Заявление о практике сертификации

Корневые удостоверяющие центры «Сименс»

История изменений документа

Версия	Дата	Автор	Комментарий к изменению
1.0	10 июня 2016 г.	Александр Виннен, Михаэль Мунцерт	Первый окончательный вариант
1.1	1 декабря 2016 г.	Руфус Бушарт	Незначительно обновленная версия
1.2	29 мая 2017 г.	Руфус Бушарт	Обновлена новая иерархия ЦС

Настоящий документ пересматривается каждый год или в случае внесения важных специальных изменений в соответствии с процессом обновления документов Отдела информационной безопасности. Каждая новая версия перед выпуском утверждается на соответствующем уровне управления.

Настоящий документ опубликован на веб-сайте www.siemens.ru/digital-id.

Область применения

Настоящий документ представляет собой Заявление о практике сертификации (ЗПС) для Корневых удостоверяющих центров «Сименс» (Корневых УЦ). Целью настоящего документа является публичное раскрытие подписчикам и доверяющим сторонам политик и методов ведения деятельности, в соответствии с которыми работает данный Корневой удостоверяющий центр.

Статус документа

Настоящий документ с версией 1.0 и статусом «Выпущен» был классифицирован как «Без ограничений».

	Название	**Отдел**	**Дата**
Автор	Различные авторы, подробная информация в истории изменений документа		
Проверил:	Тобиас Ланге Руфус Бушарт	Siemens LS Siemens GS IT HR 7 4	10 июня 2016 г. 14 июня 2017 г.
Утвердил:	Маркус Вихманн	Siemens GS IT ISEC	14 июня 2017 г.

Настоящее Заявление о практике сертификации (ЗПС) было утверждено ответственным за информационную безопасность «Сименс» 14 июня 2017 года.

Содержание

1 Введение

Структура настоящего документа соответствует рекомендациям RFC 3647 «Интернет X.509 Инфраструктура открытого ключа: Политика сертификации и основы практики сертификации» (ноябрь 2003 г.) [RFC3647].

1.1 Обзор

Настоящее Заявление о практике сертификации (ЗПС) определяет:

- меры и процедуры в контексте Служб сертификации, выполняемых Корневым ЦС «Сименс»;
- минимальные требования, предъявляемые ко всем участникам ИОК.

Заявление о практике сертификации подробно описывает имеющиеся процедуры и средства контроля для соответствия требованиям Политики сертификации. В отношении аналогичных вопросов смотрите соответствующую главу Политики сертификации (ПС).

На следующем рисунке показаны Корневые УЦ «Сименс» вместе с соответствующими Выпускающими УЦ:

