Закрытые ключи УЦ GlobalSign генерируются, активируются и хранятся в аппаратных модулях безопасности. При копировании за пределы модуля (для хранения или передачи) они шифруются. Личные ключи никогда не передаются открытым текстом.

Если GlobalSign станет известно, что закрытый ключ УЦ передан неуполномоченному лицу или организации, не связанной с УЦ, то GlobalSign отзовет все сертификаты с соответствующим открытым ключом.

6.2.7 Хранение закрытых ключей на криптографическом модуле

GlobalSign хранит закрытые ключи УЦ на устройстве, отвечающем требованиям раздела 6.2.1.

6.2.8 Метод активации закрытого ключа

GlobalSign несет ответственность за активацию закрытых ключей УЦ в соответствии с инструкциями и документацией от производителя аппаратного модуля безопасности. Абоненты несут ответственность за защиту закрытых ключей в соответствии с обязательствами, представленными в форме Абонентского договора или Условий использования.

6.2.9 Способ деактивации закрытого ключа

GlobalSign деактивирует закрытые ключи УЦ в соответствии с инструкциями и документацией, предоставленными производителем аппаратного модуля безопасности.

6.2.10 Метод уничтожения закрытого ключа

GlobalSign уничтожает закрытые ключи УЦ в соответствии с инструкциями и документацией, предоставленными производителем аппаратного модуля безопасности.
Закрытые ключи Абонентов, сгенерированные GlobalSign в GCC, хранятся в формате PKCS#12, а через 30 дней с момента генерации пара ключей автоматически удаляется.

6.2.11 Рейтинг криптографических модулей

См. раздел 6.2.1.

6.3 Другие аспекты управления парой ключей

6.3.1 Архивирование открытых ключей

GlobalSign архивирует открытые ключи от сертификатов.

6.3.2 Сроки действия сертификатов и пар ключей

У сертификатов есть максимальный срок действия:

Тип	Максимальный период использования пары ключей	Максимальный срок действия
Корневые сертификаты[9]	Не применимо	28 лет
Корневые сертификаты TPM	30 лет	41 год
Публично доверенные подчиненные УЦ	Не применимо	18 лет
Сертификаты PersonalSign	Не применимо	39 месяцев
Сертификаты подписи кода	Не применимо	39 месяцев
Сертификаты подписи кода EV	Не применимо	39 месяцев

[9] 2048-битные ключи, созданные до 2003 года с использованием RSA, могут использоваться в течение максимально разрешенного периода в соответствующих корневых хранилищах.

Строгие и многофункциональные сертификаты S/MIME	Не применимо	825 дней
S/MIME legacy Certificates	Не применимо	1185 дней
Сертификаты конечных субъектов AATL	Не применимо	39 месяцев
Квалифицированные сертификаты для электронных подписей и печатей	Не применимо	39 месяцев
Сертификаты DV SSL	Не применимо	398 дней
Сертификаты AlphaSSL	Не применимо	398 дней
Сертификаты OV SSL	Не применимо	398 дней
Сертификаты EV SSL	Не применимо	398 дней
Квалифицированные сертификаты аутентификации веб-сайта	Не применимо	398 дней
Intranet SSL	Не применимо	5 лет
Сертификаты для меток времени	15 месяцев	11 лет
Сертификаты NAESB	2 года	2 года
Сертификаты агента восстановления/архивирования закрытого ключа	Не применимо	5 лет

Для целей расчетов день измеряется как 86 400 секунд. Любое количество времени, превышающее это значение, включая доли секунды и/или дополнительные секунды, представляет собой дополнительный день. По этой причине сертификаты Абонента НЕ должны выпускаться на максимально допустимый срок по умолчанию, чтобы учесть такие корректировки.

Максимальный срок действия Сертификатов конечного субъекта с EKU id-kp-emailProtection составляет 1185 дней.

Период использования пары ключей может достигать срока действия сертификата.

Срок действия сертификатов, подписанных определенным центром сертификации, должен истекать до или в конце периода действия сертификата этого центра сертификации.

GlobalSign соответствует требованиям CA/Browser Forum в отношении максимального срока действия.

6.4 Данные активации

6.4.1 Генерация и установка данных активации

Генерация данных для активации закрытых ключей УЦ GlobalSign происходит во время церемонии ключа (см. Раздел 6.1.1). Данные активации генерируются либо автоматически соответствующим HSM, либо другим способом, отвечающим тем же требованиям. Затем они доставляются доверенному сотруднику, владельцу доли ключа. Метод доставки обеспечивает конфиденциальность и целостность данных активации.

6.4.2 Защита данных активации

Данные активации выпускающего УЦ защищены от раскрытия с помощью комбинации криптографических и физических механизмов контроля доступа. Данные активации GlobalSign хранятся на смарт-картах.

6.4.3 Другие аспекты данных активации

Данные активации GlobalSign могут храниться только у сотрудников GlobalSign на доверенных должностях.

6.5 Средства контроля компьютерной безопасности

6.5.1 Специфические технические требования к компьютерной безопасности

Следующие функции компьютерной безопасности обеспечиваются операционной системой или в сочетаниии ОС, ПО и физических средств защиты. Компоненты GlobalSign PKI должны включать следующие функции:

- Аутентификация персонала на доверенной должности.
- Избирательный доступ по принципу наименьших привилегий.
- Возможность аудита безопасности (защита целостности).
- Запрет на повторное использование объектов.
- Требование надежной политики паролей.
- Требование использования криптографии для сеансов связи.
- Требование надежной идентификации и аутентификации.
- Средства защиты от вредоносного кода.
- Средства для поддержания целостности программного обеспечения и микропрограммы.
- Изоляция домена и разделение для различных систем и процессов.
- Обеспечение самозащиты операционной системы.

GlobalSign использует многофакторную аутентификацию для учетных записей, способных напрямую инициировать выдачу сертификатов.

6.5.2 Рейтинг компьютерной безопасности

Не предусмотрено.

6.6 Технические средства контроля жизненного цикла

6.6.1 Средства контроля разработки системы

Контроль разработки системы для GlobalSign заключается в следующем:

- Использовать программное обеспечение, спроектированное и разработанное в соответствии с формальной, документированной методологией разработки.
- При вводе в эксплуатацию все аппаратные средства проверяются на соответствие требованиям и отсутствие признаков внешнего вмешательства. Аппаратное и программное обеспечение закупается так, чтобы снизить вероятность закладок в конкретные компоненты (например, случайным отбором оборудования при закупке).
- Аппаратное и программное обеспечение разрабатывается в контролируемой среде, а процессы разработки формализованы и документированы. Это требование не относится к коммерческому готовому оборудованию или программному обеспечению.
- Всё аппаратное и программное обеспечение должно быть предназначено только для работы УЦ. Не используется никаких посторонних приложений, устройств, сетевых соединений или компонентов ПО.
- Принимаются надлежащие меры для предотвращения загрузки на оборудование вредоносного ПО. На устройства устанавливаются только те приложения, которые необходимы для выполнения операций УЦ и получены из источников, разрешенных локальной политикой. При первом использовании и периодически после этого оборудование и программное обеспечение GlobalSign проверяется на вредоносный код.
- Обновления оборудования и программного обеспечения приобретаются или разрабатываются таким же образом, как и оригинальное оборудование. Их установка производится утвержденным персоналом в установленном порядке.

6.6.2 Контроль управления безопасностью

Конфигурация систем GlobalSign, а также любые модификации и обновления документируются и контролируются руководством GlobalSign. Действует механизм обнаружения несанкционированного изменения программного обеспечения или конфигурации GlobalSign. При установке и текущем обслуживании систем используется

формальная методология управления конфигурацией. При первой загрузке проверяется аутентичность происхождения программного обеспечения GlobalSign, отсутствие модификаций и правильная версия.

6.6.3 Контроль безопасности жизненного цикла

GlobalSign поддерживает схему обслуживания для обеспечения уровня доверия к программному и аппаратному обеспечению. Эта схема оценивается и сертифицируется.

6.7 Средства контроля сетевой безопасности

Компоненты GlobalSign PKI реализуют соответствующие меры безопасности для защиты от атак типа «отказ в обслуживании» и вторжений. Среди них физическая защита оборудования, использование брандмауэров и фильтрующих маршрутизаторов. Неиспользуемые сетевые порты и службы отключены. Любые устройства пограничного контроля для защиты сети с оборудованием PKI запрещают все службы, кроме необходимых для оборудования PKI, даже если эти службы разрешены для других устройств в сети.

