Регламент удостоверяющего центра

Политика сертификации УЦ «Сименс»

История изменений документа

Версия	Дата	Составитель	Комментарий к изменению
1.0	20 июня 2016 г.	Майкл Мерфи Александр Виннен	Первая выпущенная версия
1.1	1 декабря 2016 г.	Руфус Бушарт	Незначительно обновленная версия
1.2	29 мая 2017 г.	Руфус Бушарт	Обновление новой структуры иерархии ИОК «Сименс»
1.3	31 июля 2017 г.	Бьёрн Хундертмарк	Обновление главы по авторизации центра сертификации (CAA)
1.4	14 сентября 2017 г.	Руфус Бушарт	Уточнение заявления CAA
1.4	1 декабря 2017 года	Флориан Гроц	Пересмотр Авторизации центра сертификации (CAA)
1.5	12 января 2018 года	Руфус Бушарт	Глава «История изменений документа» дополнена с внесением новых пунктов Глава 1.3.2 Отсутствие прав у третьих лиц Глава 2.1 Добавлен URL для CRL и OCSP Глава 2.2 Удален URL для CRL и OCSP Глава 4.9.1 Удалены причины отзыва Глава 4.9.5 Добавлен отчет о проблеме с сертификатом Глава 5 Перемещено из корневого УЦ ЗПС
1.6	31 января 2018 года	Руфус Бушарт	Глава 4.9.1 Упомянут партнер по перекрестной сертификации Глава 4.9.9 Подробно описана спецификация OCSP Глава 5.4.1 Добавлена информация об объеме данных журнала Глава 5.4.8 Даны пояснения по периодичности Глава 8.2 Аудитор должен быть квалифицированным
1.7	6 февраля 2018 года	Руфус Бушарт	Глава 9.10.2 Добавлена доверяющая сторона Глава 6 Технические средства контроля проверены на соответствие ETSI EN 319 411-1 / 319 401 Глава 7.1 Добавлена ссылка на ETSI EN 319 412-2 Глава 4.7 Повторное использование ранее согласованной информации запрещено Изменение лицензии на CC BY-SA4.0, согласно требованиям Mozilla Глава 1.2 Добавлен OID 1.3.6.1.4.1.4329.7

Настоящий документ пересматривается каждый год или в случае внесения важных специальных изменений в соответствии с процессом обновления документов Отдела информационной безопасности. Изменения базовых требований к CA/B будет отражено после внесения соответствующих пунктов в настоящий документ. Каждая новая версия перед выпуском утверждается на соответствующем уровне управления.

Настоящий документ опубликован на веб-сайте www.siemens.com/pki.

Область применения

Настоящий документ представляет собой комплексную Политику сертификации (ПС) Удостоверяющего центра «Сименс». Удостоверяющий центр «Сименс» отвечает за работу Корневого УЦ «Сименс», а также за Выпускающие УЦ «Сименс». Целью настоящего документа является публичное раскрытие субъектам и доверяющим сторонам политик и методов ведения деятельности, в соответствии с которыми работают УЦ «Сименс».

Высшее руководство УЦ обеспечивает надлежащую реализацию установленных в настоящем документе методов сертификации, соответствующих действующим требованиям, в соответствии с Политиками информационной безопасности «Сименс».

Статус документа

Настоящий документ с версией 1.7 и статусом «Выпущен» был классифицирован как «Без ограничений» и

Статус документа

	Ф.И.О.	Отдел	Дата
Автор	Различные авторы, подробная информация в истории изменений документа		
Проверил:	Тобиас Ланге Флориан Гроц	Siemens LC Siemens GS IT HR 7 4	20 июня 2016 г. 23 февраля 2018 г.
Утвердил:	Маркус Вихманн, представляющий Руководителя Siemens ISEC Удо Виртца	Siemens GS IT ISEC	23 февраля 2018 г.

Настоящая ПС была утверждена Маркусом Вихманном, представляющим Руководителя ИБ «Сименс», 23 февраля 2018 года.

Содержание

1 Введение

Структура настоящего документа соответствует рекомендациям RFC 3647 «Интернет X.509 Инфраструктура открытого ключа: Политика сертификации и основы практики сертификации» [RFC3647].

1.1 Обзор

В настоящем документе описывается политика сертификации УЦ «Сименс». В нем описываются услуги, предоставляемые УЦ «Сименс», а также обязательные требования, которые должны выполняться поставщиками услуг и другими участниками ИОК. Кроме того, настоящий документ (совместно с ЗПС) также определяет процесс сертификации и принципы сотрудничества, обязанности и права участников ИОК.

В дополнение к требованиям, определенным в настоящей ПС и соответствующих ЗПС, ИТ-системы «Сименс» работают в соответствии с внутренними правилами ИБ «Сименс» и соответствующими руководствами по выполнению, которые определяют, как надежно использовать ИТ-системы. Эти правила ИБ являются частью СМИБ, которая определяется и внедряется в соответствии с ISO 27001.

Для делегированных задач УЦ «Сименс» и любые делегированные поставщики услуг могут распределять между собой обязательства по договору по своему усмотрению, но УЦ продолжает нести полную ответственность за выполнение всеми сторонами этих требований, как если бы эти задачи не были делегированы.

1.1.1 Иерархия ИОК

Структура иерархии ИОК «Сименс» показана на Рисунке 1.

В настоящее время существуют два отдельных активных корневых УЦ:

- Корневой УЦ «Сименс», предназначенный для внутреннего использования в компании «Сименс», а также
- Корневой УЦ QuoVadis (партнер по перекрестной сертификации для внешнего доверенного использования) для использования, когда требуется внешнее признание сертификатов

Корневые УЦ выдают сертификаты УЦ исключительно Выпускающим УЦ.

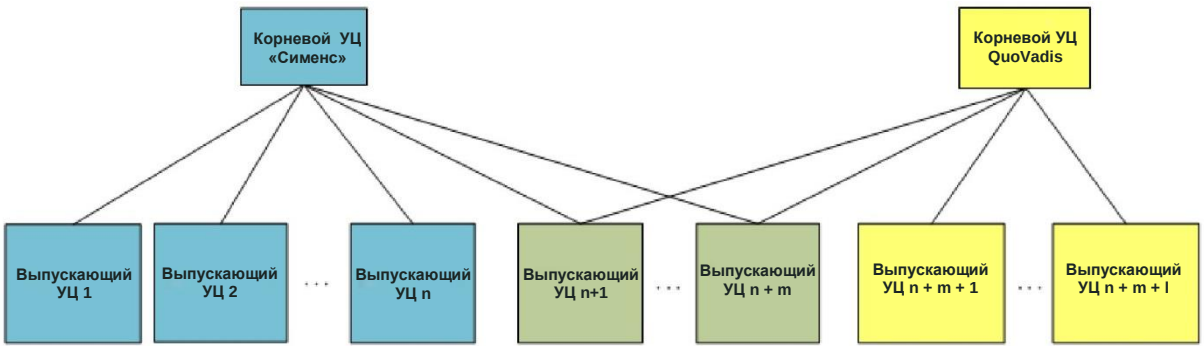

Рис. 1: Иерархия ИОК «Сименс»

Все сертификаты, выданные вышеупомянутыми УЦ, должны по крайней мере соответствовать требованиям ETSI NCP [ETSI TS 102 042]. При необходимости, дополнительные спецификации (за пределами NCP) определяются в соответствующих ЗПС.

1.1.2 Корневой УЦ «Сименс» и Корневой УЦ QuoVadis

Корневой УЦ «Сименс» и Корневой УЦ QuoVadis выдают, управляют и отзывают сертификаты X.509v3, используемые соответствующими Выпускающими УЦ. Это включает:

- ❑ Создание пар ключей Корневого УЦ
- ❑ Создание самоподписанных сертификатов для Корневых УЦ
- ❑ Создание сертификатов для Выпускающих УЦ
- ❑ Повторная сертификация для существующих ключей УЦ
- ❑ Отзыв сертификатов Выпускающего УЦ
- ❑ Ведение Списка отозванных сертификатов УЦ («CA-CRL»)

1.1.3 Выпускающие УЦ

Выпускающий УЦ вместе с другими участниками ИОК «Сименс» (например, центрами регистрации) выдают, управляют или отзывают сертификаты открытого ключа X.509v3, используемые для защиты бизнес-процессов «Сименс» как внутренних (например, сотрудников «Сименс»), так и внешних (например, сертификаты для серверов). Предлагаемые сервисы включают:

- ❑ Создание сертификатов для конечных пользователей
- ❑ Отзыв сертификатов конечных пользователей
- ❑ Ведение Списка отозванных сертификатов конечных пользователей («EE-CRL»)

1.2 Название и идентификационное обозначение документа

Настоящая ПС означает «Политику сертификации».

Наименование:	Политика сертификации - Корневые УЦ «Сименс» и Выпускающие УЦ
OID:	1.3.6.1.4.1.4329.99.1.1.1.7.0
Дата истечения срока действия:	Настоящая версия документа является самой последней, пока не будет опубликована следующая версия.

Комплект всех документов, описывающих ИОК «Сименс», обозначается OID 1.3.6.1.4.1.4329.7.

1.3 Участники ИОК

Участниками Инфраструктуры открытых ключей (ИОК) являются центры сертификации «Сименс», центры регистрации, субъекты и доверяющие партнеры.

1.3.1 Удостоверяющие центры

Графическая схема иерархии УЦ изображена на *Рисунке 1: Иерархия ИОК «Сименс».*

1.3.1.1 Корневой УЦ

Архитектура ИОК «Сименс» основана на двухуровневой структуре УЦ. Данная архитектура позволяет Корневому УЦ хранить данные в автономном режиме.

Корневой УЦ «Сименс» осуществляет подписание, выдачу и отзыв сертификатов, используемых для создания и аутентификации Выпускающего УЦ «Сименс». Корневой УЦ «Сименс» только выдает сертификаты УЦ. Корневой УЦ «Сименс» также используется для подписания списка отозванных сертификатов CRL.

1.3.1.2 Выпускающие УЦ

Выпускающие УЦ «Сименс» выдают сертификаты конечным пользователям, а также управляют и отзывают сертификаты конечных пользователей.

1.3.2 Центры регистрации

Для сертификатов, выдаваемых физическим лицам, УЦ «Сименс» может делегировать регистрацию конечных пользователей двум типам центров регистрации:

- Управление корпоративными идентификационными картами (также называемое «локальным центром регистрации» или «LRA»), как правило, служит для идентификации и аутентификации первоначальных заявителей на получение сертификата;
- Электронная служба самообслуживание ИОК («PKISS»), как правило, служит для идентификации и аутентификации при обновлении ключа для существующих сертификатов.

Для сертификата *сервера и сертификата подписи кода* УЦ «Сименс» может делегировать регистрацию одному центру регистрации:

- Сервер центра регистрации отвечает за идентификацию и аутентификацию ответственного за сервер.
- Заявитель на получение сертификата, ответственный за сервер, должен быть сотрудником «Сименс» или деловым партнером.

Обязанности центра регистрации включают:

1. Создание среды и процедур для заявителей на получение сертификата при подаче заявок на сертификаты;
2. «Идентификация и аутентификация» заявителей на получение сертификата;
3. Утверждение или отклонение заявок на сертификаты;

4. Создание среды и процедур предоставления субъектам данных активации, пар ключей и сертификата на носителях («Средства личной безопасности» или «PSE»);
5. Проверка отзыва сертификатов; либо по запросу Субъекта, либо по инициативе УЦ (или центра регистрации);
6. Идентификация и аутентификация субъектов, подающих запросы на получение нового сертификата после процесса выдачи повторного ключа и для сертификатов, выданных в ответ на одобренные запросы на выдачу сертификата с повторным ключом.