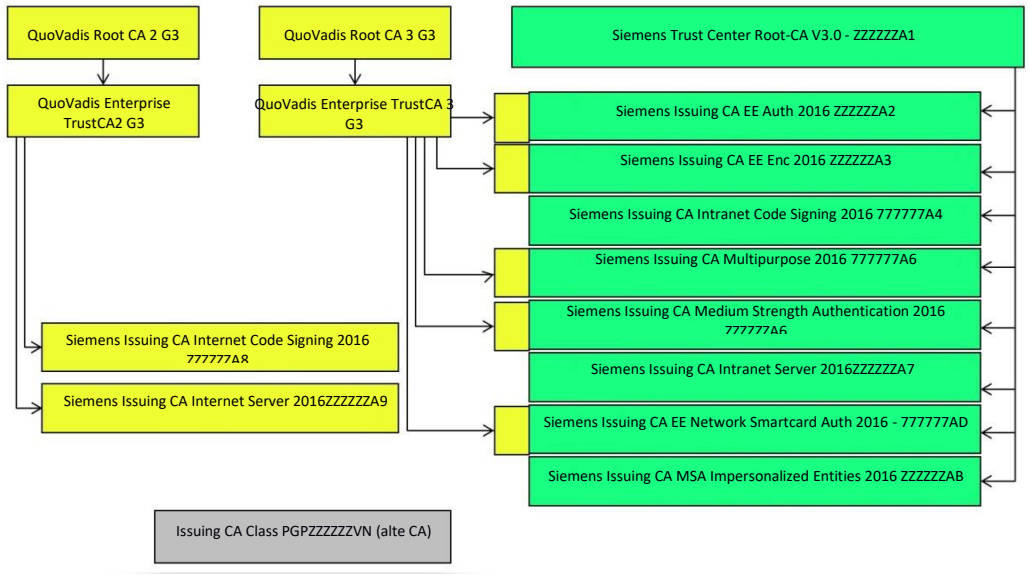

Рисунок 1: Иерархия ЦС «Сименс» по состоянию на июнь 2016 года

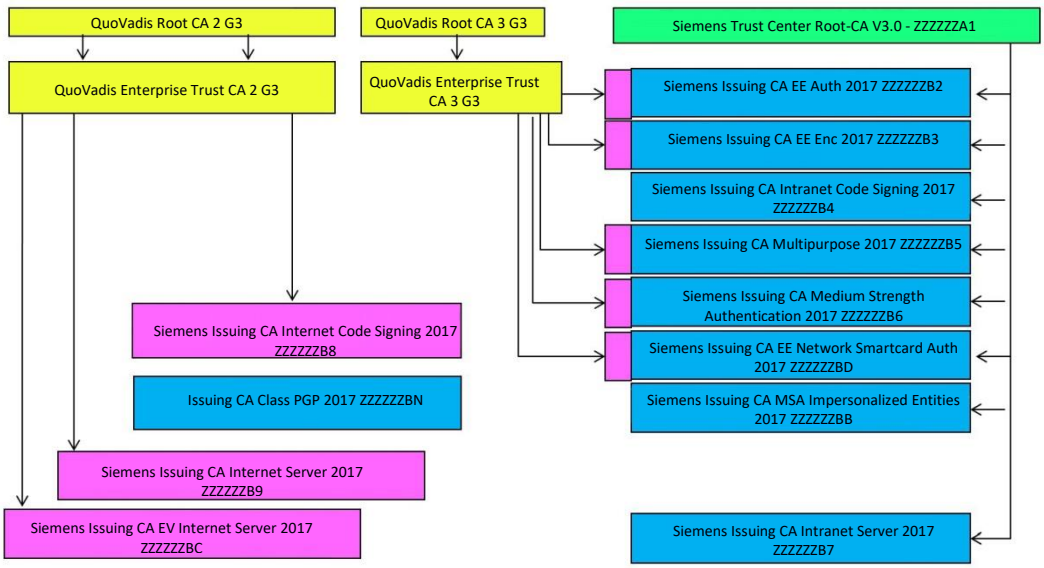

Рисунок 2: Иерархия УЦ«Сименс» по состоянию на 01 октября 2017 г.

В следующей таблице перечислены действующие в настоящее время Корневые УЦ, а также реализуемые ими требования в соответствии с [ETSI 102 042]:

ЦС	Требования		
	NCP+	OVCP	DVCP
ZZZZZZV0 Siemens Internet CA V1.0	X	-	-
ZZZZZZV1 Siemens Trust Center Root-CA V2.0	X	-	-
ZZZZZZA1 Siemens Trust Center Root-CA V3.0	X	-	-

Таблица 1: Внедрение требований ETSI Корневым ЦС

1.2 Название и идентификационное обозначение документа

ЗПС означает «Заявление о практике сертификации».

Наименование: Заявление о практике сертификации корневых УЦ«Сименс»

OID:1.3.6.1.4.1.4329.99.2.1.1.1.0

Дата истечения срока: Настоящая версия документа является самой последней, пока не будет опубликована следующая версия.

1.3 Участники ИОК

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

1.3.1 Центры сертификации

Указано в Регламенте УЦ

1.3.2 Центры регистрации

Указано в Регламенте УЦ.

1.3.3 Подписанты

Указано в Регламенте УЦ.

1.3.4 Доверяющие стороны

Указано в Регламенте УЦ.

1.3.5 Другие участники

Указано в Регламенте УЦ.

1.4 Использование сертификата

1.4.1 Надлежащее использование сертификата

Указано в Регламенте УЦ.

1.4.2 Запрещенное использование сертификата

Указано в Регламенте УЦ.

1.5 Управление политикой

1.5.1 Организация, управляющая документом

Указано в Регламенте УЦ.

1.5.2 Контактное лицо

Указано в Регламенте УЦ.

2 Обязанности по публикации и хранению

2.1 Хранилища

Указано в Регламенте УЦ.

2.2 Публикация информации о сертификации

Указано в Регламенте УЦ.

2.3 Время или периодичность публикации

Указано в Регламенте УЦ.

2.4 Контроль доступа в хранилищах

Указано в Регламенте УЦ.

3 Идентификация и аутентификация

3.1 Присвоение имени

3.1.1 Типы имен

Указано в Регламенте УЦ.

3.1.2 Информативность имен

Указано в Регламенте УЦ.

3.1.3 Анонимность или псевдоним подписчиков

Указано в Регламенте УЦ.