6.8 Метки времени

Все компоненты GlobalSign регулярно синхронизируются с надежной службой времени. GlobalSign использует один источник GPS и три неаутентифицированных источника NTP, определяя корректное время для:

- Начального времени действия сертификата УЦ.
- Отзыва сертификата УЦ.
- Публикация обновлений COC.
- Выдачи сертификатов для Абонентов и конечных субъектов.

Для поддержания системного времени могут использоваться электронные или ручные процедуры. Корректировка часов является проверяемым событием.

6.8.1 Сервисы временных меток для подписи PDF

Все цифровые подписи PDF, созданные соответствующим сертификатом, могут включать доверенную временную метку с RFC3161-совместимого сервера Центра сертификации времени (TSA), привязанного к корневому сертификату GlobalSign. Сертификат TSA должен быть расположен в HSM-устройстве стандарта FIPS 140-2 уровня 3 или выше.

6.8.2 Сервисы временных меток для подписи кода и подписи кода EV

Все цифровые подписи, созданные сертификатами подписи кода и подписи кода EV, могут включать доверенную временную метку с RFC3161-совместимого сервера TSA, привязанного к корневому сертификату GlobalSign. Сертификат TSA должен быть расположен в HSM-устройстве стандарта FIPS 140-2 уровня 3 или выше.

7.0 Профили сертификатов, COC и OCSP

7.1 Профиль сертификата

7.1.1 Номер(а) версии

GlobalSign выпускает сертификаты в соответствии с X.509 версии 3.

Расширения сертификата

GlobalSign выпускает сертификаты в соответствии с RFC 5280 и соответствующими Базовыми требованиями, за исключением случаев, упомянутых в данном документе. Критичность тоже следует лучшей практике, чтобы предотвратить ненужные риски для доверяющих сторон в отношении ограничений имен.

Сертификаты подчиненных УЦ и конечных субъектов включают расширение Extended Key Usage с одним или несколькими идентификаторами KeyPurposeId для описания предполагаемого использования сертификата. KeyPurposeId anyExtendedKeyUsage не включается в публично доверенные сертификаты конечных субъектов.

7.1.2 Идентификаторы объектов для алгоритмов

GlobalSign выпускает сертификаты со следующими алгоритмами и идентификаторами OID:

SHA1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 5}*
SHA256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 11}
SHA384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 12}
SHA512WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 13}

ECDSAWithSHA256	{iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2(3) 2}
ECDSAWithSHA384	{iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2(3) 3}
ECDSAWithSHA512	{iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2(3) 4}
RSASSA-PSS	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) rsassa-pss(10)}

*Не используется для подписи публично доверенных сертификатов конечных субъектов.

GlobalSign использует алгоритмы подписи и кодировки в соответствии с применимыми требованиями форума CA/браузера, раздел 7.1.3.

7.1.3 Формы имен

GlobalSign выпускает сертификаты с формами имен, соответствующими RFC 5280 и разделу 7.1.4 требований CA/Browser Forum.

Сертификаты S/MIME могут включать имя участника-пользователя (UPN) в записиotherName в расширении subjectAltName.
Сертификаты ответчика OCSP могут включать атрибут субъекта серийного номера для выполнения требований уникальности DN.

7.1.4 Ограничения на имена

GlobalSign может выпускать сертификаты подчиненных УЦ с ограничениями имен, и отмечать их как критические, если это необходимо. Если ограничения имени НЕ установлены для подчиненного УЦ, то он должен быть подвергнут полному аудиту, указанному в разделе 8.0 настоящего документа.

GlobalSign ограничивает имена следующими методами:
• Если сертификат включает использование расширенного ключа id-kp-serverAuth, то имя сертификата должно быть ограничено ограничениями на dNSName, iPAddress и DirectoryName, как описано в разделе 7.1.2.5.2 Базовые требования для TLS.
• Если сертификат включает использование расширенного ключа id-kp-emailProtection, для каждого имени rfc822Name в разрешенных поддеревьях каждое имя rfc822Name должно содержать либо полное доменное имя, либо символ U+002E FULL STOP («.»), за которым следует полное доменное имя. Имя rfc822Name не должно содержать адрес электронной почты. GlobalSign должна подтвердить, что Заявитель зарегистрировал полное доменное имя, содержащееся в rfc822Name, или был уполномочен владельцем регистрации домена действовать от имени регистранта в соответствии с методами проверки, указанными в Разделе 3.2.2.3 Базовых требований для S/MIME.

7.1.5 Идентификатор объекта политики сертификатов

GlobalSign предъявляет следующие требования:

Тип сертификата	**Источник**	**Раздел**
TLS	Базовые требования	7.1.6
EV TLS	Рекомендации EV	9.3.2
Code Signing и EV Code Signing	Базовые требования к подписи кода	7.1.6
S/MIME	Базовые требования для S/MIME	7.1.6

Примечание. С 1 сентября 2023 г. все сертификаты S/MIME, подпадающие под действие базовых требований для S/MIME, должны включать идентификатор политики S/MIME BR для подтверждения соответствия базовым требованиям для S/MIME. До 1 сентября 2023 г. может быть включен идентификатор политики S/MIME BR.

7.1.6 Использование расширения ограничений политики

Не предусмотрено.

7.1.7 Синтаксис и семантика квалификаторов политики

GlobalSign выпускает сертификаты с квалификатором политики и может включать соответствующий текст для пояснения доверяющим сторонам.

7.1.8 Семантика обработки для расширения критических политик сертификата

Не предусмотрено.

7.1.9 Серийные номера

Сертификаты каждого подчиненного УЦ должны включать уникальный (в контексте доменного имени и серийного номера УЦ) непоследовательный серийный номер сертификата больше нуля (0), содержащий по крайней мере 64 бита вывода из криптографически стойкого ГСПЧ (CSPRNG).

В качестве исключения из RFC 5280 в сертификатах TLS у пресертификата TLS и сертификата одно и то же значение serialNumber.

7.1.10 Специальные положения для квалифицированных сертификатов

Квалифицированные сертификаты конфигурируются в соответствии с применимыми требованиями профилей ETSI EN 319 412 и ETSI TS 119 495.

7.1.10.1 Квалифицированные сертификаты для электронных подписей

Квалифицированные сертификаты для электронных подписей содержат следующие qcStatements:

- id-etsi-qcs-QcCompliance
- id-etsi-qct-esign

Если закрытый ключ, связанный с сертифицированным открытым ключом, находится в QSCD, то добавляется поле "id-etsi-qcs-QcSSCD".

Квалифицированные сертификаты для электронных подписей, которые выдаются в соответствии с UK eIDAS, включают в себя поле "id-etsiqcs-QcCClegislation" со значением GB.

7.1.10.2 Квалифицированные сертификаты для электронных печатей

Квалифицированные сертификаты для электронных печатей содержат следующие qcStatements:

- id-etsi-qcs-QcCompliance
- id-etsi-qct-eseal

Если закрытый ключ, связанный с сертифицированным открытым ключом, находится в QSCD, то добавляется поле "id-etsi-qcs-QcSSCD".

Квалифицированные сертификаты для электронных печатей, выпущенные для использования в Open Banking, включают в себя поле "id-etsi-psd2qcStatement".

Квалифицированные сертификаты для электронных печатей, которые выдаются в соответствии с UK eIDAS, включают поле "id-etsi-qcsQcCClegislation" со значением GB.

7.1.10.3 Квалифицированные сертификаты веб-аутентификации

Квалифицированные сертификаты веб-аутентификации содержат следующие квалификационные утверждения:

- id-etsi-qcs-QcCompliance
- id-etsi-qct-web

Квалифицированные сертификаты веб-аутентификации, выпущенные для использования в Open Banking, содержат "id-etsi-psd2qcStatement".

Квалифицированные сертификаты веб-аутентификации, выданные в соответствии с UK eIDAS, включают в себя поле "id-etsi-qcsQcCClegislation" со значением GB.

7.2 Профиль COC

7.2.1 Номер(а) версий

GlobalSign выпускает списко отзыва сертификатов (COC) версии 2 в соответствии с RFC 5280. Список включает следующие поля:

- **Issuer** DN субъекта для выпускающего УЦ
- **Effective date** Дата и время
- **Next update** Дата и время
- **Signature Algorithm** sha256RSA и др. (в зависимости от продукта)
- **Signature Hash Algorithm** sha256 и др. (в зависимости от продукта)
- **Serial Number(s)** Список отозванных серийных номеров
- **Revocation Date** Дата отзыва

7.2.2 Расширения COC и записей COC

У списков COC следующие расширения:

- **CRL Number** Монотонно возрастающий серийный номер каждого COC
- **Authority Key Identifier** AKI выпускающего УЦ для соблюдения требований к цепочке/валидации

Поддерживаются следующие расширения:

- **ReasonCode** Определяет причину отзыва сертификата

Расширения указываются в записях COC для сертификатов корневых и подчиненных УЦ, включая перекрестные сертификаты. Поддерживаемые значения: keyCompromise (1), affiliationChanged (3), supersed (4), cessationOfOperation (5), privilegeWithdrawn (9).