Регистрация субъектов (лиц, сервера или функций) не может быть передана третьему лицу.

1.3.3 Подписант

Подписантом всегда является «Сименс» как юридическое лицо, которое подает заявку на сертификаты конечного объекта и владеет ими. Ответственным за ключ и содержание сертификата конечного объекта является подписант. Тем не менее, «Сименс» делегирует права назначенным лицам и отделам, которые впоследствии действуют от имени «Сименс» (субъектов). Примерами таких лиц и отделов являются администраторы или сотрудники.

Обязанности подписанта включают:
1. предоставлять полную, точную и правдивую информацию в заявке на сертификат;
2. запрашивать отзыв сертификата субъекта, когда сертификат содержит неправильную информацию, или закрытый ключ подписанта или данные активации, контролирующие его доступ, были утрачены, или, когда у подписанта имеются основания полагать, что доступ к закрытому ключу получило другое лицо, или закрытый ключ был иным образом скомпрометирован;
3. подтверждение получения или согласия на ответственность подписанта.

1.3.4 Субъект (конечный пользователь)

Субъект — это отдельное лицо, которое аутентифицируется закрытым ключом и имеет контроль над его использованием.

Субъект
(1) называется или идентифицируется в соответствующем элементе сертификата, выданного этому лицу, и
(2) ему принадлежит закрытый ключ, который соответствует открытому ключу, указанному в этом сертификате.

Обязанности субъекта включают:
1. принять все разумные и необходимые меры предосторожности для предотвращения потери, раскрытия, изменения или несанкционированного использования закрытого ключа субъекта или данных активации, контролирующих его доступ;
2. использовать сертификаты только для ведения бизнеса с «Сименс» или в ее интересах, для приложений, поддерживаемых УЦ, и в течение всего срока работы субъекта или агентства;
3. использовать только пары ключей, привязанные к действительным сертификатам; а также
4. прекратить использование закрытого ключа после отзыва или истечения срока действия Сертификата.

1.3.5 Доверяющие стороны

«Доверяющая сторона» означает участника ИОК, который использует сертификат для получения открытого ключа субъекта и может рассчитывать на заверения в сертификате. Когда какое-либо лицо полагается на сертификат в целях ведения своего бизнеса или для личного использования, то данное лицо является Доверяющей стороной. Однако, если какое-либо лицо действует от имени работодателя или другого принципала, работодатель или принципал является Доверяющей стороной. Когда устройство и приложение, полагающиеся на сертификаты, находятся под контролем организации и физических лиц, действующих от имени организации, то Доверяющей стороной является контролирующая организация.

Для целей настоящей ПС Доверяющие стороны ограничиваются лицами (физическими или юридическими лицами, или серверами, представленными указанными сотрудниками «Сименс»), которые заключили соответствующее соглашение, определяющее и контролирующее потенциальные заверения, гарантии и ответственность Выпускающих УЦ «Сименс» и других участников ИОК.

Обязанности Доверяющей стороны включают:
1. выполнять криптографические операции: проверку цифровых подписей путем ссылки на открытый ключ субъекта, указанный в действительном сертификате, и проверку наличия пути сертификата к доверенному УЦ;
2. проверять статус сертификатов, прежде чем полагаться на них, включая статус отзыва, в списке отзыва сертификатов («CRL») или посредством протокола проверки статуса сертификата онлайн («OSCP»);
3. согласиться с условиями применимого соглашения, требуемого в качестве условия для использования сертификата.

1.4 Использование сертификата

1.4.1 Надлежащее использование сертификата

Сертификаты, подписанные Корневым УЦ «Сименс», утверждаются для следующих видов использования:

Сертификат	Использование
Сертификат Корневого УЦ	Данный сертификат подписывается самим Корневым УЦ и одобряется только для подписания сертификатов Выпускающего УЦ, сертификатов CRL Корневого УЦ и сертификатов подписанта OCSP.
Сертификаты Выпускающего УЦ	Эти сертификаты одобряются только для подписания сертификатов конечных пользователей, CRL Выпускающего УЦ и сертификатов подписанта OCSP.

Утвержденные способы использования ключей и сертификатов, подписанные соответствующими Выпускающими УЦ, можно найти в соответствующих ЗПС.

1.4.2 Запрещенное использование сертификата

Все способы использования Сертификатов, не указанные в 1.4.1, запрещены.

1.5 Управление политикой

УЦ «Сименс» соответствует текущей версии Базовых требований к выпуску и управлению общедоступными доверенными сертификатами, опубликованной на веб-сайте: http://www.cabforum.org. В случае любого несоответствия между настоящим документом и этими требованиями эти требования обладают преимущественной силой перед настоящим документом.

УЦ «Сименс» соответствует текущей версии Минимальных требований к выпуску и управлению сертификатами подписи доверенного кода («Минимальные требования к подписи кода»), опубликованной на веб-сайте https://aka.ms/csbr. В случае любого несоответствия между настоящим документом и этими требованиями эти требования обладают преимущественной силой перед настоящим документом.

1.5.1 Организация, управляющая документом

Организация, ответственная за составление, поддержание и обновление настоящей регламента:

Siemens Aktiengesellschaft ("Siemens AG")
Глобальная служба («GS») Информационные технологии («IT»), «Информационная безопасность» («ISEC»)
Otto-Hahn-Ring 6, 81739 Munich, GERMANY (ГЕРМАНИЯ)
Эл. почта: contact.pki@siemens.com
Веб-сайт: https://www.siemens.com/pki/

1.5.2 Контактное лицо

Вопросы касательно настоящей ПС могут направляться по адресу:

Siemens AG
GS IT ISEC
Вниманию: PKI Siemens
Otto-Hahn-Ring 6, 81739 Munich, GERMANY (ГЕРМАНИЯ)
Эл. почта: contact.pki@siemens.com
Веб-сайт: https://www.siemens.com/pki/

1.5.3 Лицо, определяющее соответствие ПС и ЗПС Политике

Центр управления политиками (PMA) «Сименс» в §1.5.1 ПС и §1.5.2 ПС определяет соответствие ПС и ЗПС Политике.

1.5.4 Процедуры утверждения ПС и ЗПС

Ежегодная оценка риска проводится для оценки бизнес-требований и определения требований безопасности, которые должны быть включены в политику сертификации для указанного сообщества и области применения. Кроме того, ПС и ЗПС будут ежегодно пересматриваться в отношении согласованности с фактическими процессами и сервисами ИОК (см. также §8).

Настоящий документ принят и одобрен Руководителем Отдела информационной безопасности «Сименс» (ISEC).

2 Обязанности по публикации и хранению

УЦ «Сименс» делает свои ПС, ЗПС, сертификаты, CRL общедоступными через веб-сайт «Сименс» и соответствующие дополнительные каналы связи.

Кроме того, он поддерживает сетевое хранилище информации об отзыве сертификатов.

Веб-сайт можно найти по адресу: http://www.siemens.com/pki.

2.1 Хранилища

Хранилища УЦ «Сименс» используются либо самим УЦ «Сименс», либо доверенными поставщиками услуг.

В обязанности хранилища входит следующее:

1. точно публиковать информацию;
2. публиковать и архивировать сертификаты;
3. публиковать статус сертификатов;
4. обеспечивать доступность для УЦ, центров регистрации, субъектов и доверяющих сторон в период доступности, указанный в документации ИОК «Сименс»;
5. обеспечивать оперативность или периодичность публикации; а также
6. обеспечивать безопасность хранилища и контроль доступа к информации, опубликованной в хранилище, для предотвращения несанкционированного доступа и вмешательства.

Субъекты и доверяющие стороны будут иметь доступ к:

- Списку отзыва сертификатов (CRL) через:
  - HTTP: http://ch.siemens.net/pki? <GID of Issuing CA>.crl
  - LDAP: ldap://cl.siemens.net/CN=<GID of Issuing CA>,L=PKI?certificateRevocationList

- Информации о статусе сертификата в режиме онлайн через:
  - HTTP: http://ocsp.pki-services.siemens.com

2.2 Публикация информации о сертификации

УЦ «Сименс» публикует общедоступную информацию по адресу http://www.siemens.com/pki/.

Как минимум, публикуется следующая информация:

- ❑ все необходимые сертификаты, требующиеся для доверия Корневым УЦ
- ❑ все сертификаты Выпускающего УЦ, а также
- ❑ выданные сертификаты шифрования
- ❑ сведения об отзыве сертификатов Корневого УЦ и Выпускающего УЦ и сертификатов конечных пользователей
- ❑ возможная компрометация используемых алгоритмов или соответствующих параметров

Для сообщества «Сименс», сообщества серверов и сообщества деловых партнеров доступна следующая информация.

2.3 Время или периодичность публикации

Обновления ПС и ЗПС публикуются в соответствии с определениями в § 9.12 настоящего документа.

Сертификаты публикуются после выпуска.
Информация о статусе сертификата публикуется ежедневно.

2.4 Контроль доступа в хранилищах

Информация, опубликованная в хранилище (https://www.siemens.com/pki/), доступна в режиме только для чтения через Интранет «Сименс» или Интернет, в соответствии с существующими процедурами и политиками.

УЦ «Сименс» требует от операторов хранилища применять технические и организационные меры безопасности для предотвращения неправильного использования со стороны уполномоченных лиц или предотвращения несанкционированного доступа к добавлению, удалению или изменению записей в хранилище.

3 Идентификация и аутентификация

3.1 Присвоение имени

3.1.1 Типы имен

Полная политика с указанием имен и профилей сертификатов УЦ приводится в §7 соответствующей ЗПС для каждого типа сертификата.

3.1.2 Информативность имен

3.1.2.1 Имена УЦ

Стандартное имя (CN) следует указывать как полное имя УЦ. Имя УЦ указывает его назначение.

3.1.2.2 Имена конечных пользователей

Сертификаты конечных пользователей (EE) содержат общепринятые имена, позволяющие определить личность физического лица

3.1.3 Анонимность или псевдоним субъектов

3.1.3.1 Имена УЦ

Использование псевдонимов для имен УЦ запрещается.

3.1.3.2 Имена конечных пользователей

Для персональных сертификатов EE запрещается указывать анонимные имена или псевдонимы в поле темы сертификата, то есть имена, отличные от истинного личного имени субъекта.

3.1.4 Правила интерпретации различных форм имени

Не предусмотрено.

3.1.5 Уникальность имен

3.1.5.1 Имена УЦ

УЦ «Сименс» гарантирует, что имена Корневых УЦ и Выпускающих УЦ уникальны.

3.1.5.2 Имена конечных пользователей

Выпускающие УЦ «Сименс» во время процесса регистрации должны обеспечить уникальность сертификатов.

Это осуществляется путем присвоения уникального серийного номера сертификатам X.509.

3.1.6 Признание, аутентификация и роли товарных знаков

Заявителям на получение сертификата запрещено использовать имена в своих заявках на сертификаты, которые нарушают права интеллектуальной собственности других лиц. Однако УЦ «Сименс» не проверяет, имеет ли заявитель на получение сертификата права интеллектуальной собственности на имя, указанное в заявке на сертификат, а также не занимается разрешением любых споров, касающихся прав собственности на любое доменное имя, торговое название, товарный знак или знак обслуживания. Без возникновения какой-либо ответственности перед любым из заявителей на получение сертификата УЦ «Сименс» может отклонить или приостановить действие любого заявления на сертификат в связи с таким спором.