3.1.4 Правила интерпретации различных форм имени

Указано в Регламенте УЦ.

3.1.5 Уникальность имен

Указано в Регламенте УЦ.

3.1.6 Признание, аутентификация и роли товарных знаков

Указано в Регламенте УЦ.

3.2 Первоначальная проверка личности

3.2.1 Метод подтверждения наличия закрытого ключа

Указано в Регламенте УЦ.

3.2.2 Идентификация и аутентификация организации

Указано в Регламенте УЦ.

3.2.3 Идентификация и аутентификация физического лица

Указано в Регламенте УЦ.

3.2.4 Неподтвержденная информация о подписчиках

Указано в Регламенте УЦ.

3.2.5 Проверка центра

Указано в Регламенте УЦ.

3.2.6 Критерии взаимодействия между

Указано в Регламенте УЦ.

3.3 Идентификация и аутентификация запросов повторного ключа

Указано в Регламенте УЦ.

3.4 Идентификация и аутентификация запросов на отзыв

Указано в Регламенте УЦ.

4 Требования к использованию сертификата на протяжении жизненного цикла

4.1 Заявка на сертификат

4.1.1 Кто может подать заявку на сертификат?

Указано в Регламенте УЦ.

4.1.2 Процесс регистрации и обязанности

Указано в Регламенте УЦ.

4.2 Обработка заявок на сертификаты

4.2.1 Выполнение функций идентификации и аутентификации

Указано в Регламенте УЦ.

4.2.2 Утверждение или отклонение заявок на сертификаты

Указано в Регламенте УЦ

4.2.3 Время обработки заявок на сертификаты

Указано в Регламенте УЦ.

4.3 Выдача сертификата

4.3.1 Действия Корневого УЦ во время выдачи сертификата

Указано в Регламенте УЦ.

4.3.2 Уведомление подписчика УЦ о выдаче сертификата

Указано в Регламенте УЦ.

4.4 Принятие сертификата

4.4.1 Поведение, подтверждающее принятие сертификата

Указано в Регламенте УЦ.

4.4.2 Публикация сертификата УЦ

Указано в Регламенте УЦ.

4.4.3 Уведомление УЦ о выдаче сертификата другим организациям

Указано в Регламенте УЦ.

4.5 Пара ключей и использование сертификата

4.5.1 Закрытый ключ субъекта и использование сертификата

Указано в Регламенте УЦ.

4.5.2 Открытый ключ доверяющей стороны и использование сертификата

Указано в Регламенте УЦ.

4.6 Продление сертификата

Указано в Регламенте УЦ.

4.6.1 Обстоятельства для продления сертификата

Указано в Регламенте УЦ.

4.6.2 Кто может запросить продление?

Указано в Регламенте УЦ.

4.6.3 Обработка запроса на продление сертификата

Указано в Регламенте УЦ.

4.6.4 Уведомление о выдаче нового сертификата субъекту

Указано в Регламенте УЦ.

4.6.5 Поведение, подтверждающее принятие продленного сертификата

Указано в Регламенте УЦ.

4.6.6 Публикация продленного сертификата УЦ

Указано в Регламенте УЦ.

4.6.7 Уведомление УЦ о выдаче сертификата другим организациям

Указано в Регламенте УЦ.

4.7 Сертификат с повторным ключом

Указано в Регламенте УЦ.

4.7.1 Обстоятельства для выдачи сертификатов с повторным ключом

Указано в Регламенте УЦ.

4.7.2 Кто может запросить сертификацию нового открытого ключа?

Указано в Регламенте УЦ.

4.7.3 Обработка запроса на выдачу сертификата с повторным ключом

Указано в Регламенте УЦ.

4.7.4 Уведомление о выдаче нового сертификата подписчику

Указано в Регламенте УЦ.

4.7.5 Поведение, подтверждающее принятие сертификата с повторным ключом

Указано в Регламенте УЦ.

4.7.6 Публикация сертификата с повторным ключом УЦ

Указано в Регламенте УЦ.

4.7.7 Уведомление УЦ о выдаче сертификата другим организациям

Указано в Регламенте УЦ.

4.8 Изменение сертификата

4.8.1 Обстоятельства для изменения сертификата

Указано в Регламенте УЦ.

4.8.2 Кто может запросить изменение сертификата?

Указано в Регламенте УЦ.

4.8.3 Обработка запросов на изменение сертификата

Указано в Регламенте УЦ.

4.8.4 Уведомление о выдаче нового сертификата субъекту

Указано в Регламенте УЦ.