Расширение может включаться в запись COC также для сертификата конечного субъекта Абонента. Поддерживаемые значения: keyCompromise (1), affiliationChanged (3), supersed (4), cessationOfOperation (5), certificateHold (6), privilegeWithdrawn (9).

Для SSL-сертификатов, сертиифкатов подписи кода или S/MIME BR значение certificateHold (6) не поддерживается.

7.3 Профиль OCSP

Компания GlobalSign использует онлайн-профиль статуса сертификата (OCSP) в соответствии с RFC 6960 и RFC 5019, на что указывает расширение AIA через URL-адрес OCSP-профиля.

7.3.1 Номер(а) версий

GlobalSign выпускает ответы OCSP версии 1 со следующими полями:

- Responder ID — Хэш SHA-1 открытого ключа ответчика
- Produced Time — Время, когда был подписан ответ
- Certificate Status — Статус сертификата по ссылке (хороший/отозван/неизвестный)
- ThisUpdate/NextUpdate — Рекомендуемый интервал валидности для ответа
- Signature Algorithm — SHA256, RSA и др. (в зависимости от продукта)
- Signature — Значение подписи, генерируемое ответчиком
- Certificates — Сертификат OCSP-ответчика

Запрос OCSP должен содержать следующие данные:

- Версия протокола
- Запрос на обслуживание
- Идентификатор целевого сертификата

Поддерживаются следующие поля:

- revocationReason — Определяет причину отзыва сертификата.

Это поле присутствует в ответах OCSP для сертификата корневого или подчиненного УЦ, включая перекрестные сертификаты, и может присутствовать для сертификата конечного субъекта Абонента, если сертификат отозван. Поле CRLReason содержит серийный номер COC, как указано в разд. 7.2.2.

7.3.2 Расширения OCSP

SingleExtensions ответа OCSP не содержит расширение записи CRL ReasonCode (OID 2.5.29.21).

8.0 Аудит соответствия и другие оценки

Процедуры данного CPS разработаны для соответствия требованиям, перечисленным в разделе 1.0. Они охватывают все соответствующие части применимых в настоящее время стандартов PKI для различных вертикальных отраслей PKI, в которых работает GlobalSign.

8.1 Частота и обстоятельства оценки

Компания GlobalSign подтверждает соответствие стандартам WebTrust/eIDAS/UK eIDAS, указанным в разделе 1.0, с помощью квалифицированного аудитора на ежегодной (WebTrust), двухгодичной (eIDAS/UK eIDAS) и непрерывной основе.

8.2 Идентификация/квалификация аудитора

Аудит GlobalSign проводится «квалифицированным аудитором» со следующими квалификациями и навыками:

- Независимость от объекта аудита.
- Способность проводить аудит, отвечающий критериям, указанным в разделе 8.0 «Квалифицированный аудит» настоящего документа.
- Привлекает лиц, обладающих знаниями в области изучения технологии инфраструктуры открытых ключей, инструментов и методов информационной безопасности, аудита информационных технологий и безопасности, а также функции аттестации третьей стороны.
- Сертифицирован, аккредитован, лицензирован или иным образом оценен как отвечающий квалификационным требованиям, предъявляемым к аудиторам в соответствии со схемой аудита.
- Подчиняется закону, государственному регулированию или профессиональному этическому кодексу.
- За исключением случаев внутреннего государственного аудиторского агентства, имеет страхование профессиональной ответственности/ошибок и упущений с лимитом покрытия не менее одного миллиона ($1 000 000) долларов США.

Для eIDAS аудит проводится органом по оценке соответствия, аккредитованным национальным органом по аккредитации государства-члена Европейского союза на основе стандарта EN ISO/IEC 17065 в соответствии с ETSI EN 319 403 и, в частности, с учетом требований, определенных в Регламенте eIDAS (ЕС) № 910/2014.

Для eIDAS Великобритании аудит проводится органом по оценке соответствия, аккредитованным на основе EN ISO/IEC 17065 в соответствии с профилем ETSI EN 319 403 и, в частности, в соответствии с требованиями, определенными в Регламенте eIDAS Великобритании (eIDAS UK) и Положении о сервисах электронной идентификации и доверия для электронных транзакций 2016 года.

8.3 Отношения оценщика с оцениваемой организацией

GlobalSign выбрала аудитора/оценщика, который полностью независим от GlobalSign.

8.4 Темы, которые покрывает оценка

Аудит соответствует требованиям схем аудита, в соответствии с которыми проводится оценка. Эти требования перечислены в разделе 1.0 и могут меняться по мере обновления схем аудита.

8.5 Действия в результате обнаружения недостатков

GlobalSign, включая подчиненные УЦ с перекрестной подписью, у которых нет технических ограничений, следуют одному и тому же процессу. Аудиторы предъявляют существенное несоответствие и создают подходящий план корректирующих действий для устранения недостатка. Планы корректирующих действий, которые непосредственно влияют на политику и процедуры, продиктованные CP и CPS, передаются в орган по политике GlobalSign.

8.6 Сообщение о результатах

Результаты аудита сообщаются директивному органу для анализа и устранения любых недостатков посредством плана корректирующих действий. Результаты также могут быть предоставлены другим организациям, имеющим право на получение копии результатов по закону, постановлению или соглашению.

Копии отчетов об аудите WebTrust для УЦ компании GlobalSign можно найти по адресу https://www.globalsign.com/en/repository/.

8.7 Самостоятельный аудит

GlobalSign следит за соблюдением Политики сертификации, Положения о сертификационной практике и других требований, строго контролируя качество своих услуг, проводя самоаудит не реже раза в квартал на основе не менее 3% выпущенных сертификатов (6% для EV SSL-сертификатов и EV сертификатов подписи кода), которые выбираются случайным образом.

9.0 Прочие деловые и юридические вопросы

9.1 Сборы

9.1.1 Плата за выдачу или продление сертификата

GlobalSign взимает плату за выдачу и продление сертификата. Перевыпуск осуществляется бесплатно. Сборы и любые связанные с ними положения и условия разъясняются заявителям в процессе регистрации через веб-интерфейс, а также в торговых и маркетинговых материалах на всех веб-сайтах GlobalSign для разных регионов.

9.1.2 Плата за доступ к сертификату

GlobalSign может взимать плату за доступ к любой базе данных, в которой хранятся выданные сертификаты.

9.1.3 Плата за доступ к информации об отзыве или статусе сертификата

GlobalSign может взимать дополнительную плату с Абонентов с большим сообществом доверяющих сторон, которые решили не использовать степлинг (склеивание запросов)

OCSP или другие подобные методы для снижения нагрузки на инфраструктуру статуса сертификатов GlobalSign.

9.1.4 Плата за другие услуги

GlobalSign может взимать плату за другие дополнительные услуги, такие как простановка меток времени.

9.1.5 Политика возврата средств

Если клиент заключил договор с GlobalSign, заказал сертификат непосредственно в GlobalSign и не полностью удовлетворен выданным сертификатом, он может запросить возврат средств в течение 7 дней после выдачи сертификата. Возврат будет осуществлен за вычетом всех расходов, понесенных GlobalSign.

9.2 Финансовая ответственность

9.2.1 Страховое покрытие

GlobalSign NV/SA осуществляет страхование общей коммерческой ответственности с лимитом страхового покрытия не менее двух миллионов долларов США ($2 000 000) и страхование ошибок и упущений / профессиональной ответственности с лимитом страхового покрытия не менее пяти миллионов долларов США ($5 000 000). Страховые полисы GlobalSign включают покрытие (1) исков о возмещении ущерба, возникшего в результате действия, ошибки или упущения, непреднамеренного нарушения договора или небрежности при выдаче или обслуживании EV-сертификатов, и (2) исков о возмещении ущерба, возникшего в результате нарушения прав собственности третьих лиц (за исключением нарушения авторских прав, патентов и товарных знаков), вторжения в частную жизнь и рекламного ущерба. Страхование осуществляется через компании с рейтингом не ниже A- по рейтингу страхователя в текущем издании Best's Insurance Guide (или в ассоциации компаний, каждый из членов которой имеет такой рейтинг).

9.2.2 Прочие активы

Не предусмотрено.

9.2.3 Страхование или гарантийное покрытие для конечных субъектов

GlobalSign предлагает Абонентам гарантийную политику, опубликованную на веб-сайте GlobalSign по адресу https://www.globalsign.com/en/company/corporate-policies.