3.2 Первоначальная проверка личности

Заявителями на получение сертификатов являются конечные объекты. Заявитель всегда действует от имени подписанта («Сименс»).

Сертификат выдается субъекту только в том случае, если субъект подал запрос на получение сертификата и может доказать УЦ владение соответствующим закрытым ключом.

3.2.1 Метод подтверждения наличия закрытого ключа

Запросы на сертификаты принимаются только в виде заявок на сертификаты PKCS#10 или согласно другим

одобренным методам УЦ «Сименс». Проверка подписи запроса PKCS#10 является достаточным доказательством владения соответствующим закрытым ключом. Если пара ключей создается УЦ «Сименс» от имени субъекта (например, если предварительно сгенерированная пара ключей для дешифрования размещается на устройстве создания защищенной подписи, таком как смарт-карта), это требование не применяется.

3.2.2 Идентификация и аутентификация организации

Только заявители, являющиеся членами организации «Сименс», могут запрашивать сертификаты.

3.2.3 Идентификация и аутентификация физического лица

Для всех сертификатов конечных пользователей УЦ «Сименс» должен обеспечить подтверждение ЦР, что:

- заявитель на получение сертификата является лицом, указанным в заявке на сертификат;
- заявитель на получение сертификата по праву имеет закрытый ключ, соответствующий открытому ключу, который должен быть указан в сертификате; а также
- информация, которая должна быть включена в сертификат, является точной, за исключением неподтвержденной информации о подписчике.

Для целей такого подтверждения, ЦР используют информацию из баз данных Отдела по управлению персоналом «Сименс» для утверждения или отклонения заявок на сертификат.

До выдачи сертификата заявители на получение сертификата должны либо:

1. лично присутствовать для проверки уполномоченным ЦР или его назначенным представителем личности заявителя на получение сертификата посредством общепризнанной формы государственной или корпоративной идентификации (например, паспорт, водительское удостоверение или корпоративная идентификационная карточка «Сименс»);
2. проверяться с помощью соответствующей проверки в рамках процесса PKISS;
3. проверяться электронным образом сервером ЦР.

3.2.4 Неподтвержденная информация о заявителе

Не предусмотрено.

3.2.5 Проверка центра

Не предусмотрено.

3.2.6 Критерии взаимодействия между доверенными сообществами

УЦ «Сименс» является членом Европейского моста УЦ и обменивается информацией в отношении ИОК со своими партнерами.

3.3 Идентификация и аутентификация запросов повторного ключа

3.3.1 Корневой УЦ

До истечения срока действия сертификата Выпускающего УЦ инициируется процедура смены ключа. Процедура выполняется доверенным персоналом под двойным контролем в защищенной среде.

3.3.2 Выпускающий УЦ

До истечения срока действия сертификата EE начинается процедура выдачи повторного ключа. Запрос сертификата на основе текущей пары ключей EE должен быть отправлен в соответствующий УЦ (через Портал самообслуживания).

Если подлежащий замене сертификат уже истек или был отозван, должен быть запущен новый процесс идентификации.

3.4 Идентификация и аутентификация запросов на отзыв

3.4.1 Корневой УЦ

Отзыв сертификатов Выпускающего УЦ производится только вручную доверенными сотрудниками УЦ «Сименс» под двойным контролем.

3.4.2 Выпускающий УЦ

Процедуры идентификации и аутентификации для запроса на отзыв сертификатов EE такие же, как и для первоначальной проверки личности.

4 Требования к использованию сертификата на протяжении жизненного цикла

В этом разделе рассматривается администрирование пары ключей Корневого УЦ «Сименс» и Выпускающего УЦ на протяжении всего жизненного цикла Корневого УЦ и Выпускающего УЦ, в том числе вопросы о том, как

- открытый и закрытый ключи генерируются и / или повторно генерируются (т. е. выдача повторного ключа)
- закрытые ключи хранятся, защищаются и в конечном итоге уничтожаются
- открытые ключи распространяются и архивируются.

4.1 Заявка на сертификат

4.1.1 Кто может подать заявку на сертификат?

4.1.1.1 Корневой УЦ

Руководство УЦ «Сименс» решает, когда будет создан новый Выпускающий УЦ и будет подписан Корневой УЦ.

4.1.1.2 Выпускающие УЦ

Заявители на получение сертификата могут быть членами *Сообщества «Сименс» или Сообщества делового партнера «Сименс»*.
Подробная информация указана в ЗПС для Выпускающих УЦ.

4.1.2 Процесс регистрации и обязанности

4.1.2.1 Корневой УЦ

Для получения сертификатов УЦ следующая информация должна быть оформлена документально:

- ❑ Имя УЦ в соответствии с Правилами раздела 3.1 «Присвоение имени» настоящей ПС
- ❑ Дата запроса
- ❑ Срок действия сертификата УЦ, который не может превышать срок действия Сертификата Корневого УЦ;
- ❑ ЗПС для нового Выпускающего УЦ этого Корневого УЦ
- ❑ Профиль сертификата нового Выпускающего УЦ и
- ❑ Профили сертификатов конечного пользователя, которые должны быть подписаны этим новым Выпускающим УЦ

4.1.2.2 Выпускающие УЦ

Заявители на получение сертификата конечного пользователя проходят процесс регистрации, включающий:

- генерирование или организация генерирования пары ключей
- заполнение заявки на сертификат и предоставление необходимой информации
- подтверждение соответствующему ЦР, что у заявителя на получение сертификата владеет закрытым ключом, соответствующим открытому ключу, включенному в заявку на сертификат, и
- уведомление о заявителей на получение сертификата о соответствующих обязанностях субъекта для использования закрытого ключа и сертификатов

Заявки на сертификаты подаются для обработки, одобрения или отклонения, в соответствующие ЦР.

4.2 Обработка заявок на сертификаты

4.2.1 Выполнение функций идентификации и аутентификации

УЦ «Сименс» гарантирует, что заявители на получение сертификата (= «субъекты») будут правильно идентифицированы и аутентифицированы.

Для сертификатов ЕЕ УЦ «Сименс» делегирует выполнение этих задач соответствующим ЦР.

4.2.2 Утверждение или отклонение заявок на сертификаты

После подачи заявки на сертификат заявителем на получение сертификата УЦ «Сименс» должен ее одобрить или отклонить.

УЦ «Сименс» проверяет, является ли заявка на сертификат полной, точной и надлежащим образом разрешенной. Если заявка на сертификат не пройдет проверку, то она будет отклонена.
Для сертификатов ЕЕ эти задачи могут быть делегированы соответствующим ЦР.

4.2.3 Время обработки заявок на сертификаты

Заявки на сертификаты должны своевременно одобряться или отклоняться.

4.2.4 Авторизация центра сертификации (CAA)

"Сименс" проверяет наличие записи об Авторизации центра сертификации (CAA) для каждого DNS-имени в расширении subjectAltName Сертификата, который должен быть выдан в соответствии с процедурой в RFC 6844, согласно инструкциям по обработке, установленным в RFC 6844, для любых найденных записей. Если "Сименс" выпускает Сертификат, "Сименс" делает это в пределах TTL записи CAA или 8 часов, в зависимости от того, что больше. При обработке записей CAA "Сименс" обрабатывает выпуск и выпускает раздельные записи, как указано в RFC 6844. "Сименс" не выдает Сертификат, если обнаруживается непризнанное свойство с критической меткой.

"Сименс" может не проверять записи CAA на наличие следующих исключений:

(i) для Сертификатов, для которых был создан предварительный сертификат прозрачности и зарегистрирован, по крайней мере, в двух общедоступных журналах, а также для которых проводилась проверка CAA.

(ii) для Цифровых сертификатов, выданных технически ограниченным Сертификатом подчиненного УЦ, где отсутствие проверки CAA прямо предусмотрено договором с Заявителем.

(iii) если УЦ или Аффилированное лицо УЦ является DNS-оператором (как определено в RFC 7719) DNS домена.

"Сименс" рассматривает ошибку поиска записи как разрешение на выдачу, если:

(i) сбой находится вне инфраструктуры УЦ;

(ii) попытка поиска повторялась, по крайней мере, один раз; и

(iii) зона домена не имеет цепочки проверки модулей безопасности службы доменных имен (DNSSEC) для корня Корпорации по управлению доменными именами и IP-адресами (ICANN).

"Сименс" документально подтверждает потенциальные выпуски, которые были приостановлены из-за записи CAA, и отправляет отчеты о таких запросах выпуска контактному лицу, указанному в записи (записях) коммуникативного формата описания инцидентных объектов (IODEF) CAA, если таковые имеются.

"Сименс" поддерживает схемы URL вида mailto: и https: в записи IODEF. Идентифицирующий домен CAA для "Сименс" - siemens.com'. Результаты проверки записей CAA регистрируются в Центре регистрации сервера "Сименс" (ServerRA).

4.3 Выдача сертификата

4.3.1 Действия Корневого УЦ во время выдачи сертификата

Для обеспечения надлежащей безопасности пары ключей Корневого УЦ компьютер, на котором запущены службы Корневого УЦ, не подключается к сети и находится в автономном хранилище безопасности, которое соответствует стандартам безопасности для криптографических модулей, указанных в главе 6.2.1.

Процедуры устанавливаются и утверждаются для обеспечения целостности и предотвращения отказа запросов на сертификаты и сертификации открытого ключа Выпускающего УЦ. Доступ к устройствам Корневого УЦ «Сименс» предоставляется только уполномоченному персоналу. Кроме того, аутентификация M*N используется для обеспечения надлежащего доступа к службам Корневого УЦ.

4.3.2 Действия Корневого УЦ во время выдачи сертификата

Сертификат создается и выдается с использованием защищенных средств после утверждения заявки на сертификат. УЦ «Сименс»:

1. генерирует для субъекта сертификат на основании информации, содержащейся в заявке на сертификат, после ее одобрения
2. проверяет авторизацию соответствующего ЦР через безопасный сервер, а также
3. предоставляет сертификат, пары ключей и данные активации (совместно «Средства личной безопасности» или «PSE») субъекту через соответствующие ЦР с использованием защищенных средств. Если был получен запрос PKCS#10, то субъекту предоставляется только сертификат.

Эти процедуры также используются для выдачи сертификатов в связи с подачей запроса на замену (то есть на выдачу повторного ключа) сертификата.

4.3.3 Уведомление субъекта о выдаче сертификата УЦ

После генерации сертификата соответствующий ЦР должен проинформировать субъектов о доступности их сертификатов и средствах для безопасного получения их сертификатов.

4.4 Принятие сертификата

4.4.1 Корневой УЦ

Принятие сертификата выполняется как в рамках или в результате Процедуры создания УЦ.

4.4.2 Выпускающий УЦ

После выдачи сертификатов данные активации (например, ПИН-код субъекта) предоставляются субъектам посредством сообщения (по электронной почте или иным образом). Субъект должен надежным образом получить пару ключей и / или сертификат через соответствующий ЦР.

4.4.3 Уведомление УЦ о выдаче сертификата другим организациям

УЦ «Сименс» является членом Европейского моста УЦ и предоставляет партнерам информацию о выдаче сертификатов.