4.8.5 Поведение, подтверждающее принятие измененного сертификата

Указано в Регламенте УЦ.

4.8.6 Публикация измененного сертификата УЦ

Указано в Регламенте УЦ.

4.8.7 Уведомление УЦ о выдаче сертификата другим организациям

Указано в Регламенте УЦ.

4.9 Отзыв и приостановка сертификата

4.9.1 Обстоятельства для отзыва

Указано в Регламенте УЦ.

4.9.2 Кто может запросить отзыв?

Указано в Регламенте УЦ.

4.9.3 Процедура подачи запроса на отзыв

Указано в Регламенте УЦ.

4.9.4 Период отсрочки для подачи запроса на отзыв

Указано в Регламенте УЦ.

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

Указано в Регламенте УЦ.

4.9.6 Требование к проверке отзыва для доверяющих сторон

Указано в Регламенте УЦ.

4.9.7 Частота выпуска списков отзыва сертификатов (CRL)

Указано в Регламенте УЦ.

4.9.8 Максимальное время ожидания для списков отзыва сертификатов (CRL)

Указано в Регламенте УЦ.

4.9.9 Возможность проверить статус отзыва в режиме онлайн

Указано в Регламенте УЦ.

4.9.10 Другие доступные формы сообщений об отзыве

Указано в Регламенте УЦ.

4.9.11 Специальные требования к компрометации закрытого ключа

Указано в Регламенте УЦ.

4.9.12 Обстоятельства для приостановки

Указано в Регламенте УЦ.

4.10 Службы проверки статуса сертификатов

4.10.1 Эксплуатационные характеристики

Указано в Регламенте УЦ.

4.10.2 Доступность службы

Указано в Регламенте УЦ.

4.10.3 Дополнительные характеристики

Указано в Регламенте УЦ.

4.11 Окончание подписки

Указано в Регламенте УЦ.

4.12 Депонирование и восстановление ключей

Указано в Регламенте УЦ.

5 Управление, операционный и физический контроль

Управление, операционный и физический контроль определены в соответствии с [ETSI-F].

Надежные системы и продукты УЦ «Сименс» защищены от несанкционированного изменения для обеспечения технической и криптографической безопасности поддерживаемого ими процесса.

УЦ «Сименс» работает в соответствии с Системой менеджмента информационной безопасности («СМИБ») «Сименс», которая поддерживает требования безопасности настоящего ЗПС. СМИБ основана на ISO27001. Ниже приведен обзор требований безопасности для Корневого УЦ «Сименс».

5.1 Контроль физической безопасности

5.1.1 Расположение и строительство объекта

Объект сертифицирован в соответствии с TÜV Trusted Site Infrastructure Level 4.

5.1.2 Физический доступ

Объект сертифицирован в соответствии с TÜV Trusted Site Infrastructure Level 4.

5.1.3 Электроснабжение и кондиционирование воздуха

Объект сертифицирован в соответствии с TÜV Trusted Site Infrastructure Level 4.

5.1.4 Водоснабжение

Объект сертифицирован в соответствии с TÜV Trusted Site Infrastructure Level 4.

5.1.5 Противопожарная защита

Объект сертифицирован в соответствии с TÜV Trusted Site Infrastructure Level 4.

5.1.6 Средства хранения данных

Все носители, содержащие производственное программное обеспечение и данные, а также данные аудита, архивов или резервные копии, хранятся в специально защищенных хранилищах в нескольких местах или в безопасном внешнем хранилище с соответствующими физическими и логическими средствами контроля доступа, предназначенными для ограничения доступа в пределах уполномоченного персонала и защиты таких носителей от случайного повреждения (например, от воды, огня и электромагнитного излучения).

5.1.7 Утилизация отходов

Конфиденциальные документы и материалы измельчаются перед утилизацией в соответствии с DIN66933. Носители, используемые для сбора или передачи конфиденциальной информации, делаются нечитаемыми перед утилизацией. Криптографические устройства физически уничтожаются или обнуляются перед утилизацией в соответствии с инструкциями производителей.

5.1.8 Внешнее резервное копирование

Выполняется регламентное резервное копирование критических системных данных, данных журнала аудита и другой конфиденциальной информации. Физическая безопасность внешних резервных

носителей при хранении обеспечивается с помощью средств аварийного восстановления «Сименс».