9.3 Конфиденциальность деловой информации

9.3.1 Объем конфиденциальной информации

Следующие элементы классифицируются как конфиденциальная информация и поэтому подлежат осторожному обращению и вниманию со стороны персонала GlobalSign, включая специалистов по проверке и администраторов:

- Персональная информация, которая перечислена в разделе 9.4.
- Журналы аудита из систем УЦ и РЦ.
- Данные активации, используемые для активации закрытых ключей УЦ, как описано в разделе 6.4.
  Внутренняя документация по бизнес-процессам GlobalSign, включая планы аварийного восстановления (DRP) и планы обеспечения непрерывности бизнеса (BCP).
- Отчеты об аудите от независимого аудитора, которые описаны в разделе 8.0.

9.3.2 Информация, не входящая в область конфиденциальной

Любая информация, не определенная как конфиденциальная в рамках данного CPS, считается открытой. Информация о статусе сертификата и сами сертификаты считаются публичными.

9.3.3 Ответственная защита конфиденциальной информации

GlobalSign защищает конфиденциальную информацию, обучая сотрудников, агентов и подрядчиков, а также проверяя соблюдение правил.

9.4 Конфиденциальность персональной информации

9.4.1 План обеспечения конфиденциальности

GlobalSign защищает личную информацию в соответствии с политикой конфиденциальности, опубликованной на сайте GlobalSign по адресу https://www.globalsign.com/repository.

9.4.2 Информация, которая считается конфиденциальной

GlobalSign рассматривает всю личную информацию о Физическом лице, которая не является общедоступной в содержимом Сертификата, как личную информацию. Сюда входит информация, которая связывает псевдоним с реальной личностью Субъекта физического лица и применима как к тем заявителям, которым удалось получить сертификат, так и к тем заявителям, которым это не удалось и было отклонено.

9.4.3 Информация, которая не считается конфиденциальной

Любое содержимое сертификата и информация о его статусе не считаются конфиденциальными.

9.4.4 Ответственность за защиту конфиденциальной информации

GlobalSign несет ответственность за безопасное хранение частной информации в соответствии с опубликованным документом Политики конфиденциальности и может хранить информацию, полученную как в бумажной, так и в цифровой форме. GlobalSign защищает частную информацию, используя соответствующие меры безопасности и разумную степень осторожности, и требует того же от любых поставщиков услуг, которые обрабатывают личную информацию от имени GlobalSign или РЦ.

9.4.5 Уведомление и согласие на использование конфиденциальной информации

Личная информация, полученная от заявителей в процессе подачи заявления и регистрации, считается конфиденциальной. Для ее использования требуется разрешение заявителя. GlobalSign включает все требуемые согласия в Абонентский договор, включая разрешение на получение дополнительной информации от третьих лиц, которая может быть понадобиться в процессе проверки для продуктов или услуг GlobalSign. GlobalSign требует того же от любых поставщиков услуг, которые обрабатывают личную информацию от имени GlobalSign или RA.

9.4.6 Раскрытие информации в соответствии с судебным или административным процессом

GlobalSign может раскрывать личную информацию, если этого требует закон или нормативный акт, без уведомления заявителей или абонентов.

9.4.7 Другие обстоятельства раскрытия информации

Не предусмотрено.

9.5 Права интеллектуальной собственности

GlobalSign сознательно не нарушает права интеллектуальной собственности третьих лиц. Открытые и закрытые ключи остаются собственностью Абонентов, которые владеют ими на законных основаниях. GlobalSign сохраняет право собственности на сертификаты, однако предоставляет разрешение на воспроизведение и распространение сертификатов на неэксклюзивной, безвозмездной основе, при условии, что они воспроизводятся и распространяются в полном объеме.

GlobalSign и логотип GlobalSign являются зарегистрированными торговыми марками GMO GlobalSign K.K.

9.6 Заявления и гарантии

9.6.1 Заявления и гарантии УЦ

GlobalSign использует настоящий CPS и применимые Абонентские соглашения для передачи Абонентам и проверяющим сторонам юридических условий использования выданных сертификатов.

Выдавая сертификат, GlobalSign предоставляет перечисленные здесь гарантии следующим бенефициарам сертификата:
1. Абонент, являющийся стороной Абонентского соглашения или Условий использования Сертификата;
2. Все поставщики прикладного программного обеспечения, с которыми корневой центр сертификации заключил договор о включении своего сертификата корневого центра сертификации в программное обеспечение, распространяемое таким поставщиком прикладного программного обеспечения; и
3. Все Доверяющие стороны, которые обоснованно полагаются на Действительный сертификат.

GlobalSign заявляет и гарантирует бенефициарам сертификата, что в течение периода действия сертификата выдающий центр сертификации соблюдал свою политику сертификации и/или заявление о практике сертификации при выдаче сертификата и управлении им:

9.6.1.1 Основные заявления и гарантии РЦ

Для сертификатов SSL, EV SSL, SMIME, подписи кода и подписи кода EV компания GlobalSign заявляет и гарантирует бенефициарам сертификатов, что в течение периода действия сертификата GlobalSign соблюдает свою политику сертификации и/или заявление о практике сертификации при выдаче и управлении. Сертификат и:

- Право на использование доменного имени или IP-адреса: для SSL-сертификатов, которые на момент выдачи GlobalSign (i) внедрили процедуру проверки того, что заявитель либо имел право использовать доменное имя, либо контролировал его(s) и IP-адрес(а), указанные в поле «Субъект» сертификата и расширении subjectAltName (или, только в случае с доменными именами, такое право или контроль были делегированы кем-то, кто имел такое право на использование или контроль); (ii) соблюдал процедуру при выдаче Сертификата; и (iii) точно описал процедуру в Политике сертификации GlobalSign и/или Положении о практике сертификации (см. Раздел 3.2).
- Право на использование адреса почтового ящика: для сертификатов SMIME, которые на момент выдачи GlobalSign (i) реализовали процедуру проверки того, что заявитель либо имел право использовать, либо контролировал адреса почтовых ящиков, перечисленные в сертификате. поле субъекта и расширение subjectAltName (или было делегировано такое право или контроль кем-то, кто имел такое право на использование или контроль); (ii) соблюдал процедуру при выдаче Сертификата; и iii. точно описал процедуру в CP и/или CPS GlobalSign (см. раздел 3.2).
- Разрешение на выдачу Сертификата: на момент выдачи GlobalSign (i) провела процедуру проверки того, что Субъект разрешил выдачу Сертификата и что Представитель заявителя уполномочен запрашивать Сертификат от имени Субъекта; (ii) соблюдал процедуру при выдаче Сертификата; и (iii) точно описал процедуру в Политике сертификации GlobalSign и/или Положении о практике сертификации (см. раздел 3.2.5);
- Точность информации: на момент выдачи GlobalSign (i) применяла процедуру проверки всей информации, содержащейся в сертификате (за исключением атрибута subject:organizationalUnitName и subject:serialNumber (сертификаты, не относящиеся к EV).) было правдивым и точным; (ii) соблюдал процедуру при выдаче Сертификата; и (iii) точно описал процедуру в Политике сертификации GlobalSign и/или Положении о практике сертификации (см. разделы 3.2.2, 3.2.3, 3.2.4);
- Личность заявителя: если сертификат содержит идентификационную информацию субъекта, GlobalSign (i) провела процедуру проверки личности заявителя в соответствии с разделом 3.2 и разделом 7 применимых требований форума CA/браузера; (ii) соблюдал процедуру при выдаче и управлении Сертификатом; и (iii) точно описал процедуру в Политике сертификации GlobalSign и/или Положении о практике сертификации (см. разделы 3.2.3, 3.2.3, 3.2.4);

- Соглашение с Абонентом: если GlobalSign и Абонент не являются аффилированными лицами, то Абонент и центр сертификации являются сторонами юридически действительного и имеющего юридическую силу соглашения с Абонентом, которое удовлетворяет применимым требованиям форума CA/браузера, или, если GlobalSign и Абонент являются аффилированными лицами, представитель заявителя подтвердил и принял Условия использования (см. Раздел 4.1);
- Статус: GlobalSign поддерживает круглосуточный общедоступный репозиторий с текущей информацией о статусе сертификатов как действительных или отозванных в течение периода, требуемого применимыми требованиями форума CA/браузера; и
- Отзыв: GlobalSign отзовет Сертификат по любой из причин, указанных в применимых требованиях форума CA/браузера (см. раздел 4.9.1).