4.5 Пара ключей и использование сертификата

4.5.1 Закрытый ключ Корневого УЦ и использование сертификата

Закрытый ключ Корневого УЦ используется только для:

- ❑ Выдачи сертификатов Корневого УЦ «Сименс»
- ❑ Выдачи сертификатов Выпускающего УЦ
- ❑ Выдача CRL Корневого УЦ «Сименс»
- ❑ Выдача сертификатов подписанта OCSP

4.5.2 Закрытый ключ Выпускающего УЦ и использование сертификата

Закрытый ключ Выпускающего УЦ используется только для:

- ❑ Выдача сертификатов конечных пользователей
- ❑ Выдача CRL Выпускающего УЦ «Сименс»
- ❑ Выдача сертификатов подписанта OCSP
- ❑ Защита (шифрование) центрально генерируемых закрытых ключей

4.5.3 Закрытый ключ субъекта и использование сертификата

Закрытые ключи субъекта и сертификаты должны использоваться только для целей, указанных в сертификате.

4.5.4 Открытый ключ доверяющей стороны и использование сертификата

Перед любыми действиями, основанными на доверии, доверяющие стороны должны

- ❑ надежным образом получить сертификат Корневого УЦ «Сименс», сертификат Выпускающего УЦ и любые другие сертификаты в соответствующей цепочке сертификатов, а также
- ❑ надежным образом получить и проверить действие, приостановку действия или отзыв сертификата, используя информацию о текущем статусе отзыва, которая указывается доверяющей стороне всех сертификатов в цепочке сертификатов
- ❑ учитывать любые ограничения в использовании и лимиты ответственности по Сертификату, указанные для доверяющей стороны в настоящей ПС

Доверяющие стороны несут ответственность за проверку сертификатов, включая цепочку сертификатов и статус отзыва.

4.6 Продление сертификата

Продление сертификата означает выдачу нового сертификата лицу без изменения открытого ключа или любой другой информации в сертификате.

В принципе, продление сертификата не предусматривается.

4.6.1 Обстоятельства для продления сертификата

Не предусмотрено.

4.6.2 Кто может запросить продление?

Не предусмотрено.

4.6.3 Обработка запроса на продление сертификата

Не предусмотрено.

4.6.4 Уведомление о выдаче нового сертификата субъекту

Не предусмотрено.

4.6.5 Поведение, подтверждающее принятие продленного сертификата

Не предусмотрено.

4.6.6 Публикация продленного сертификата УЦ

Не предусмотрено.

4.6.7 Уведомление УЦ о выдаче сертификата другим организациям

Не предусмотрено.

4.7 Сертификат с повторным ключом

«Выпуск повторного ключа» означает генерацию новой пары ключей, применяется для выдачи нового сертификата и заменяет существующую пару ключей.

Как правило, к выпуску повторного ключа сертификата применяются те же требования, что и в §4.3. Выдача сертификата. Ранее подтвержденная информация не подлежит повторному использованию.

4.7.1 Обстоятельства для выдачи сертификатов с повторным ключом

Процесс выпуска повторного ключа запрашивается только в том случае, если право собственности на соответствующий сертификат подтверждается сертификатом, который все еще является действительным.

4.7.2 Кто может запросить сертификацию нового открытого ключа?

4.7.2.1 Выпуск повторного ключа Выпускающим УЦ

Выпуск повторного ключа для сертификатов Выпускающего УЦ запрещается.

4.7.2.2 Выпуск повторного ключа сертификатов конечных пользователей

Не предусмотрено дополнительных требований.

4.7.3 Обработка запроса на выдачу сертификата с повторным ключом

Не предусмотрено дополнительных требований.

4.7.4 Уведомление о выдаче нового сертификата субъекту

Не предусмотрено дополнительных требований.

4.7.5 4 Поведение, подтверждающее принятие сертификата с повторным ключом

Не предусмотрено дополнительных требований.

4.7.6 Публикация сертификата с повторным ключом УЦ

Не предусмотрено дополнительных требований.

4.7.7 Уведомление УЦ о выдаче сертификата другим организациям

Не предусмотрено дополнительных требований.

4.8 Изменение сертификата

Изменение сертификата означает, что ключи сертификата остаются неизменными, но изменяется больший объем информации о сертификате, чем при продлении сертификата.

Не допускается изменение сертификата.

4.8.1 Обстоятельства для изменения сертификата

Не применимо.

4.8.2 Кто может запросить изменение сертификата?

Не применимо.

4.8.3 Обработка запросов на изменение сертификата

Не применимо.

4.8.4 Уведомление о выдаче нового сертификата субъекту

Не применимо.

4.8.5 Поведение, подтверждающее принятие измененного сертификата

Не применимо.

4.8.6 Публикация измененного сертификата УЦ

Не применимо.

4.8.7 Уведомление УЦ о выдаче сертификата другим организациям

Не применимо.

4.9 Отзыв и приостановка сертификата

4.9.1 Обстоятельства для отзыва

4.9.1.1 Отзыв сертификатов Выпускающего УЦ

В дополнение к причинам, указанным в соответствующем ЗПС, «Сименс» выполняет условия своего партнера по перекрестному подписанию. Кроме того, могут существовать следующие технические причины для отзыва Сертификата:

- ❑ используемые длины ключа или алгоритмы больше не кажутся достаточно безопасными
- ❑ необходимо изменить иерархию УЦ, и
- ❑ Центр управления политиками признает наличие острой угрозы еще неизвестного технического характера.

4.9.2 Кто может запросить отзыв?

Не предусмотрено дополнительных требований

4.9.3 Процедура подачи запроса на отзыв

УЦ «Сименс» поддерживает безопасный и аутентифицированный отзыв сертификатов EE и обеспечивает возможность быстрой передачи такого отзыва посредством выпуска CRL, публикуемого по мере необходимости.

После отзыва сертификата Выпускающего УЦ или сертификата EE вновь отозванный сертификат записывается в CRL, который публикуется в течение 24 часов.

Лицо, запрашивающее отзыв сертификата EE, должно передать запрос в УЦ «Сименс» через соответствующий ЦР, чтобы инициировать отзыв сертификата, который выполняется незамедлительно. Сообщение о таком

запросе на отзыв должно быть предоставлено в соответствии с §3.4 ПС.

4.9.4 Период отсрочки для подачи запроса на отзыв

Запросы на отзыв направляются запрашивающим лицом сразу, как только у него возникнут основания полагать, что имеются обстоятельства для отзыва сертификата.

4.9.5 Время, в течение которого УЦ должен обработать запрос на отзыв

УЦ «Сименс» обрабатывает запрос на отзыв и отчеты о проблеме с сертификатом в течение 24 часов после его направления.

4.9.6 Требование к проверке отзыва для доверяющих сторон

Доверяющие стороны проверяют статус сертификатов, на которые они хотят полагаться, в последнем CRL или используя другой применимый метод.

4.9.7 Частота выпуска списков отзыва сертификатов (CRL)

CRL выпускаются каждые 24 часа.

4.9.8 Максимальное время ожидания для списков отзыва сертификатов (CRL)

CRL размещаются в хранилище в течение разумного периода времени после их создания. Обычно это делается автоматически в течение нескольких минут.

4.9.9 Возможность проверить статус отзыва в режиме онлайн

Предлагается услуга проверки статуса сертификата на основании ответчика OCSP, использующего RFC2560, RFC5019 и RFC6960. Ответчик OCSP поддерживает работу HTTP GET для целей запроса статуса сертификата. Обратный статус всегда основывается на самом последнем доступном CRL или непосредственно на информации в базе данных УЦ. Если ответчик OCSP получает запрос статуса сертификата, который не был выпущен, ответчик отвечает обратным кодом UNKNOWN. УЦ «Сименс» контролирует файлы журнала ответчиков OCSP на признаки несуществующих сертификатов.

4.9.10 Требования к проверке отзыва в режиме онлайн

Доверяющие стороны проверяют статус сертификата в последнем CRL, опубликованном УЦ «Сименс» или ответчиком OCSP.

4.9.11 Другие доступные формы сообщений об отзыве

Не предусмотрено.

4.9.12 Специальные требования к компрометации закрытого ключа

Если у УЦ «Сименс» имеются основания полагать, что закрытый ключ УЦ был скомпрометирован, он должен уведомить об этом потенциальные доверяющие стороны через свой веб-сайт.

Если у субъекта имеются основания полагать, что закрытый ключ ЕЕ УЦ был скомпрометирован, он должен уведомить свой соответствующий ЦР о принятии соответствующих мер, включая направление запроса на отзыв.

4.9.13 Обстоятельства для приостановки

Приостановка сертификата для сертификатов, выданных УЦ «Сименс», не предусматривается.

4.10 Службы проверки статуса сертификатов

4.10.1 Эксплуатационные характеристики

Не предусмотрено.

4.10.2 Доступность службы

Служба должна быть доступна двадцать четыре (24) часа в день, семь (7) дней в неделю, за исключением случаев форс-мажорных обстоятельств (§ 9.16.5 ПС). Ее работа постоянно контролируется с той целью, чтобы время отклика составляло менее десяти (10) секунд на запрос.

Что касается отчетов о проблеме с сертификатом с высоким приоритетом, см. ЗПС §4.9.3.

4.10.3 Дополнительные характеристики

Не предусмотрено.

4.11 Окончание срока действия подписи

Поскольку единственным подписантом УЦ «Сименс» является «Сименс», УЦ «Сименс» прекращает работу в случае окончания срока действия подписи.

4.12 Депонирование и восстановление ключей

Депонирование ключей выполняется только для ключей шифрования конечных пользователей.

Закрытый ключ субъекта может быть восстановлен для субъекта или для третьей стороны при следующих условиях:

- Субъект может запросить восстановление в любое время
- Контролер субъекта может запросить восстановление, если субъект покинул компанию
- Контрольно-правовой или юридический отдел может запросить восстановление с согласия PMA

5 Управление, операционный и физический контроль

Управление, операционный и физический контроль определены в соответствии с [ETSI EN 319 411-1] и [ETSI EN 319 401].

Надежные системы и продукты, которые использует УЦ «Сименс», защищены от модификации для обеспечения технической и криптографической безопасности поддерживаемого ими процесса.

УЦ «Сименс» работает в соответствии с системой управления информационной безопасностью ("СМИБ") "Сименс", которая поддерживает требования безопасности данного ЗПС. Такая СМИБ основана на стандарте ISO27001. Ниже приведен обзор требований безопасности для корневого УЦ «Сименс».

5.1 Контроль физической безопасности

5.1.1 Месторасположение и оборудование

Узел сертифицирован в соответствии с 4-м уровнем Безопасной инфраструктуры для ИТ-систем TÜV.

5.1.2 Физический доступ

Узел сертифицирован в соответствии с 4-м уровнем Безопасной инфраструктуры для ИТ-систем TÜV.

5.1.3 Электропитание и кондиционирование воздуха

Узел сертифицирован в соответствии с 4-м уровнем Безопасной инфраструктуры для ИТ-систем TÜV.

5.1.4 Воздействие воды

Узел сертифицирован в соответствии с 4-м уровнем Безопасной инфраструктуры для ИТ-систем TÜV.

5.1.5 Пожарная безопасность

Узел сертифицирован в соответствии с 4-м уровнем Безопасной инфраструктуры для ИТ-систем TÜV.

5.1.6 Хранение носителей

Все носители информации, содержащие производственное программное обеспечение и данные, информацию по проверкам, архивную или резервную информацию, хранятся на специально охраняемых территориях в различных местах или в надежном внешнем хранилище с соответствующим физическим и логическим контролем доступа, созданным для ограничения доступа с его предоставлением только уполномоченному персоналу и защиты таких носителей от случайного повреждения (например, воды, огня и электромагнитных волн).