5.2 Контроль процедур

5.2.1 Доверенные роли

Доверенные роли для работы с Корневым УЦ «Сименс» включают всех сотрудников, которые имеют доступ или выполнят внутренние операции Корневого УЦ, которые могут существенно повлиять на:

- ❑ проверку правильности информации в заявках на сертификаты;
- ❑ принятие, отклонение или иную обработку заявок на сертификаты, повторных ключей, запросов на отзыв или информации о регистрации;
- ❑ выдачу или отзыв сертификатов, включая доступ к частям хранилища ограниченного пользования.

Персонал, выполняющий доверенные роли при работе с Корневым ЦС, включает, среди прочего Доверенные роли, определенные в ETSI TS 102 042 V2.4.1 (2013-02):

- ❑ Ответственные за безопасность
- ❑ Системные администраторы
- ❑ Системные операторы
- ❑ Системные аудиторы

Дополнительные доверенные роли в УЦ «Сименс»:

- ❑ Ответственный за защиту данных
- ❑ Ответственный за корпоративную информационную безопасность (CISO)

5.2.2 Количество лиц, необходимое для выполнения одной задачи

Установление и поддержание строгих процедур контроля обеспечивает разделение должностных обязанностей на основе ответственности за работу. Важные задачи должны выполняться несколькими доверенными лицами.
Следующие действия требуют, чтобы не менее двух доверенных сотрудников имели физический или логический доступ к устройству или месту:

- ❑ Доступ к объектам повышенной безопасности.
- ❑ Логический и физический доступ к аппаратным модулям безопасности (HSM).
- ❑ Физический доступ к архиву данных.
- ❑ Логический доступ к центральным, важным или критическим системам Корневого УЦ«Сименс» и системам резервного копирования.

5.2.3 Идентификация и аутентификация для каждой роли

Идентификация и аутентификация лиц в областях, связанных с безопасностью, осуществляется с помощью двухфакторной аутентификации. Доступ к критическим системам контролируется смарт-картами. В системах контроля авторизация пользователей управляется ролями.
Средства контроля внедрены для защиты оборудования, информации, носителей и программного обеспечения, связанных с операциями УЦ, от несанкционированного выноса за пределы объекта.

5.2.4 Роли, требующие разделения обязанностей

Любая доверенная роль для операций УЦ «Сименс» требует присутствия и участия, как минимум, двух доверенных сотрудников. Поэтому нет необходимости в разделении обязанностей в рамках одной роли.

5.3 Контроль безопасности персонала

5.3.1 Требования к квалификации, опыту и наличию разрешений

Лица, желающие получить доверенные роли, должны предоставить доказательства наличия необходимых знаний, квалификации и опыта, требующихся для успешного выполнения потенциальных должностных обязанностей, а также доказательства наличия разрешений, выданных государственными органами, если таковые имеются, необходимых для выполнения услуг сертификации по государственным контрактам.

5.3.2 Процедуры специальной проверки сведений

Проверка правильности предоставленных сведений в отношении всех кандидатов на работу

(подрядчиков и внешних пользователей) осуществляется в соответствии с применимыми законами, нормативными актами и этикой и соразмерно требованиям бизнеса, классификации информации, к которой предоставляется доступ, и предполагаемым рискам. Полицейские проверки на наличие судимости, фактов уголовного преследования, прекращения уголовного преследования или эквивалентные проверки повторяются через регулярные промежутки времени.

Все сотрудники, которые не пройдут первоначальное или периодическое расследование, не будут выполнять или продолжать выполнять доверенную роль.

5.3.3 Требования к обучению

Весь персонал, выполняющий управленческие обязанности в отношении работы УЦ «Сименс», должен пройти всестороннее обучение по следующим вопросам:

- ❑ принципы и механизмы обеспечения безопасности;
- ❑ знание требований мер безопасности;
- ❑ все используемые версии программного обеспечения;
- ❑ все обязанности, которые они должны выполнять;
- ❑ аварийное восстановление и процедуры обеспечения непрерывности бизнеса.

5.3.4 Частота и требования к переподготовке

Персонал, выполняющий доверенные роли, должен проходить повторное обучение и курсы повышения квалификации в объеме и с частотой, требуемыми для обеспечения необходимого уровня квалификации для успешного выполнения своих должностных обязанностей. Обучение по безопасности данных и защите конфиденциальности данных предоставляется на постоянной основе.

5.3.5 Частота и последовательность ротации должностей

Не предусмотрено.

5.3.6 Санкции за несанкционированные действия

Надлежащие дисциплинарные меры могут приниматься за несанкционированные действия или другие нарушения политики и процедур обеспечения безопасности информации и защиты конфиденциальности данных и могут быть соразмерными частоте и серьезности несанкционированных действий. Принимаемые дисциплинарные меры включают меры вплоть до прекращения.