9.6.1.2 Заявления и гарантии для сертификатов подписи кода

Для сертификатов подписи кода, в дополнение к заявлениям и гарантиям, указанным в разделе **9.6.1.1, GlobalSign представляет и гарантирует бенефициарам сертификата в течение периода действия сертификата:**

- Соответствие: GlobalSign и любая служба подписи соблюдают базовые требования к подписи кода, а также применимую политику сертификации и заявление о практике сертификации при выдаче каждого сертификата подписи кода и эксплуатации своей PKI или службы подписи;
- Юридическое существование: в отношении сертификатов подписи кода EV компания GlobalSign подтвердила учреждающему или регистрационному агентству в юрисдикции субъекта регистрации или регистрации, что на дату выдачи сертификата подписи кода EV Субъект сертификата подписи кода EV является юридически существует как действительная организация или юридическое лицо в юрисдикции регистрации или регистрации;
- Идентичность Абонента: на момент выпуска GlobalSign или Служба подписи заявляет, что (i) использовала процедуру проверки личности Абонента, которая, по крайней мере, соответствует требованиям раздела 3.2 настоящего документа, (ii) следовала процедуре при выдаче Сертификата или управлении им, и (iii) точно описал ту же процедуру в Политике сертификации GlobalSign или Заявлении о практике сертификации;
- Защита ключей: компания GlobalSign заявляет, что на момент выдачи она предоставила Абоненту документацию о том, как безопасно хранить и предотвращать неправомерное использование закрытых ключей, связанных с сертификатами подписи кода, или, в случае службы подписи, надежно хранить и предотвращать несанкционированное использование закрытых ключей. неправомерное использование закрытых ключей, связанных с сертификатами подписи кода; и
- Абонентское соглашение: GlobalSign и Signing Service подтверждают, что GlobalSign или Signing Service заключили юридически действительное и имеющее исковую силу Абонентское соглашение с Заявителем, которое удовлетворяет настоящим Требованиям, или, если они являются аффилированными лицами, Представитель заявителя подтвердил и принял Условия использования.

9.6.1.3 Заявления и гарантии для сертификатов EV SSL и подписи кода EV

Для сертификатов EV SSL и подписи кода EV, в дополнение к заявлениям и гарантиям, указанным в разделе 9.6.1.1, GlobalSign представляет и гарантирует Бенефициарам сертификата в течение периода действия сертификата:

- Юридическое существование: компания GlobalSign подтвердила учреждающему или регистрационному агентству в юрисдикции регистрации или регистрации Субъекта, что на дату выдачи Сертификата Субъект, указанный в Сертификате, юридически существует как действующая организация или юридическое лицо в юрисдикции Субъекта. Учреждение или регистрация;
- Идентичность: компания GlobalSign подтвердила, что на дату выдачи Сертификата юридическое имя Субъекта, указанного в Сертификате, совпадает с именем в официальных государственных записях Агентства по регистрации или регистрации в юрисдикции регистрации или регистрации Субъекта, и если вымышленное имя также включено, то вымышленное имя должным образом зарегистрировано Субъектом в юрисдикции его места ведения бизнеса;
- Право на использование доменного имени: для сертификатов EV SSL компания GlobalSign предприняла все разумно необходимые шаги для проверки того, что на дату выдачи сертификата Субъект, указанный в сертификате, имеет право использовать все доменные имена. указан в Сертификате;
- Разрешение на получение сертификата EV: компания GlobalSign предприняла все разумно необходимые шаги для проверки того, что Субъект, указанный в сертификате, разрешил выдачу сертификата; и
- Абонентское соглашение: Субъект, указанный в Сертификате, заключил юридически действительное и имеющее юридическую силу Абонентское соглашение с GlobalSign, которое удовлетворяет требованиям настоящего Руководства, или, если они являются аффилированными лицами, Представитель заявителя подтвердил и принял Условия использования.

9.6.1.4 Абоненты из Североамериканского совета по энергетическим стандартам (NAESB)

- Для сертификатов NAESB, в дополнение к заявлениям и гарантиям, указанным в разделе 9.6.1.1, GlobalSign представляет и гарантирует бенефициарам сертификата в течение периода действия сертификата:
- GlobalSign выдала и будет управлять сертификатом в соответствии со стандартом NAESB WEQ PKI;
- GlobalSign выполнила все требования стандартов NAESB WEQ PKI при идентификации Абонента и выдаче Сертификата;
- В Сертификате не содержится искажений фактов, которые фактически известны или могут быть обоснованно известны GlobalSign, и GlobalSign проверила информацию в Сертификате;
- Информация, предоставленная Заявителем для включения в Сертификат, была точно записана в Сертификат; и
- Сертификат соответствует требованиям к материалам стандартов NAESB WEQ PKI.

9.6.2 Заявления и гарантии РЦ

РА гарантирует, что:

• Процессы выпуска соответствуют настоящей CPS и соответствующему CP.

• Вся информация, предоставленная GlobalSign, не содержит вводящей в заблуждение или ложной информации; и

• Все переведенные материалы, предоставленные РА, являются точными.

9.6.3 Заверения и гарантии Абонента

В рамках Абонентского соглашения или Условий использования GlobalSign требует, чтобы Заявитель взял на себя обязательства и гарантии, изложенные в этом разделе, в интересах GlobalSign и Бенефициаров сертификата.
До выдачи Сертификата GlobalSign получает, в явной выгоде GlobalSign и Бенефициаров сертификата, либо Заявителя:
1. Согласие с Абонентским соглашением с GlobalSign; или
2. Признание Условий использования.
GlobalSign реализует процесс, гарантирующий, что каждое Соглашение Абонента или Условия использования имеет юридическую силу в отношении Заявителя. В любом случае Соглашение применяется к Сертификату, который выдается в соответствии с запросом на Сертификат.

Для каждого запроса сертификата может использоваться отдельное соглашение, или одно соглашение может использоваться для покрытия нескольких будущих запросов на сертификаты и полученных сертификатов, при условии, что каждый сертификат, который GlobalSign выдает заявителю, четко подпадает под действие этого Абонентского соглашения или Условий Использовать.

Абонентское соглашение или Условия использования содержат положения, налагающие на самого Заявителя (или сделанные Заявителем от имени своего принципала или агента в рамках отношений субподрядчика или услуги хостинга) следующие обязательства и гарантии:

Абоненты и/или заявители гарантируют, что:

- Точность информации: Абонент всегда будет предоставлять точную и полную информацию компании GlobalSign, как в запросе на сертификат, так и по иным запросам GlobalSign в связи с выдачей сертификата;
- Защита закрытого ключа: Заявитель должен принять все разумные меры для обеспечения единоличного контроля, сохранения конфиденциальности и постоянной надлежащей защиты закрытого ключа, который будет включен в запрошенный сертификат(ы), и любых связанных с ним данных или устройств активации, например, пароль или токен; В отношении сертификатов подписи кода Абонент должен единолично контролировать, сохранять конфиденциальность и должным образом защищать в любое время в соответствии с разделом 6.2.7.4 «Базовых требований к подписи кода» закрытый ключ, соответствующий открытому ключу, который должен быть включен в сертификаты подписи кода. запрошенный сертификат(ы) (и любые связанные с ним данные активации или устройство, например пароль или токен). Абонент гарантирует, что он будет генерировать и эксплуатировать любое устройство, хранящее закрытые ключи, безопасным способом. Абонент должен использовать пароли, генерируемые случайным образом и состоящие как минимум из 16 символов, содержащих прописные и строчные буквы, цифры и символы, для передачи закрытых ключей.
- Повторное использование закрытого ключа: для сертификатов подписи кода Абонент не должен подавать заявку на получение сертификата подписи кода, если открытый ключ в сертификате используется или будет использоваться с сертификатом, не относящимся к подписи кода;
- Принятие сертификата: Абонент не должен использовать сертификат до тех пор, пока заявитель или агент заявителя не просмотрит и не проверит точность содержания сертификата.