5.1.7 Утилизация отходов

Конфиденциальные документы и материалы измельчаются перед утилизацией в соответствии с DIN66933. Носители, используемые для сбора или передачи защищаемой информации, перед утилизацией приводятся в нечитаемый вид. Криптографические устройства физически уничтожаются или обнуляются в соответствии с указаниями изготовителей перед их утилизацией.

5.1.8 Внешнее резервное копирование

Выполняется регулярное резервное копирование важных системных данных, данных журнала аудита и другой защищаемой информации. Внешние носители резервных копий хранятся физически безопасным образом с помощью средств аварийного восстановления "Сименс".

5.2 Контроль процедур

5.2.1 Доверенные функции

Доверенные функции для работы корневого УЦ «Сименс» включают весь персонал, имеющий доступ или контроль над "внутренними" операциями корневого УЦ, которые могут существенно повлиять на:

- проверку информации в заявках на сертификат;
- принятие, отклонение или иную обработку заявок на сертификаты, запросов повторного ключа или отзывов, или информации для регистрации, а также
- выдачу или отзыв сертификатов, включая доступ к ограниченным частям Хранилища.

Доверенные функции в работе корневого УЦ включают, без ограничений:

Доверенные функции, определенные в ETSI TS 102 042 V2.4.1 (2013-02):

- ❑ сотрудники службы безопасности
- ❑ системные администраторы
- ❑ системные операторы
- ❑ системные аудиторы

Дополнительные доверенные функции в УЦ «Сименс»:

- ❑ Сотрудник по защите данных
- ❑ Руководитель по информационной безопасности (CISO)

5.2.2 Количество персонала, которое требуется для выполнения Задания

Определение и поддержание четкой процедуры контроля обеспечивает разделение функций на основе должностных обязанностей. Для выполнения важных задач требуется несколько Доверенных лиц.

Следующие действия требуют, чтобы как минимум два доверенных сотрудника имели физический или логический доступ к устройству или локации:

- ❑ Доступ к объектам высокого уровня безопасности;
- ❑ Логический и физический доступ к HSM;
- ❑ Физический доступ к архиву данных, и
- ❑ Логический доступ к центральным, защищаемым или критическим системам корневого УЦ «Сименс» и его системам резервного копирования.

5.2.3 Идентификация и аутентификация каждой функции

Идентификация и аутентификация лиц в зонах безопасности осуществляется с помощью двухфакторной аутентификации. Доступ к критическим системам контролируется смарт-картами. В системах управления авторизация пользователей управляется в зависимости от функций.

Реализованы меры контроля для защиты от несанкционированного выноса с территории оборудования, информации, носителей и программного обеспечения, связанного с услугами УЦ.

5.2.4 Функции, требующие разделения обязанностей

Любая Доверенная функция в деятельности УЦ «Сименс» требует присутствия и участия как минимум двух доверенных сотрудников. Таким образом, не требуется никаких условий для разделения обязанностей в рамках одной функции.

5.3 Контроль безопасности персонала

5.3.1 Требования к квалификации, опыту и допуску

Кандидаты на Доверенные должности должны представить свидетельства наличия соответствующего образования, полномочий и опыта, необходимых для компетентного и удовлетворительного выполнения предполагаемых должностных обязанностей, а также свидетельства наличия разрешений, выданных государственными органами, если таковые имеются, которые необходимы для оказания услуг сертификации по государственным контрактам.

5.3.2 Процедура проверки биографических данных

Проверка биографических данных всех кандидатов на работу (подрядчиков и внешних пользователей) проводится согласно соответствующим законам, Правилам и этическим нормам и соразмерна бизнес-требованиям, классификации информации, к которой предоставляется доступ, а также предполагаемым рискам. Через регулярные промежутки времени проводятся проверки судимости или аналогичные проверки.

Сотрудники, не прошедшие первоначальные или периодические проверки, не могут выполнять или продолжать выполнять Доверенные функции.

5.3.3 Требования к обучению

Весь персонал, выполняющий управленческие обязанности в отношении работы УЦ «Сименс», должен пройти

всестороннее обучение по:

- ❑ принципам и механизмам безопасности;
- ❑ осведомленности о безопасности;
- ❑ всем используемым версиям программного обеспечения;
- ❑ всем обязанностям, которые они должны выполнять, и
- ❑ процедурам аварийного восстановления и обеспечения непрерывности бизнес-процессов.

5.3.4 Периодичность и требования к переподготовке

Сотрудники с Доверенными функциями должны проходить обучение и повышение квалификации в объеме и с периодичностью, которые требуются для поддержания необходимого уровня квалификации для выполнения своих должностных обязанностей грамотно и удовлетворительно. Обучение по безопасности данных и защите конфиденциальности данных должно проводиться на постоянной основе.

5.3.5 Периодичность и порядок ротации должностей

Не предусмотрено.

5.3.6 Взыскания за несанкционированные действия

За несанкционированные действия или другие нарушения политики и процедур защиты информационной безопасности и конфиденциальности данных предусмотрены соответствующие дисциплинарные взыскания, которые могут быть соизмеримы с частотой и серьезностью несанкционированных действий. Дисциплинарные взыскания включают различные меры вплоть до увольнения.

5.3.7 Требования к независимому подрядчику

Независимые подрядчики, внешние консультанты или стажеры не должны привлекаться к выполнению Доверенных функций в работе УЦ «Сименс».

Если привлечение независимых подрядчиков, консультантов или стажеров необходимо, им должен предоставляться доступ к защищенным объектам, только если их сопровождают и напрямую контролируют уполномоченные сотрудники с Доверенными функциями.

5.3.8 Документы, предоставляемые персоналу

Персоналу, выполняющему Доверенные функции, предоставляется "Руководство по корпоративной информационной безопасности" компании "Сименс АГ" и иная документация, которая является обязательной для всех сотрудников, выполняющих доверенные функции.

Эта информация необходима, чтобы сотрудники выполняли свои должностные обязанности грамотно и удовлетворительно.

5.4 Процедуры ведения журнала аудита

Цель ведения журнала заключается в непрерывной проверке изменений параметров, изменений конфигурации и т. п. компонентов систем УЦ. Ведение журнала сосредоточено, в частности, на следующем:

- ❑ Действия с административными компонентами, и
- ❑ Вмешательства в приложения: Веб-сервер, База данных, Аутентификация, Удостоверяющий Центр.

Собранные данные анализируются автоматически.

5.4.1 Типы регистрируемых событий

УЦ «Сименс» регистрирует сведения о действиях, предпринятых для обработки запросов на сертификаты и выдачи Сертификатов, включая всю сгенерированную информацию и полученную документацию в связи с запросом на сертификат; время и дату; а также задействованный персонал.

УЦ регистрирует как минимум следующие события:

1. События управления жизненным циклом ключа УЦ, включая:
   a. Создание ключей, резервное копирование, хранение, восстановление, архивирование и уничтожение; и
   b. События управления жизненным циклом криптографических устройств.

2. События управления жизненным циклом сертификатов УЦ и Подписчика, включая:
    a. Запросы на сертификаты, обновления и запросы повторного ключа, а также отзыв;
    b. Все проверочные мероприятия, предусмотренные настоящими Требованиями, а также Заявления о практике сертификации УЦ;
    c. Дата, время, используемый номер телефона, контактные лица и конечные результаты проверки телефонных звонков;
    d. Прием и отклонение запросов на получение сертификата;
    e. Выдача Сертификатов; и
    f. Создание Списков отзыва сертификатов и записей OCSP.
3. События безопасности, включая:
    a. Удачные и неудачные попытки доступа к системе ИОК;
    b. Выполненные действия ИОК и системы безопасности;
    c. Изменения профиля безопасности;
    d. Отказы системы, сбои оборудования и другие аномалии;
    e. Действия брандмауэра и маршрутизатора; и
    f. Входы и выходы из здания УЦ.

Записи журнала включают следующие элементы:

1. Дата и время записи;
2. Личность лица, делающего запись в журнале; и
3. Описание записи.

5.4.2 Частота обработки информации в журнале аудита

Данные аудита и журнала должны контролироваться PMA после всех событий УЦ. УЦ «Сименс» делает записи, созданные в соответствии с §5.4.1, доступными для Квалифицированного аудитора в качестве доказательства соответствия УЦ настоящим Требованиям.

5.4.3 Срок хранения информации Журнала аудита

Журналы аудита хранятся на месте в течение неограниченного времени.

5.4.4 Защита Журналов аудита

Журналы аудита защищены электронной системой журнала аудита, которая включает механизмы защиты файлов журнала от несанкционированного просмотра, изменения, удаления или других вмешательств. Информация по действиям, введенная вручную, должна быть защищена от несанкционированного просмотра, изменения и уничтожения.

5.4.5 Процедура резервного копирования информации из Журнала аудита

Полное резервное копирование выполняется после каждой процедуры создания УЦ. После этого система остается в автономном режиме.

5.4.6 Система сбора для мониторинга информации (внутренняя или внешняя)

Сбор и хранение данных аудита и технического журнала осуществляется в защищенных помещениях.

5.4.7 Уведомление субъекта, инициирующего событие

Если человек или устройство, находящееся под его контролем, инициирует событие аудита, которое приводит к оповещению или создает другую аномальную запись в журнале аудита, либо обнаруживается иным образом, первая ответная реакция должна предотвратить любое дальнейшее вторжение со стороны человека или устройства.

Событие аудита будет проанализировано, чтобы как можно быстрее идентифицировать нарушителя или устройство. Этот анализ включает тщательное изучение всех соответствующих событий аудита. Должны быть приняты меры в соответствии с Процедурой "Сименс" по управлению инцидентами.

5.4.8 Оценка уязвимости

В рамках ежегодной оценки внутренней безопасности "Сименс" проверяется потенциальная уязвимость УЦ «Сименс». Кроме того, текущее состояние уязвимости фиксируется документально с помощью системы оценки

риска, которая документируется и обрабатывается в соответствии с Правилами СМИБ.

5.5 Архив записей

5.5.1 Типы архивируемых записей

Типы архивируемых записей включают следующие категории сведений из журнала аудита:

- ❑ Технические данные журнала
  Технические данные журнала используются для мониторинга событий рабочего состояния для выработки корректирующих действий.
  Технические данные журнала генерируются автоматически и электронно благодаря системным функциям УЦ и сохраняются и помещаются в архив автоматически;
- ❑ Данные аудита
  Данные аудита генерируются автоматически или вручную, используются для событий доступа и предотвращения отказа и требуются УЦ «Сименс» для коммерческих, юридических или организационных целей.

- *Автоматические данные аудита* состоят из информации об аудите, выставлении счетов и статистической информации
  Информация по аудиту служит свидетельством событий, демонстрируя, были ли выполнены действия в соответствии с согласованными процедурами, и в каком объеме идентифицируемые задачи выполняются и завершаются;

  Платежная информация является основой для взимания платы за услуги, оказанные в соответствии с соглашением (соглашениями) об уровне услуг (“SLA”), а также предоставляет количественную информацию о доходах;

  Статистическая информация показывает, соблюдены ли требования SLA, и предоставляет данные для количественного и профилактического анализа систем.
- *Данные аудита, введенные вручную*, состоят из информации о процедуре, которая хранится в рукописном виде в качестве оригинала и подписывается, когда это необходимо для целей представления доказательств. Такие данные включают записи журнала, сокращенные версии документа, инструкции по обновлению и т. д.