5.3.7 Требования к независимым подрядчикам

Независимые подрядчики, внешние консультанты или стажеры не должны привлекаться для выполнения доверенных ролей в УЦ «Сименс».

Если необходимо сотрудничество с независимыми подрядчиками, консультантами или стажерами, им разрешается иметь доступ к защищенным объектам только в сопровождении и под непосредственным контролем уполномоченного персонала, выполняющего доверенные роли.

5.3.8 Документы, предоставленные персоналу

Персоналу, выполняющему доверенные роли, предоставляется «Корпоративное руководство по безопасности информации» Siemens AG и другая документация, которая является обязательной для всего персонала, выполняющего доверенные роли.

Эта информация необходима сотрудникам для надлежащего выполнения своих должностных обязанностей.

5.4 Процедуры ведения журнала аудита

Целью ведения журнала является постоянная проверка изменений параметров, изменений конфигурации и т. д. для компонентов систем Корневого УЦ. В процессах ведения журнала основное внимание уделяется следующему:

- ❑ Любые действия, осуществляемые с административными компонентами;
- ❑ Любое вмешательство в приложения: Веб-сервер, База данных, Аутентификация, Центр сертификации.

Собранные данные анализируются автоматически.

5.4.1 Типы регистрируемых событий

Записываются следующие типы данных, которые включают информацию о событиях, связанных с

функционированием Корневого УЦ:

- Данные мониторинга
  Данные представляют собой текущий обзор операций Корневого УЦ и включают информацию о состоянии системы, попытках проникновения и текущих предупреждениях.
- Данные регистрации
  Эти данные отслеживают доступ к защищенным объектам Корневого УЦ, а также вход и выход из дополнительных защищенных помещений (например, резервные объекты). Доступ к компьютерным системам отслеживается в файлах системных журналов.
- Данные аудита
  Операции Корневого УЦ записываются в аудиторской документации по событиям: Данные аудита соответствующих событий на протяжении жизненного цикла сертификата генерируются при выдаче, передаче и отзыве сертификатов и материалов по связанным с ними ключам. Данные аудита собираются и хранятся в течение более длительного периода времени, чем данные мониторинга. Кроме того, документируются изменения в аппаратных и / или программных компонентах. Документация регулярно проверяется в рамках процедур аудита соответствия.

5.4.2 Частота обработки данных журнала аудита

Данные журнала аудита должны контролироваться Центром управления политиками (PMA) после всех событий УЦ.

5.4.3 Период хранения данных журнала аудита

Журналы аудита хранятся на объекте неограниченный срок.

5.4.4 Защита журналов аудита

Журналы аудита защищены электронной системой ведения журналов аудита, которая включает механизмы защиты файлов журнала от несанкционированного просмотра, изменения, удаления или других вмешательств. Вводимые вручную данные аудита должны быть защищены от несанкционированного просмотра, изменения и уничтожения.

5.4.5 Процедуры резервного копирования данных журнала аудита

Полное резервное копирование выполняется после каждой Процедуры УЦ. После этого система переводится в автономный режим.

5.4.6 Система сбора информации для мониторинга (внутренняя или внешняя)

Сбор и хранение данных журнала аудита и технического состояния осуществляется в безопасных объектах.

5.4.7 Уведомление субъекта, инициирующего событие

Если лицо или устройство под контролем лица инициирует событие аудита, что приводит к предоставлению предупреждения об опасности или создает другую ненадлежащую запись в журнале аудита или обнаруживается иным образом, первоначальные меры реагирования заключаются в том, чтобы предотвратить дальнейшее вмешательство такого лица или устройства.

Событие аудита анализируется с тем, чтобы как можно скорее идентифицировать вторгшееся лицо или устройство. Этот анализ включает тщательный анализ всех соответствующих событий аудита. Принимаются меры в соответствии с Процессами управления инцидентами «Сименс».

5.4.8 Оценки уязвимостей

В рамках регулярных внутренних оценок безопасности «Сименс» проверяется потенциальная уязвимость УЦ «Сименс». Кроме того, текущий статус уязвимости документируется с помощью оценки рисков, результаты которой оформляются и обрабатываются в соответствии с Правилами СМИБ.

5.5 Архив записей

5.5.1 Типы архивируемых записей

Типы архивируемых записей включают категории данных журнала аудита, перечисленные ниже:

- Данные журнала технического состояния
  Данные журнала технического состояния используются для событий мониторинга рабочего состояния и служат основой для корректирующих действий. Данные журнала

технического состояния генерируются автоматически в электронном виде системными функциям ЦС, а также хранятся и архивируются автоматически;

- ❑ Данные аудита
  Данные аудита генерируются автоматически или вручную, используются для событий доступа и невозможности отказа и требуются УЦ «Сименс» для коммерческих, юридических или организационных целей.