• Использование сертификата. Для сертификатов TLS Абонент должен установить Сертификат только на серверах, доступных по альтернативному имени субъекта, указанному в Сертификате, и использовать Сертификат исключительно в соответствии со всеми применимыми законами и исключительно в соответствии с Соглашением Абонента. или Условия использования. В отношении сертификатов S/MIME Абонент должен использовать Сертификат только на адресах почтовых ящиков, перечисленных в Сертификате, и использовать Сертификат исключительно в соответствии со всеми применимыми законами и исключительно в соответствии с Соглашением Абонента или Условиями использования. Для сертификатов подписи кода Абонент должен использовать сертификат и связанный с ним закрытый ключ только в авторизованных и законных целях, в том числе не использовать сертификат для подписи подозрительного кода и использовать сертификат и закрытый ключ исключительно в соответствии со всеми применимыми законами и исключительно в соответствии с Абонентское соглашение или Условия использования;

• Предотвращение неправомерного использования: для сертификатов подписи кода Абонент должен обеспечить адекватные сетевые и другие меры безопасности для защиты от неправильного использования закрытого ключа, а также то, что GlobalSign отзовет сертификат без предварительного уведомления в случае несанкционированного доступа к закрытым ключам;

• Отчетность и отзыв: Абонент принимает на себя обязательство и гарантирует (a) незамедлительно запросить отзыв сертификата и прекратить использование его и связанного с ним закрытого ключа, если имеет место фактическое или предполагаемое неправильное использование или компрометация закрытого ключа Абонента, связанного с Открытый ключ, включенный в сертификат; и (b) незамедлительно запросить отзыв Сертификата и прекратить его использование, если какая-либо информация в Сертификате является или становится неверной или неточной; или (c) имеются доказательства того, что Сертификат использовался для подписи Подозрительного кода;

• Обмен информацией: для сертификатов подписи кода Абонент признает и принимает, что, если: (a) сертификат или заявитель идентифицируются как источник подозрительного кода, (b) полномочия, запрашивающие сертификат, не могут быть проверены, или (c) Сертификат отозван по причинам, отличным от запроса Абонента (например, в результате компрометации закрытого ключа, обнаружения вредоносного ПО и т. д.), тогда GlobalSign имеет право поделиться информацией о Заявителе, подписанном приложении, Сертификате и окружающих обстоятельства взаимоотношений с другими центрами сертификации или отраслевыми группами, включая Форум центров сертификации/браузеров;

• Прекращение использования сертификата: Абонент должен незамедлительно прекратить использование закрытого ключа, связанного с открытым ключом в сертификате, после отзыва этого сертификата; и

• Оперативность: Абонент должен ответить на инструкции GlobalSign относительно компрометации или неправильного использования сертификата в течение сорока восьми (48) часов; и

• Подтверждение и принятие: Заявитель признает и принимает, что GlobalSign имеет право немедленно отозвать Сертификат, если Заявитель нарушает условия Абонентского соглашения или Условия использования или если отзыв требуется CP и/или CPS GlobalSign или соответствующим центром сертификации. /Требования форума к браузеру.

9.6.3.1 Доверяющие стороны Североамериканского совета по энергетическим стандартам (NAESB)

Конечные организации, участвующие в Стандарте деловой практики WEQ-012 v3.0 и использующие сертификаты для приложений WEQ-012, должны быть зарегистрированы в NAESB EIR и предоставить подтверждение того, что они являются организацией, уполномоченной заниматься оптовой торговлей электроэнергией. Субъекты или организации, которым может потребоваться доступ к приложениям с использованием аутентификации, указанной в стандартах NAESB WEQ PKI, но не квалифицируемые как участники оптового рынка электроэнергии (например, регулирующие органы, университеты, консалтинговые фирмы и т. д.), должны зарегистрироваться.

Зарегистрированные конечные организации и сообщество пользователей, которое они представляют, должны соблюдать все обязательства конечных организаций, предусмотренные стандартами NAESB WEQ PKI.

Каждая организация-Абонент подтверждает свое понимание следующих обязательств стандартов NAESB WEQ PKI через GlobalSign следующим образом:

Каждая конечная организация должна удостоверить свою сертифицирующую организацию, что она рассмотрела и подтверждает следующие стандарты NAESB WEQ PKI.

A. Конечная организация признает потребность электроэнергетической отрасли в безопасных частных электронных коммуникациях, которые способствуют достижению следующих целей:

Конфиденциальность: гарантия для объекта того, что никто не сможет прочитать конкретный фрагмент данных, кроме явно предназначенного получателя(ов).
Аутентификация: гарантия одному объекту того, что другой объект является тем, кем он/она/оно себя выдает.
Целостность: гарантия субъекту того, что данные не были изменены (намеренно или непреднамеренно) между «там» и «здесь» или между «тогда» и «сейчас»; и
Неотказ от ответственности/обязательство по содержанию: сторона не может отрицать свое участие в транзакции или отправку электронного сообщения.

Конечная организация подтверждает одобрение отрасли криптографии с открытым ключом, которая использует сертификаты для привязки открытого ключа человека или компьютерной системы к своей организации и для поддержки обмена ключами симметричного шифрования.

B. Конечная организация провела оценку каждого Заявления о практике сертификации выбранного ею Сертификационного центра в свете тех отраслевых стандартов, которые определены Сертифицирующим органом.

Когда это применимо, конечные организации обязаны зарегистрировать свою юридическую идентификационную информацию о бизнесе и получить «Код организации», который будет опубликован в NAESB EIR и использоваться во всех приложениях Абонентов, подаваемых этой конечной организацией, и в Сертификатах, выданных ей.

Конечные организации также должны соблюдать следующие требования:

Защитите свои закрытые ключи от доступа других сторон.
Если применимо, укажите через NAESB EIR конкретную организацию, которую они выбрали GlobalSign для использования в качестве своего уполномоченного центра сертификации.
Заключить все соглашения и контракты с GlobalSign, как того требует Положение о практике сертификации GlobalSign, необходимое для того, чтобы GlobalSign выдавала сертификаты конечной организации для использования в целях защиты электронных коммуникаций.
Соблюдать все обязательства, требуемые и предусмотренные GlobalSign в настоящем CPS, например, процедуры подачи заявки на сертификат, подтверждение/проверку личности заявителя и методы управления сертификатами.
Подтвердить, что у компании есть программа управления сертификатами PKI, что все задействованные сотрудники обучены этой программе и установлены средства контроля для обеспечения соблюдения этой программы. Эта программа должна включать, помимо прочего:
Политика безопасности и обработки закрытого ключа сертификата.
Политика(и) отзыва сертификатов
Определите тип Абонента (т. е. физическое лицо, роль, устройство или приложение) и предоставьте полную и точную информацию для каждого запроса на сертификат.

9.6.4 Заявления и гарантии проверяющей стороны

Прежде чем полагаться на Сертификат, проверяющие стороны должны принять Соглашение с проверяющей стороной и действовать в соответствии с Соглашением с проверяющей стороной и настоящим CPS.

Сторона, полагающаяся на Сертификат, гарантирует:

• Иметь техническую возможность использовать Сертификаты.
• Получать уведомление о выдающем УЦ и связанных с ним условиях для проверяющих сторон.
• Проверить сертификат выдающего центра сертификации, используя информацию о состоянии сертификата (например, CRL или OCSP), опубликованную выдающим центром сертификации, в соответствии с надлежащей процедурой проверки пути сертификата.
• Доверяйте сертификату выдающего центра сертификации только в том случае, если вся информация, содержащаяся в таком сертификате, может быть проверена с помощью такой процедуры проверки на предмет правильности и актуальности.
• Полагайтесь на сертификат выдающего центра сертификации только в тех случаях, когда это может быть разумно в данных обстоятельствах; и
• Немедленно уведомите соответствующий уполномоченный орган, если проверяющая сторона узнает или подозревает, что закрытый ключ был скомпрометирован.

Обязанности Проверяющей стороны, если она должна обоснованно полагаться на Сертификат, заключаются в следующем:

• Проверьте действительность или отзыв сертификата УЦ, используя текущую информацию о статусе отзыва, указанную проверяющей стороне.
• Принимать во внимание любые ограничения на использование Сертификата, указанные Проверяющей стороне либо в Сертификате, либо в настоящем CPS; и
• Примите любые другие меры предосторожности, предписанные сертификатом выдающего центра сертификации, а также любые другие политики или условия, доступные в контексте приложения, в котором может использоваться сертификат.

Доверяющие стороны должны всегда доказывать, что разумно полагаться на Сертификат в данных обстоятельствах, принимая во внимание такие обстоятельства, как конкретный контекст приложения, в котором используется сертификат.

9.6.4.1 Доверяющие стороны Североамериканского совета по энергетическим стандартам (NAESB)

Обязательства проверяющей стороны должны быть указаны в контексте каждого требования NAESB, в котором используются настоящие стандарты NAESB WEQ PKI, в дополнение к следующему:

• Сертификат выдан GlobalSign, зарегистрированным уполномоченным центром сертификации.
• вся цепочка проверки сертификатов/доверительности к GlobalSign для NAESB, выдающей корневой сертификат уполномоченного центра сертификации, не повреждена и действительна.
• Сертификат действителен и не отозван; и
• Сертификат выдан под одним из идентификаторов объекта уровня безопасности NAESB.

9.6.4.2 Полагающие стороны для квалифицированных сертификатов

Для квалифицированных сертификатов в соответствии с Директивой о платежных услугах (ЕС) 2015/2366 или Open Banking полагающая сторона должна учитывать законодательство, применимое к полагающей стороне и Субъекту сертификата. Полагающая сторона должна учитывать как минимум следующую информацию, включенную в Сертификат:

• Компетентный орган
• Поставщик платежных услуг или финансовое учреждение

Для квалифицированных сертификатов, которые включают OID LRA 1.3.6.1.4.1.4146.1.45.1, необходимо учитывать принадлежность физического лица к организации, указанной в сертификате.