5.5.2 Период хранения архивированной информации из Журнала аудита

Срок хранения технических данных Журнала, указанных в §5.5.1, составляет не менее шести недель. Срок хранения автоматических данных аудита, указанных в §5.5.1, составляет не менее десяти лет, при этом должны соблюдаться различные договорные требования, а статистическая информация должна храниться не менее одного года. Данные аудита, введенные вручную, хранятся не менее десяти лет. Сроки хранения устанавливаются законодательством Германии о конфиденциальности данных и могут быть изменены без дальнейшего уведомления для отражения изменений в законодательстве.

5.5.3 Защита архивированной информации из Журнала аудита

Защита архивированных записей осуществляется в соответствии с СМИБ «Сименс». Архивированные записи размещаются на нескольких объектах. Структура безопасности на этих объектах и особый контроль за средствами резервного копирования и архивированными записями включают различные методы защиты от кражи или несанкционированного уничтожения, изменения или утраты, что подробно изложено в Правилах СМИБ.

5.5.4 Процедура резервного копирования архива

Процедуры резервного копирования архива реализованы в соответствии с Правилами СМИБ. Что касается Технических данных Журнала и Автоматических данных об аудите, проводится ежедневное инкрементное резервное копирование и еженедельное полное резервное копирование. Данные аудита, введенные вручную, сохраняются в момент создания. Перед обновлением системы осуществляется полное резервное копирование всех Технических данных Журнала и Автоматических данных об аудите, а также соответствующего программного обеспечения.

5.5.5 Требования к добавлению отметки времени записи

Не предусмотрено.

5.5.6 Система сбора архива (внутренняя или внешняя)

Не предусмотрено.

5.5.7 Процедура получения и проверки архивированной информации

Процедуры получения и проверки сохраненных записей реализованы в соответствии с Правилами СНИБ. Автоматизированная процедура сохранения содержит этапы контроля, которые подтверждают, что сохраненная информация из журнала аудита в дальнейшем может быть проанализирована и предоставлена, а также снова прочитана.

5.6 Смена ключа

Подробная информация приведена в соответствующих ЗПС.

5.7 Компрометация и аварийное восстановление

5.7.1 Процедура действий в случае инцидентов и компрометации

При возникновении чрезвычайных ситуаций и компрометации во время работы УЦ создается Аварийная группа в соответствии с Правилами СМИБ. Эта Аварийная группа собирает информацию, оценивает риски, разрабатывает процедуру, а также предлагает и реализует эту процедуру с одобрения CISO "Сименс". Выбор наиболее подходящей процедуры зависит от последствий конкретного инцидента или компрометации, а также последующего распределения ответственности между участниками ИОК в соответствии с законом или договором.

5.7.2 Повреждение вычислительных ресурсов, программного обеспечения и / или данных

Если вычислительные ресурсы, программное обеспечение или данные УЦ «Сименс» повреждены (например, в результате стихийного бедствия или враждебной атаки), УЦ «Сименс» сообщает об этом в PMA. В этом случае применяется порядок действий при реальных или потенциальных враждебных атаках.

Если затрагивается только корневой УЦ, Выпускающий УЦ может продолжать работать, потому что:

(i) заменяющее аппаратное обеспечение с высокой вероятностью будет быстро закуплено;

(ii) программное обеспечение системы корневого УЦ доступно;

(iii) Закрытый ключ корневого УЦ и CRL хранятся отдельно и в безопасных местах, и

(iv) если пункты (i)-(iii) выполнены, система корневого УЦ может быть повторно активирована по первому требованию.

5.7.3 Процедура в случае компрометации Закрытого ключа организации

Если Закрытый ключ корневого УЦ «Сименс» скомпрометирован или предположительно скомпрометирован, необходимо выполнить следующие процедуры:

- ❑ проинформировать субъекты, Доверяющие стороны и Европейский мост УЦ;
- ❑ указать, что сертификаты и информация о состоянии отзыва, выданные с помощью этого ключа корневого УЦ, более не могут быть действительными;
- ❑ аннулировать Сертификат и службу распространения CRL для Сертификатов и Списков отзыва сертификатов, выданных с использованием скомпрометированного Закрытого ключа; и
- ❑ запросить отзыв всех затронутых Сертификатов.

5.7.4 Возможности обеспечения непрерывности деятельности после аварии

Высокая доступность услуг сертификации, предоставляемых УЦ «Сименс», гарантируется внедрением избыточной установки системы.

В случае повреждения или потери вычислительных ресурсов, программного обеспечения или данных реализуется соответствующий План аварийного восстановления и обеспечения бесперебойной работы согласно Правилам СМИБ на объекте, расположенном в отдельной зоне, способной предоставлять услуги УЦ.

Критически важные услуги, таких как приостановка/отзыв Сертификата, проверка Сертификата и публикация CRL, восстанавливаются в течение двадцати четырех (24) часов максимум. Полная функциональность восстанавливается в течение 30 дней.

5.8 Прекращение УЦ

Если "Сименс" необходимо прекратить предоставление услуг УЦ, УЦ «Сименс» уведомляет Доверяющие стороны и другие заинтересованные организации заранее о прекращении УЦ через свой веб-сайт. Следующий план прекращения должен свести к минимуму нарушения для Доверяющих сторон:

- Публикация уведомления для сторон, которых затрагивает прекращение, включая Европейский мост УЦ;
- Отзыв Сертификата, выданного Выпускающим УЦ;
- Сохранение архивов и записей УЦ за периоды времени, которые установлены в этом ЗПС;
- Продолжение работы Службы поддержи клиентов и Справочной службы;
- Сохранение услуг по отзыву, таких как выдача CRL;
- Размещение Закрытого ключа корневого УЦ, и
- Принятие мер, необходимых для перехода фактических служб корневого УЦ к последующему корневому УЦ.

6 Технический контроль безопасности

Технический контроль безопасности определяется в соответствии с [ETSI TS 102042].

Подробная информация приведена в ЗПС.

6.1 Генерация и установка пары ключей

Подробная информация приведена в ЗПС.

6.2 Защита закрытого ключа и технические средства контроля криптографического модуля

Подробная информация приведена в ЗПС.

6.3 Другие аспекты управления парой ключей

Подробная информация приведена в ЗПС.

6.4 Данные активации

Подробная информация приведена в ЗПС.

6.5 Контроль компьютерной безопасности

Подробная информация приведена в ЗПС.

6.6 Контроль безопасности на протяжении жизненного цикла

Подробная информация приведена в ЗПС.

6.7 Контроль сетевой безопасности

Подробная информация приведена в ЗПС.

6.8 Процесс присвоения отметок времени

Подробная информация приведена в ЗПС.

7 Сертификат, профили CRL и OCSP

7.1 Профиль сертификата

Определения профиля сертификата для самого Выпускающего УЦ «Сименс» и выданных им сертификатов субъекта, а также требования к содержимому сертификата для выданных сертификатов соответствуют

- Рекомендациям ITU-T X.509 Версия 3, и
- RFC 5280
- ETSI EN 319 412-2

Подробная информация приведена в ЗПС.

7.2 Профиль CRL

Подробная информация приведена в ЗПС.

7.3 Профиль OCSP

Подробная информация приведена в ЗПС.

8 Аудит соответствия и другие оценки

Соблюдение УЦ «Сименс» требований настоящей ПС и ЗПС будет проверяться ежегодно. Кроме того, проводится ежегодная классификация активов служб ИОК и ее компонентов, которая выполняется в соответствии с процессом управления корпоративными рисками «Сименс». Эта классификация активов может привести к адаптации реализованных механизмов безопасности и средств контроля и к соответствующим изменениям в ПС и ЗПС.

8.1 Частота или обстоятельства оценки

УЦ «Сименс» проверяются и сертифицируются в соответствии с ETSI EN 319 411-1. Аудит проводится ежегодно. В дополнение к аудиту соответствия, УЦ «Сименс» может проводить или обеспечивать проведение других оценок для обеспечения надежности своих доверенных поставщиков услуг или участников ИОК, включая, без ограничений:

- УЦ «Сименс» может по своему собственному усмотрению в любое время провести оценку в отношении себя самого, ЦР или другого участника ИОК в случае, когда УЦ «Сименс» имеет основания полагать, что проверяемая организация не работала в соответствии с указанными политиками безопасности или процедурами, приведенными в документации ИОК.
- УЦ «Сименс» может проводить дополнительные оценки в отношении себя самого, ЦР или другого Участника ИОК после получения неполных или нетипичных результатов в ходе аудита соответствия или в рамках общего процесса управления рисками в ходе обычной деятельности.

8.2 Идентификационные данные / квалификация оценщика

Аудит соответствия выполняется внешним аудитором, который:

- ❑ демонстрирует профессионализм в технологиях ИОК, средствах и методах информационной безопасности, аудите безопасности и аттестации третьих сторон
- ❑ аккредитован признанной профессиональной организацией или ассоциацией, которая требует наличия определенных навыков, применяет меры обеспечения качества, такие как экспертная оценка, проверка компетентности, стандарты в отношении надлежащего назначения персонала для участия и требования к дополнительному профессиональному образованию

8.3 Отношения между оценщиком и оцениваемым лицом

Оценщик должен быть организационно независимым от оцениваемого лица в части осуществления деятельности и определения политик.

8.4 Оцениваемые вопросы

Область применения аудита соответствия или других оценок УЦ «Сименс» или других участников ИОК «Сименс» включают проверку проектной и эксплуатационная эффективности средств контроля оцениваемого лица за определенный период времени. Аудит или другая оценка должны проводиться с использованием соответствующих критериев, включающих управление средой, управление ключами и контроль жизненного цикла сертификата оцениваемого лица. Цель аудита или другой оценки заключается в оценке эффективности внедренных мер контроля и их соответствия определенной деловой практике, как указано в соответствующих политиках и процедурах безопасности.

8.5 Меры, предпринимаемые в результате обнаружения недостатков

Если в результате аудита соответствия или других оценок будут выявлены недостатки оцениваемого лица, то необходимо принять решение о мерах, которые необходимо предпринять. Это решение принимается РМА с помощью аудитора / оценщика. УЦ «Сименс» отвечает за разработку и реализацию плана корректирующих действий.

Если РМА определит, что такие недостатки представляют собой непосредственную угрозу безопасности или целостности ИОК «Сименс», план корректирующих действий должен быть разработан в течение тридцати (30) дней и реализован в коммерчески разумный период времени, а повторная оценка проводится в течение тридцати (30) дней после завершения корректирующих действий. Для менее серьезных недостатков УЦ «Сименс» оценивает важность таких проблем и определяет соответствующие меры реагирования.

Возможные действия указаны в [RFC3647]:

- ❑ временное приостановление операций до устранения недостатков
- ❑ отзыв сертификатов, выданных оцениваемому лицу
- ❑ изменения в персонале
- ❑ инициирование специальных расследований или более частые последующие оценки соблюдения, а также
- ❑ требования о возмещении убытков в отношении оцениваемого лица

8.6 Сообщение результатов

Сводные отчеты о результатах аудита соответствия публикуются вместе с сертификатом аудита.

8.7 Автоаудит

УЦ «Сименс» контролирует соблюдение своей Политики сертификации, Заявления о практике сертификации и BRG CA/B, а также строго контролирует качество своего обслуживания путем проведения автоаудитов не реже одного раза в квартал на случайной выборке из одного сертификата или как минимум трех процентов Сертификатов, в зависимости от того, что больше, выданных им в период, начинающийся сразу после отбора предыдущей выборки для автоаудита.