  - Данные автоматического аудита включают аудиторскую, биллинговую и статистическую информацию
    Аудиторская информация подтверждает события, показывая, были ли выполнены действия в соответствии с согласованными процедурами, и в какой мере выполняются и завершаются идентифицируемые задачи;
  - Биллинговая информация служит основой для взимания платы за услуги, оказываемые в соответствии с соглашением(-ами) об уровне обслуживания («SLA»), а также предоставляет количественную информацию о доходах;
  - Статистическая информация показывает, выполняются ли требования SLA, а также предоставляет данные для количественного и профилактического анализа системы.
  - Данные ручного аудита состоят из информации о процедуре, которая хранится в рукописной форме в качестве оригинала и подписывается, если это необходимо для целей подтверждения. Такие данные включают в себя записи журналов, разрешающие документы, инструкции по обновлению и т. д.

5.5.2 Период хранения архивируемых данных журнала аудита

Срок хранения данных журнала технического состояния составляет не менее шести недель. Срок хранения данных автоматического аудита составляет не менее десяти лет с учетом различных контрактных требований и уточнения, что статистическая информация хранится не менее одного года. Данные ручного аудита хранятся не менее десяти лет.

5.5.3 Защита архивируемых данных журнала аудита

Защита архивируемых записей осуществляется в соответствии с СМИБ «Сименс». Архивируемых записи находятся в нескольких местах. Инфраструктура безопасности в этих местах и специальный мониторинг объектов резервного копирования и архивируемых записей включают в себя различные методы защиты от краж или несанкционированного уничтожения, изменения или потери, которые подробно изложены в Правилах СМИБ.

5.5.4 Процедуры архивирования резервных копий

Процедуры архивирования резервных копий реализуются в соответствии с Правилами СМИБ. Для данных журнала технического состояния и данных автоматического аудита выполняется ежедневное добавочное резервное копирование и еженедельное полное резервное копирование. Данные ручного аудита хранятся всегда после их генерации. Перед обновлением системы выполняется полное резервное копирование всех данных журнала технического состояния и данных автоматического аудита и соответствующего программного обеспечения.

5.5.5 Требования к присвоению отметок времени записям

Не предусмотрено.

5.5.6 Система сбора архивированных данных (внутренняя или внешняя)

Не предусмотрено.

5.5.7 Процедуры получения и проверки архивируемых данных

Процедуры получения и проверки сохраненных записей осуществляются в соответствии с Правилами СМИБ. Автоматизированные процедуры сохранения включают этапы контроля, подтверждающие, что доступ к хранящимся данным журнала аудита может быть получен впоследствии, и такие данные могут быть снова прочитаны.

5.6 Смена ключа

Срок действия ключей истекают одновременно со сроком действия соответствующих сертификатов. Смена ключа должна осуществляться до истечения срока действия соответствующих сертификатов (Дата прекращения выдачи) и должна выполняться вручную.

ЦС	Срок действия	Период функционирования (Дата прекращения выдачи)
Корневые удостоверяющие центры «Сименс»	12 лет	6 лет

В Дату прекращения выдачи **УЦ** «Сименс» прекращает выдавать сертификаты со старым ключом и инициирует создание новых ключей. Публикуется новый сертификат нового открытого ключа. Запросы на выдачу сертификата, полученные после Даты прекращения выдачи, выписываются с новым закрытым ключом ЦС.

5.7 Компрометация и аварийное восстановление

5.7.1 Процедуры обработки инцидентов и случаев компрометации

При возникновении инцидентов и случаев компрометации при работе УЦ создается группа по чрезвычайным ситуациям в соответствии с Правилами СМИБ. Группа по чрезвычайным ситуациям собирает информацию, оценивает риски, разрабатывает процедуру, предлагает и реализует данную процедуру с согласия Ответственного за корпоративную информационную безопасность «Сименс». Решение о том, какая процедура является наиболее уместной, принимается на основании последствий конкретного инцидента или компрометации и любого последующего распределения ответственности между Участниками ИОК в соответствии с законодательством или контрактом.

5.7.2 Повреждение вычислительных ресурсов, программного обеспечения и / или данных

Если вычислительные ресурсы, программное обеспечение или данные УЦ «Сименс» повреждены (например, при стихийном бедствии или враждебной атаке), УЦ «Сименс» должен сообщить о таких случаях в PMA. Процедуры урегулирования выполняются для фактических или угрожающих враждебных атак.