9.6.5 Заявления и гарантии других участников

Не предусмотрено.

9.7 Отказ от гарантий

ЗА ИСКЛЮЧЕНИЕМ СЛУЧАЕВ, ЗАПРЕЩЕННЫХ ЗАКОНОМ ИЛИ ИНЫМ ОБРАЗОМ ПРЕДУСМОТРЕННЫХ В НАСТОЯЩЕМ ДОКУМЕНТЕ, GLOBALSIGN ОТКАЗЫВАЕТСЯ ОТ ВСЕХ ГАРАНТИЙ, ВКЛЮЧАЯ ЛЮБЫЕ ГАРАНТИИ ТОВАРНОГО СОСТОЯНИЯ И/ИЛИ ПРИГОДНОСТИ ДЛЯ КОНКРЕТНОЙ ЦЕЛИ.

9.8 Ограничения ответственности

В ТОЙ МЕРЕ, В КАКОЙ GLOBALSIGN ВЫДАЛА И УПРАВЛЯЛА СЕРТИФИКАТОМ В СООТВЕТСТВИИ С ТРЕБОВАНИЯМИ CA/BROWSER FORUM И НАСТОЯЩИМ CPS, ОНА НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ ПЕРЕД АБОНЕНТОМ, ДОВЕРЯЮЩЕЙ СТОРОНОЙ ИЛИ ЛЮБЫМИ ТРЕТЬИМИ ЛИЦАМИ ЗА ЛЮБЫЕ УБЫТКИ, ПОНЕСЕННЫЕ В РЕЗУЛЬТАТЕ ИСПОЛЬЗОВАНИЯ ИЛИ ДОВЕРИЯ К ТАКОМУ СЕРТИФИКАТУ. В ПРОТИВНОМ СЛУЧАЕ ОТВЕТСТВЕННОСТЬ GLOBALSIGN ПЕРЕД АБОНЕНТОМ, ДОВЕРЯЮЩЕЙ СТОРОНОЙ ИЛИ ЛЮБЫМИ ТРЕТЬИМИ ЛИЦАМИ ЗА ЛЮБЫЕ ТАКИЕ УБЫТКИ НИ ПРИ КАКИХ ОБСТОЯТЕЛЬСТВАХ НЕ ДОЛЖНА ПРЕВЫШАТЬ ОДНУ ТЫСЯЧУ ДОЛЛАРОВ ($1000) ЗА ОДИН СЕРТИФИКАТ И ДВЕ ТЫСЯЧИ ДОЛЛАРОВ ($2000) ЗА СЕРТИФИКАТ EV ИЛИ ПОДПИСИ КОДА EV.

ДАННЫЙ ЛИМИТ ОТВЕТСТВЕННОСТИ ОГРАНИЧИВАЕТ УЩЕРБ, ВОЗМЕЩАЕМЫЙ ВНЕ КОНТЕКСТА ГАРАНТИЙНОЙ ПОЛИТИКИ GLOBALSIGN. ДЛЯ СУММ, ВЫПЛАЧИВАЕМЫХ В РАМКАХ ГАРАНТИЙНОЙ ПОЛИТИКИ, ДЕЙСТВУЮТ СОБСТВЕННЫЕ ОГРАНИЧЕНИЯ ОТВЕТСТВЕННОСТИ.

НИ ПРИ КАКИХ ОБСТОЯТЕЛЬСТВАХ КОМПАНИЯ GLOBALSIGN НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ ЗА ЛЮБЫЕ КОСВЕННЫЕ, СЛУЧАЙНЫЕ, СПЕЦИАЛЬНЫЕ ИЛИ ПОСЛЕДУЮЩИЕ УБЫТКИ, А ТАКЖЕ ЗА УПУЩЕННУЮ ВЫГОДУ, ПОТЕРЮ ДАННЫХ ИЛИ ДРУГИЕ КОСВЕННЫЕ, СЛУЧАЙНЫЕ ИЛИ ПОСЛЕДУЮЩИЕ УБЫТКИ, ВОЗНИКАЮЩИЕ В РЕЗУЛЬТАТЕ ИЛИ В СВЯЗИ С ИСПОЛЬЗОВАНИЕМ, ДОСТАВКОЙ, ДОВЕРИЕМ, ЛИЦЕНЗИЕЙ, ИСПОЛНЕНИЕМ ИЛИ НЕИСПОЛНЕНИЕМ СЕРТИФИКАТОВ, ЦИФРОВЫХ ПОДПИСЕЙ ИЛИ ЛЮБЫХ ДРУГИХ ОПЕРАЦИЙ ИЛИ УСЛУГ, ПРЕДЛАГАЕМЫХ ИЛИ ПРЕДУСМОТРЕННЫХ НАСТОЯЩИМ CPS.

ВЫШЕИЗЛОЖЕННОЕ НЕ ОГРАНИЧИВАЕТ ОТВЕТСТВЕННОСТЬ GLOBALSIGN В ОТНОШЕНИИ КВАЛИФИЦИРОВАННЫХ СЕРТИФИКАТОВ В СООТВЕТСТВИИ СО СТАТЬЕЙ 13 EIDAS ИЛИ ПОЛОЖЕНИЙ UK EIDAS.

9.9 Возмещение убытков

9.9.1 Возмещение убытков компанией GlobalSign

GlobalSign защищает, возмещает и ограждает каждого поставщика программного обеспечения от любых претензий, ущерба или убытков, понесенных им в связи с SSL-сертификатом расширенной проверки или сертификатом подписи кода расширенной проверки, выданным GlobalSign, независимо от причины иска или правовой теории, за исключением случаев, когда претензия, ущерб, или убытки, понесенные поставщиком ПО, были непосредственно вызваны тем, что его программное обеспечение отобразило или (1) действительный и надежный EV-сертификат как недействительный или ненадежный, или (2) (i) истекший сертификат как надежный, или (ii) отозванный сертификат, если статус отзыва доступен в Интернете, но программное обеспечение поставщика прикладного программного обеспечения не проверило или проигнорировало этот статус.

9.9.2 Возмещение убытков Абонентами

В пределах, разрешенных законом, каждый Абонент обязан возместить убытки компании GlobalSign, ее партнерам, а также их соответствующим директорам, должностным лицам, сотрудникам, агентам и подрядчикам от любых потерь, ущерба или расходов, включая разумные гонорары адвокатов, связанных с (i) любым искажением или упущением существенного факта Абонентом, независимо от того, было ли это искажение или упущение преднамеренным или непреднамеренным; (ii) нарушением Абонентом Абонентского

договора, настоящего CPS или действующего законодательства; (iii) компрометацией или несанкционированным использованием сертификата или закрытого ключа из-за небрежности Абонента; (iv) неправильным использованием Абонентом сертификата или закрытого ключа.

9.9.3 Возмещение убытков доверяющими сторонами

В разрешенных законом пределах каждая доверяющая сторона должна возместить GlobalSign, ее партнерам и любым организациям с перекрестной подписью, а также их соответствующим директорам, должностным лицам, сотрудникам, агентам и подрядчикам любые убытки, ущерб или расходы, включая разумные гонорары адвокатов, связанные с (i) нарушением соглашения с доверяющей стороной, настоящего CPS или действующего законодательства; (ii) необоснованным доверием к сертификату; или (iii) неспособностью проверить статус сертификата перед использованием.

9.10 Срок действия и прекращение действия

9.10.1 Срок

Настоящее CPS остается в силе до тех пор, пока GlobalSign не сообщит об обратном на своем веб-сайте или в репозитории.

9.10.2 Прекращение действия

Уведомленные изменения соответствующим образом помечаются указанием версии. Изменения вступают в силу немедленно после публикации.

9.10.3 Последствия прекращения действия

GlobalSign будет сообщать об условиях и последствиях прекращения действия настоящего CPS через соответствующий репозиторий.

9.11 Индивидуальные уведомления и связь с участниками

GlobalSign принимает уведомления, связанные с настоящим CPS, посредством сообщений с цифровой подписью или в бумажной форме. После получения от GlobalSign действительного, подписанного цифровой подписью подтверждения получения, отправитель уведомления считает это сообщение действительным. Отправитель должен получить такое подтверждение в течение двадцати (20) рабочих дней, в противном случае письменное уведомление должно быть отправлено в бумажной форме через курьерскую службу, подтверждающую доставку, или по сертифицированной или заказной почте, с предоплаченной почтой, с запросом о возврате квитанции, на имя отправителя. Индивидуальные сообщения, направляемые в GlobalSign, должны быть адресованы на адрес legal@globalsign.com или по почте GlobalSign по адресу, указанному в разделе 1.5.2.