9 Прочие коммерческие и юридические вопросы

Прочие коммерческие и юридические вопросы в целом касаются следующего:

- сборы, взимаемые за услуги, связанные с УЦ (§ 9.1 ПС)
- финансовая ответственность Участников ИОК «Сименс» за:
  - (i) поддержание ресурсов для текущих операций, и
  - (ii) осуществление выплат по постановлениям, решениям или урегулированию в ответ на предъявленные им претензии, включая страхование гражданской ответственности (§9.2 ПС/ЗПС)
- юридические обязанности и распределение потенциальной ответственности и рисков среди участников ИОК (§9.3 - § 9.17 ПС/ЗПС)

9.1 Сборы

В отношении *Сообщества «Сименс»* взимаются сборы за услуги, связанные с сертификатами, и оплачиваются ответственным лицом «Сименс». В отношении *Сообщества делового партнера* взимаются сборы за услуги, связанные с сертификатами, и могут оплачиваться либо деловым партнером, либо спонсором из «Сименс», либо компанией «Сименс», осуществляющей или планирующей осуществлять бизнес с деловым партнером. В отношении *Сообщества сервера* взимаются сборы за услуги, связанные с сертификатами, и оплачиваются ответственным лицом «Сименс».

Во всех случаях договорное соглашение с УЦ «Сименс» является решающим в отношении сборов.

9.2 Финансовая ответственность

Если иное явно не оговорено или прямо не предусмотрено в ПС/ЗПС, утвержденных «Сименс» CIO, ответственность УЦ «Сименс» перед доверяющими сторонами и любыми другими организациями ограничивается в отношении любых претензий любого рода во всех случаях, разрешенных применимым законодательством, в том числе договорного характера, в пределах сертификата, независимо от количества транзакций, цифровых подписей или оснований для подачи претензии, вытекающих из такого сертификата или связанных с ним, или любых услуг, предоставляемых в отношении такого сертификата, и на совокупной основе.
С учетом вышеизложенных ограничений лимит ответственности УЦ «Сименс» в отношении доверяющих сторон и любых других юридических лиц на весь срок действия сертификата, выданного УЦ «Сименс» (например, 6 лет, если не отозван) по отношению ко всем лицам в отношении такого сертификата ограничивается суммой, определенной «Сименс» CIO, если иное не определено в применимом договорном соглашении.

9.3 Конфиденциальность коммерческой информации

9.3.1 Состав конфиденциальной информации

Вся информация, используемая или передаваемая в УЦ «Сименс», классифицируется в соответствии с Системой менеджмента информационной безопасности «Сименс».

Как минимум, следующая информация должна считаться конфиденциальной:

- ❑ Централизованно генерируемые ключи EE и данные активации, необходимые для использования таких закрытых ключей
- ❑ Транзакционные записи (как полные записи, так и контрольный журнал транзакций)
- ❑ Аудиторские записи, созданные или сохраненные УЦ «Сименс», ЦР или аудитором
- ❑ Планы действий в случае непредвиденных обстоятельств и аварийного восстановления
- ❑ Меры безопасности, контролирующие операции Корневого УЦ и аппаратное и программное обеспечение Выпускающего УЦ «Сименс», а также администрирование служб сертификации и назначенных служб регистрации
- ❑ Не обозначенная специально информация считается конфиденциальной, если она, очевидно, содержит коммерческую тайну или другую конфиденциальную информацию

9.3.2 Информация, не входящая в состав конфиденциальной информации

Информация в сертификатах, CRL и другая информация о статусе в хранилище не считается конфиденциальной.

9.3.3 Ответственность за защиту конфиденциальной информации

УЦ «Сименс» и соответствующие ЦР должны требовать от своих сотрудников или подрядчиков соблюдения

обязательств по сохранению конфиденциальности конфиденциальной информации в соответствии с §9.3.1 ПС. Субъекты должны соблюдать применимые части §9.3.1 ПС.

9.4 Конфиденциальность персональных данных

УЦ «Сименс» и соответствующие центры регистрации должны защищать «Персональные данные» заявителей на получение сертификата в соответствии с применимым законодательством и, если применимо, в соответствии с «Обязательными корпоративными правилами (ОКП) для компаний Группы «Сименс» и других присоединяющихся компаний по защите персональных данных», с Циркуляром № 216 («Обязательные корпоративные правила»).
УЦ «Сименс» и соответствующие ЦР должны соблюдать или обеспечивать соблюдение своими доверенными поставщиками услуг требований действующего национального законодательства о защите конфиденциальности данных при обработке персональных данных в заявке на сертификат или сертификате, включая законодательство государства-члена, реализующего Директиву Европейского Союза 95/46/EC о защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных [EU95/46/EC].
Анонимные, псевдонимные или другие неперсональные данные в заявках на сертификаты, сертификатах, CRL и другой информации о статусе в хранилище не считаются конфиденциальными в ИОК.
УЦ «Сименс» применяет подходящие организационные и технические меры по обеспечению информационной безопасности для защиты персональных данных заявителей на получение сертификата от неправильного использования или случайного или незаконного уничтожения, потери или изменения и несанкционированного раскрытия или доступа.

Персональные данные заявителей на получение сертификата или субъекта, которые необходимы для важных общественных интересов или для предъявления, осуществления или защиты исковых требований, могут быть переданы в соответствии с применимым законодательством о защите конфиденциальности данных. Стороне, которой передаются такие персональные данные, сообщается, что переданные персональные данные могут обрабатываться или использоваться только для той цели, для которой они были переданы.

УЦ «Сименс» требует от своих доверенных поставщиков услуг обеспечить, чтобы персональные данные соответствовали действительности и обновлялись по мере необходимости, чтобы были приняты соответствующие меры для исправления или удаления неточной или неполной информации, а также чтобы право заявителя на получение сертификата и субъекта на исправление, стирание, блокирование и предъявление возражений относительно информации соблюдались в соответствии с применимым законодательством о защите данных или корпоративными правилами.

9.5 Права интеллектуальной собственности

Распределение прав интеллектуальной собственности (например, авторского права, товарных знаков) на настоящую ПС, сертификаты и пары ключей среди участников ИОК «Сименс» (кроме субъектов и доверяющих сторон) регулируется применимыми соглашениями, которые всегда имеют преимущественную силу над настоящим §9.5. Для субъектов и доверяющих сторон распределение прав интеллектуальной собственности рассматривается ниже в разделе §9.5.1-9.5.4 ПС.

9.5.1 Права интеллектуальной собственности на сертификаты и информация об отзывах

Siemens AG сохраняет за собой все права интеллектуальной собственности на сертификаты и информацию об отзывах, выданные Корневым УЦ «Сименс» и соответствующими Выпускающими УЦ. Siemens AG предоставляет разрешение на воспроизведение и распространение сертификатов на неисключительной и безвозмездной основе в хранилище или иным образом при условии, что сертификаты будут воспроизводиться полностью, за исключением случаев, когда использование сертификатов иным образом регулируется применимым соглашением. Siemens AG может предоставить разрешение на использование информации об отзывах для выполнения функций доверяющей стороны по применимому соглашению, например, путем проверки CRL.

9.5.2 Права интеллектуальной собственности на ПС

Siemens AG сохраняет все права интеллектуальной собственности на настоящую ПС и связанные с ней основные документы по ИОК «Сименс».

9.5.3 Права интеллектуальной собственности на имена

Заявитель на получение сертификата сохраняет все права, которые он имеет (если применимо) на любой товарный знак или торговое название, содержащееся в любой заявке на сертификат и «имени субъекта» в любом сертификате, выданном такому заявителю на получение сертификата в качестве субъекта. УЦ «Сименс» не несет ответственности за разрешение споров среди конкурирующих претендентов на права интеллектуальной собственности на такие имена.

9.5.4 Права собственности владельцев сертификатов

Любая информация, полученная с помощью сертификатов УЦ, остается собственностью соответствующего владельца сертификата.

9.6 Заверения и гарантии

За исключением случаев, прямо указанных в соответствующем соглашении или эквивалентной документации, предоставленной в соответствии с трудовым законодательством и практикой, применимой к соответствующим участникам ИОК «Сименс», Siemens AG отказывается от любых

- ❑ заверений (которые обычно относятся к правильности высказывания или состоянию дел в прошлом и в настоящее время) и
- ❑ гарантий (которые обычно относятся к обеспечению правильности или обеспечению состояния дел в будущем), явных или подразумеваемых.

9.7 Отказ от гарантий

За исключением случаев, прямо указанных в соответствующем соглашении или эквивалентной документации, предоставленной в соответствии с трудовым законодательством и практикой, применимой к соответствующим участникам ИОК «Сименс», Корневой УЦ «Сименс» отказывается от всех заверений, гарантий (явных или подразумеваемых) и ответственности, за исключением случаев умышленного ненадлежащего поведения или грубой небрежности.

9.8 Ограничения ответственности

За исключением случаев, прямо указанных в соответствующем соглашении или эквивалентной документации, предоставленной в соответствии с трудовым законодательством и практикой, применимой к соответствующим участникам ИОК «Сименс», УЦ «Сименс» исключает возмещение Корневым УЦ «Сименс», Выпускающими УЦ «Сименс», доверенными поставщиками услуг или соответствующими ЦР или хранилищем ущерба, штрафных убытков, упущенной выгоды или дохода, потерю возможностей по использованию или производству во всех случаях, разрешенных применимым законодательством, за исключением случаев умышленного ненадлежащего поведения или грубой небрежности.

9.9 Гарантии возмещения ущерба

За исключением случаев, прямо указанных в соответствующем соглашении или эквивалентной документации, предоставленной в соответствии с трудовым законодательством и практикой, применимой к соответствующим участникам ИОК «Сименс», не существует обязательства, требующего от одного участника ИОК полностью отвечать за убытки или ущерб, понесенные этим участником ИОК в результате поведения другого участника ИОК в отношении третьих сторон, т. е. гарантия возмещения ущерба отсутствует.

9.10 Срок действия и прекращение

9.10.1 Срок действия

Срок действия настоящей ПС начинается с даты вступления в силу, указанную в §1.2 ПС, и продолжается до прекращения действия, как указано в §9.10.2 ПС.

9.10.2 Прекращение действия

Настоящая ПС прекращает действовать, если срок действия сертификатов Корневого УЦ или сертификатов Выпускающего УЦ истекает и не продлевается, или если иным образом необходимо прекратить ее действие по любой причине.

До прекращения оказания УЦ «Сименс» своих услуг должны быть выполнены, по крайней мере, следующие процедуры:

- УЦ «Сименс» сообщает о прекращении: всем подписчикам и другим лицам, с которыми УЦ «Сименс» имеет соглашения или другие формы установленных отношений, среди которых доверяющие стороны и УЦ «Сименс». Кроме того, эта информация должна быть предоставлена другим доверяющим сторонам
- УЦ «Сименс» прекращает все полномочия субподрядчиков действовать от имени УЦ «Сименс» при выполнении любых функций, связанных с процессом выдачи сертификатов
- УЦ «Сименс» должен предпринять необходимые меры для передачи обязательств по ведению информации о регистрации, информации о статусе отзыва и архивов журнала событий за соответствующий указанный период времени подписчику и доверяющей стороне
- УЦ «Сименс» должен уничтожить или отказаться от использования своих закрытых ключей

9.10.3 Последствия прекращения деятельности и сохранение функционала

До прекращения деятельности УЦ «Сименс» должен приложить все коммерчески разумные усилия для подготовки и реализации плана прекращения деятельности, указанного в §5.8 ПС, для устранения последствий

прекращения деятельности и сохранения функционала. Там, где это возможно, УЦ «Сименс» предпримет действия по передаче функционала, включая открытые ключи существующих клиентов, другому УЦ.

9.11 Индивидуальные уведомления и взаимодействие с участниками

Индивидуальные уведомления и сообщения должны отправляться по электронной почте, если иное не установлено в применимом соглашении.

9.12 Поправки

9.12.1 Процедура внесения поправок

В случае внесения поправок в ПС, процедуры внесения изменений могут включать:

- механизм предоставления уведомлений участникам ИОК «Сименс» о предлагаемых поправках
- период для предоставления комментариев; механизм, посредством которого комментарии принимаются, рассматриваются и включаются в документ, и
- механизм, посредством которого поправки становятся окончательными и действительными

9.12.2 Механизм предоставления уведомлений и срок

Внесение изменений или поправок в ПС/ЗПС ведет к составлению новой версии ПС/ЗПС.

Новая версия ПС/ЗПС будет опубликована после ее выпуска на следующем веб-сайте: https://www.siemens.com/pki/.

9.12.3 Обстоятельства, при которых идентификатор объекта (OID) должен быть изменен

Изменения, которые не будут существенным образом снижать уверенность в том, что ПС или ее реализация окажут и будут оцениваться Центром управления политиками (§ 1.5 ПС) как оказывающие незначительное влияние на приемлемость сертификатов, не требуют изменения идентификатора объекта (OID) ПС. Изменения, которые существенным образом изменяют приемлемость сертификатов для определенных целей, могут потребовать соответствующих изменений в идентификаторе объекта (OID) ПС.

9.13 Разрешение споров

Любые споры или требования, возникающие в результате или в связи с настоящей ПС или ЗПС или их предметом, подлежат окончательному разрешению следующим образом.

- Для *Сообщества «Сименс»* любые споры или требования, возникающие в результате или в связи с настоящей ПС или ЗПС или их предметом, подлежат окончательному разрешению в соответствии с любыми процедурами разрешения споров Группы «Сименс», Региона или Операционной компании, в которой работает субъект, или в соответствии с применимым соглашением.
- Для *Сообщества делового партнера* любые споры или требования, возникающие в результате или в связи с настоящей ПС или ЗПС или их предметом, подлежат окончательному разрешению в соответствии с процедурами разрешения споров применимого соглашения, заключенного между компанией «Сименс» и деловым партнером.

9.14 Применимое право

Материальное право, применимое к настоящей ПС или ее предмету, является следующим, за исключением норм коллизионного права.

- Для Сообщества «Сименс» настоящая ПС и ее предмет подлежат регулированию и толкованию в соответствии с законодательством Германии для всех участников ИОК.
- Для Сообщества делового партнера любой вопрос, связанный с настоящей ПС или ее предметом, подлежит регулированию и толкованию в соответствии с законодательством, согласованным в применимом соглашении между компанией «Сименс» и деловым партнером, и, если такое соглашение не заключено, в соответствии с законодательством Германии.

9.15 Соответствие действующим нормативным требованиям

Использование сертификатов «Сименс» всегда должно соответствовать применимому законодательству, особенно в части регулирования экспорта, импорта или использования аппаратного обеспечения, программного обеспечения или технологий шифрования.

9.16 Прочие положения

Приведенные ниже так называемые «типовые» положения, которые применяются к настоящей ПС или другим документам ИОК «Сименс», будут рассматриваться в применимых соглашениях.

9.16.1 Полнота соглашения

Не предусмотрено.

9.16.2 Уступка

Не предусмотрено.

9.16.3 Автономность положений

Не предусмотрено.

9.16.4 Обеспечение исполнения (гонорар адвокатов и отказ от прав)

Не предусмотрено.

9.16.5 Форс-мажор

Не предусмотрено.

9.17 Заключительные положения

9.17.1 Порядок приоритетности ПС

В случае возникновения противоречий между следующими документами, эти документы имеют преимущественную силу в следующем порядке:

1. Настоящая ПС
2. ЗПС Корневых УЦ
3. Документация, составленная или прямо одобренная УЦ «Сименс»
4. ЗПС Выпускающего УЦ
5. Любая другая политика, практика, процедура или планы ИОК «Сименс»

10 Справочные материалы

[CAB_Forum] Базовые требования к выпуску и управлению общедоступными доверенными сертификатами; Правила консорциума сертификационных центров и провайдеров интернет браузеров; http://www.cabforum.org

[ETSI TS 102042] Электронные подписи и инфраструктура (ESI); Требования к политике для центров сертификации, выдающих сертификаты открытых ключей (февраль 2013 г.)

[ISO27001] Информационные технологии - Методы обеспечения безопасности - Системы менеджмента информационной безопасности - Требования (март 2015 г.)

[RFC3647] Интернет X.509 Инфраструктура открытых ключей Политика сертификации и основы практики сертификации, Рабочая группа по сетям: С. Чохани, У. Форд, Р. Сабетт, К. Меррил, С. Ву (ноябрь 2003 г.).

[RFC5280] Интернет X.509 Инфраструктура открытых ключей, сертификат и список отзыва сертификатов (CRL), Рабочая группа по сетям: Р. Хусли, У. Полк, У. Форд, Д. Соло (май 2008 г.)

[TRUST_SITE] Безопасная инфраструктура для ИТ-систем, Trusted Site Infrastructure, TÜViT, 2016

11 Приложение A: Сокращения и определения

11.1 Определения

Деловой партнер	Физические или юридические лица, не являющиеся членами сообщества «Сименс», но имеющие договорные отношения с «Сименс». Примерами являются внешние консультанты, субподрядчики или поставщики компонентов.
Сертификат УЦ	Сертификат открытого ключа центра сертификации
Политика сертификации (ПС)	Сравните раздел 1.1
Удостоверяющий центр (УЦ)	Центр, имеющий право на сертификацию открытых ключей; сравните главу 1.3.1.
Перекрестный сертификат	Сертификат, используемый для подтверждения доверительных отношений между двумя УЦ
Служба каталогов	ИОК-служба для онлайн-доступа к сертификатам и CRL; обычно реализуемая через облегченный протокол доступа к каталогам (LDAP)
Уникальное имя	Последовательность полей данных, описывающих эмитента УЦ и / или субъекта уникальным образом. Формат Уникального имени определен в стандарте [X.501].
Сертификат EE	См. «Сертификат конечного пользователя»
Конечный пользователь	Эквивалент субъекту; идентификационные данные конечного пользователя подключаются к сертификату и связанной с ним паре ключей. См. также главу 1.3.3
Сертификат конечного пользователя	Сертификат, который не должен использоваться для сертификации и выдачи CRL или других сертификатов.
Сертификат пользователя	Сертификат, который не может использоваться для сертификации и выдачи других сертификатов или CRL
Функциональная группа	Группа функций представляет собой неличную функцию, например, почтовый ящик с особым назначением, почтовый ящик группы, службу поддержки. Несколько лиц могут иметь доступ к функциональной группе.
Центр управления политиками	Орган Siemens AG, отвечающий за установление, внедрение и администрирование решений в отношении настоящей ПС и соответствующих документов и соглашений в ИОК «Сименс»
Центр регистрации (ЦР)	Встроенное в ИОК средство для аутентификации участников. См. также главу 1.3.2
Доверяющие стороны	Физическое или юридическое лицо, использующее сертификаты; см. также главу 1.3.5.
Защищенное устройство	Компонент (например, смарт-карта), подходящий для защиты закрытого ключа, хранящегося на этом устройстве. Все криптографические операции с использованием закрытого ключа выполняются внутри этого защищенного устройства.
Удостоверяющий центр «Сименс»	Внутренняя организация «Сименс», которая выпускает и управляет сертификатами. Эта организация управляет Корневыми УЦ «Сименс», а также Выпускающими УЦ «Сименс».
Сообщество «Сименс»	Лица, являющиеся членами сообщества «Сименс», которые могут запросить сертификат «Сименс». Примерами являются сотрудники или администраторы.
Выпускающий УЦ «Сименс»	Технические компоненты (аппаратное и программное обеспечение), которые подписывают сертификаты пользователей и связанную с ними информацию, такую как списки отзыва или сертификаты подписантов OCSP.
Корневой УЦ «Сименс»	Технические компоненты (аппаратное и программное обеспечение), которые подписывают сертификаты Выпускающих УЦ «Сименс» и связанную с ними информацию, такую как списки отзыва или сертификаты подписантов OCSP.
Смарт-карта	Интеллектуальная карточка, оснащенная микропроцессором, который может использоваться для генерации цифровых подписей и для других приложений ИОК
Субъект	Конечный пользователь, который использует закрытый ключ конечного пользователя (EE-ключ). Конечный пользователь может отличаться от подписчика.

Подписант	Подписантом всех сертификатов, выданных ИОК «Сименс», является «Сименс» как юридическое лицо. В течение срока действия сертификата «Сименс» делегирует права назначенным лицам или отделам. Например, когда сотрудник запрашивает сертификат EE, «Сименс» делегирует этому сотруднику право выступать в качестве подписантаа. То же самое относится к сертификатам делового партнера. В этом случае «Сименс» делегирует право деловому партнеру запрашивать сертификат. См. также главу 1.3.3
Токен	Среда передачи для сертификатов и ключей
Доверенный оператор	УЦ «Сименс» несет общую ответственность за выдачу сертификатов субъектам, а также за управление и отзыв сертификатов. УЦ «Сименс» может делегировать часть или все эти функции при осуществлении своей общей ответственности ЦР или другим внутренним поставщикам услуг «Сименс», которые называются Доверенными операторами

11.2 Сокращения

BRG	Руководство по базовым требованиям
УЦ	Удостоверяющий Центр
CAB	Консорциум сертификационных центров и провайдеров интернет браузеров (CA/B Форум))
CISO	Руководитель по информационной безопасности
CN	Стандартное имя
ПС	Политика сертификации
ЗПС	Заявление о практике сертификации
CRL	Список отзыва сертификатов
DN	Уникальное имя
DVCP	Политика проверки сертификата домена
EE	Конечный пользователь
FG	Функциональная группа
FIPS	Федеральный стандарт обработки информации
FQDN	Полноценное доменное имя
HSM	Аппаратный модуль безопасности
ISO	Международная организация по стандартизации
СМИБ (ISMS)	Система управления информационной безопасностью
LCP	Облегченная политика сертификации
LDAP	Облегченный протокол доступа к каталогам
NetSec-CAB	Требования к сетевой безопасности - CA/B Форум
NCP	Стандартизированная политика сертификации
NCP+	Стандартизированная политика сертификации, требующая безопасного пользовательского устройства
OCSP	Протокол проверки статуса сертификата онлайн
OID	Идентификатор объекта
OVCP	Политика сертификации с проверкой организации
ПИН	Персональный идентификационный номер
ИОК	Инфраструктура открытых ключей
PMA	Центр управления политиками
PUK	Персональный ключ разблокировки
ЦР (RA)	Центр регистрации
RFC	Запрос комментариев
PSE	Средства личной безопасности
SSCD	Устройство создания защищенной подписи
SUD	Защищенное пользовательское устройство
URL	Унифицированный локатор ресурса
UTF8	Формат преобразования Юникода, 8-битный