9.12 Поправки

9.12.1 Процедура внесения поправок

Данное CPS пересматривается не реже одного раза в 365 дней и может пересматриваться чаще. Перед включением все изменения рассматриваются и утверждаются органом GlobalSign CA Governance Policy Authority. Изменения в данном CPS обозначаются соответствующей нумерацией.

9.12.2 Механизм и период уведомления

GlobalSign разместит на своих веб-сайтах соответствующее уведомление о крупных или значительных изменениях в настоящем CPS, а также о периоде, когда пересмотренное CPS будет считаться принятым.

9.12.3 Обстоятельства, при которых должен быть изменен OID

Не предусмотрено.

9.13 Положения о разрешении споров

Прежде чем прибегнуть к любому механизму разрешения споров, включая судебное разбирательство или любой вид альтернативного разрешения споров (включая мини-суд, арбитраж, обязательную консультацию эксперта, мониторинг сотрудничества и обычную

консультацию эксперта), стороны, подавшие жалобу, соглашаются уведомить GlobalSign о споре для поиска разрешения спора.

После получения уведомления о споре GlobalSign созывает комитет по спорам, который консультирует руководство GlobalSign о том, как действовать в данном споре. Комитет по спорам собирается в течение двадцати (20) рабочих дней с момента получения уведомления о споре. В состав комитета входят адвокат, сотрудник по защите данных, член оперативного руководства GlobalSign и сотрудник службы безопасности. Адвокат или сотрудник по защите данных председательствует на заседании. В своих решениях комиссия по спорам предлагает исполнительному руководству GlobalSign урегулировать спор. Исполнительное руководство может впоследствии сообщить о предложенном урегулировании стороне, подавшей жалобу.

Если спор не урегулирован в течение двадцати (20) рабочих дней после первоначального уведомления в соответствии с CPS, стороны передают спор в арбитраж, в соответствии со ст. 1676-1723 Судебного кодекса Бельгии.

В арбитраже будут участвовать три (3) арбитра, из которых каждая сторона предлагает одного, а третьего арбитра выбирают обе стороны спора. Местом проведения арбитража является г. Лёвен, Бельгия, и арбитры определяют все сопутствующие расходы.

9.14 Регулирующее законодательство

Настоящее CPS регулируется, толкуется и интерпретируется в соответствии с законодательством Бельгии. Такой выбор закона сделан для обеспечения единообразного толкования настоящего CPS, независимо от места проживания или места использования сертификатов GlobalSign или других продуктов и услуг. Право Бельгии применяется также ко всем коммерческим или договорным отношениям GlobalSign, в которых может применяться или косвенно или явно цитироваться настоящий CPS в отношении продуктов и услуг GlobalSign, где GlobalSign выступает в качестве поставщика, поставщика, получателя выгоды или иным образом.

Все стороны, включая партнеров GlobalSign, Абонентов и доверяющие стороны, безоговорочно подчиняются юрисдикции окружных судов города Лёвен, Бельгия.

9.15 Соблюдение действующего законодательства

GlobalSign соблюдает действующее законодательство Бельгии. Экспорт некоторых типов программного обеспечения, используемого в определенных продуктах и услугах GlobalSign по управлению публичными сертификатами, может потребовать разрешения соответствующих государственных или частных органов. Стороны (включая GlobalSign, Абонентов и доверяющие стороны) соглашаются соблюдать действующие экспортные законы и правила Бельгии.

9.16 Различные положения

9.16.1 Полное соглашение

GlobalSign по договору обяжет каждый РЦ, участвующий в выдаче сертификатов, соблюдать настоящее CPS и все действующие отраслевые руководства. Никакая третья сторона не может полагаться на такое соглашение или предъявлять иск о его принудительном исполнении.

9.16.2 Назначение

Организации, осуществляющие деятельность в рамках данного CPS, не могут переуступать свои права или обязательства без предварительного письменного согласия GlobalSign.

9.16.3 Делимость

Если какое-то положение настоящего CPS, включая положения об ограничении ответственности, признано недействительным или не имеющим исковой силы, остальные положения настоящего CPS будут истолкованы в соответствии с первоначальными намерениями сторон.

Каждое положение настоящего CPS, предусматривающее ограничение ответственности, является самостоятельным и независимым от любого другого положения и должно применяться как таковое.

9.16.4 Обеспечение исполнения (гонорар адвоката и отказ от прав)

GlobalSign может потребовать от стороны возмещения убытков, потерь и расходов, связанных с поведением этой стороны, и оплаты услуг адвокатов. Отказ GlobalSign обеспечить соблюдение какого-либо положения настоящего CPS не лишает GlobalSign права обеспечить соблюдение тех же положений в дальнейшем или права обеспечить соблюдение любых других положений настоящего CPS. Чтобы любой отказ имел силу, он должен быть оформлен в письменном виде и подписан GlobalSign.

9.16.5 Форс-мажор

GlobalSign не несет ответственности за любые потери, затраты, расходы, обязательства, ущерб или претензии, возникающие в результате или связанные с задержками в выполнении или невыполнением своих обязательств, если такие задержки или невыполнение вызваны обстоятельствами, находящимися вне разумного контроля GlobalSign, включая, без ограничений, действия любых правительственных органов, войну, восстание, саботаж, эмбарго, пожар, наводнение, забастовку или другие, прерывание или задержку транспортировки, недоступность, прерывание или задержку телекоммуникаций или услуг третьих лиц.

9.17 Другие положения

Нет.

10.0 Приложение A

10.1. Сертификаты S/MIME BR

10.1.1 Требования к РЦ предприятия

Для сертификатов S/MIME BR, если компания проверяет запросы на сертификаты для субъектов внутри своей организации, компания действует как РЦ предприятия, и применяются следующие требования:

Согласие
Предприятие РЦ должен соблюдать положения GlobalSign CP, CPS и базовые требования для S/MIME, применимые к Предприятию РЦ.

Информационная безопасность
Предприятие РЦ должно применять лучшие практики информационной безопасности, используя надежные системы и продукты, защищенные от изменений и обеспечивающие техническую безопасность и надежность поддерживаемых ими процессов.

Квалификация
Прежде чем привлекать какое-либо лицо к процессу управления сертификатами, будь то в качестве сотрудника, агента или независимого подрядчика, Предприятие РЦ должен проверить личность и надежность такого лица.

Мониторинг
GlobalSign имеет право осуществлять мониторинг не реже одного раза в год за соблюдением Предприятие РЦ обязательств по настоящему Соглашению и CPS.

Удержание
Предприятие РЦ должно сохранять в течение не менее двух (2) лет:
Вся архивная документация, относящаяся к проверке, выдаче и отзыву запросов на сертификаты и сертификатов после последующего возникновения:
1. такие записи и документация в последний раз использовались при проверке, выдаче или отзыве запросов на сертификаты и сертификаты; или

2. истечение срока действия Сертификатов Абонента, основанных на таких записях и документации.

10.1.1.1 Спонсор утвержден
Для Сертификатов, включающих атрибуты Индивидуального (Физического лица) совместно с Организацией:

Индивидуальная информация
Предприятие РЦ должен предоставить значение subject:commonName в запросе сертификата, которое должно быть либо личным именем, либо псевдонимом субъекта.

1. Личное имя должно представлять собой значимое представление имени Субъекта, подтвержденное идентификационной документацией или записями Предприятия РЦ. Допускаются имена, состоящие из нескольких слов. Имена, соединенные через дефис, считаются одним именем. Субъекты, имеющие более одного имени, могут выбрать одно или несколько своих имен в любой последовательности. Субъекты могут выбирать порядок расположения своих имен и фамилий в соответствии с национальными предпочтениями.

2. Псевдоним должен представлять собой идентификатор, выбранный РЦ предприятия, который однозначно идентифицирует субъект сертификата внутри организации, включенный в атрибут subject:organizationName.

Сбор и хранение
Enterprise РЦ должен собирать, проверять и хранить доказательства следующих атрибутов личности Физического лица:
1. Имя(а) и фамилия(я), которые должны быть настоящими именами;
2. Псевдоним (если используется);
3. Должность (если используется); и
4. Дополнительная информация, необходимая для однозначной идентификации заявителя.

Атрибуты должны собираться, проверяться и подтверждаться на основе записей (например, Active Directory), поддерживаемых Предприятием РЦ.

Предприятие РЦ может повторно использовать имеющиеся доказательства для подтверждения личности, если доказательства были получены не более чем за 825 дней до выдачи Сертификата.