Если затронут только Корневой УЦ, Выпускающий УЦ может продолжать работать, поскольку:

(i) замена оборудования, скорее всего, будет быстро осуществлена;
(ii) доступно программное обеспечение системы Корневого УЦ;
(iii) Закрытый ключ Корневого УЦ и список отзыва сертификатов (CRL) хранятся отдельно и в безопасных местах, и
(iv) если применяются пункты (i) - (iii), система Корневого УЦ может быть повторно активирована в кратчайшие сроки.

5.7.3 Порядок действий в случае компрометации закрытого ключа организации

Если закрытый ключ Корневого УЦ «Сименс» скомпрометирован или предположительно скомпрометирован, выполняются следующие процедуры:

- ❑ проинформировать Субъектов, Доверяющие стороны и Европейский мост УЦ;
- ❑ указать, что сертификаты и информация о статусе отзыва, выпущенные с использованием этого ключа Корневого УЦ, могут быть больше недействительными;
- ❑ прекратить действие сертификата и Службы распространения CRL для сертификатов и CRL, выпущенных с использованием скомпрометированного закрытого ключа;
- ❑ запросить отзыв всех затронутых сертификатов.

5.7.4 Возможности по обеспечению непрерывности бизнеса после аварийной ситуации

Высокая доступность служб сертификации, предоставляемых УЦ «Сименс», гарантируется внедрением установки системы с резервированием.

В случае нарушения или потери вычислительных ресурсов, программного обеспечения или данных соответствующий План аварийного восстановления и обеспечения непрерывности бизнеса в соответствии с Правилами СМИБ должен реализовываться на объекте, расположенном отдельно, который способен предоставлять услуги УЦ.

Восстановление критически важных служб, таких как приостановка / отзыв сертификатов, проверка сертификатов и публикация списков отзыва сертификатов, должно быть осуществлено в течение максимум двадцати четырех (24) часов. Полная функциональность должна быть восстановлена в течение 30 дней.

5.8 Прекращение работы УЦ

В случае, если «Сименс» прекратит обслуживание УЦ, УЦ «Сименс» должен уведомить Доверяющие

стороны и других затронутых лиц перед прекращением функционирования УЦ через свой веб-сайт. Следующий план действий при прекращении функционирования должен свести к минимуму негативные последствия для Доверяющих сторон:

- ❑ Публикация уведомления для сторон, затрагиваемых прекращением функционирования УЦ, включая Европейский мост УЦ.
- ❑ Отзыв сертификата, выданного Выпускающим УЦ.
- ❑ Сохранение архивов и записей УЦ за периоды времени, требуемые настоящим ЗПС.
- ❑ Продолжение функционирования службы обслуживания и поддержки клиентов.
- ❑ Продолжение функционирования служб отзыва, таких как выпуск CRL.
- ❑ Утилизация закрытого ключа Корневого УЦ.
- ❑ Меры, необходимые для перехода фактических служб Корневого УЦ к преемнику Корневого УЦ.

6 Технический контроль безопасности

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

Технические средства контроля безопасности включают:

- ❑ меры безопасности, предпринятые УЦ «Сименс» для защиты его корневых пар ключей и данных активации (например, паролей)
- ❑ другие технические средства контроля безопасности, используемые для безопасного выполнения функций, перечисленных в Регламенте УЦ 1.1, включая технические средства контроля, такие как средства контроля безопасности на протяжении жизненного цикла (например, безопасность среды разработки программного обеспечения, методология разработки надежного программного обеспечения) и оперативные средства контроля безопасности.

6.1 Генерация и установка пары ключей

6.1.1 Генерация пары ключей

В настоящее время пары ключей Корневых центров сертификации и Выпускающих центров сертификации генерируются с помощью аппаратного модуля безопасности («HSM»), который сертифицирован в соответствии с уровнем 3 FIPS 140-2.

6.1.2 Предоставление закрытого ключа субъекту

Не применимо.

6.1.3 Предоставление закрытого ключа эмитенту сертификата

Не применимо.

6.1.4 Предоставление закрытого ключа УЦ доверяющим сторонам

Сертификаты УЦ «Сименс» распространяются среди доверяющих сторон для целей проверки правильности пути сертификации. Открытые ключи УЦ «Сименс» публикуются на веб-сайте «Сименс» ИОК.

6.1.5 Размеры ключа

Алгоритмы и длина ключей, разрешенные УЦ «Сименс», определены в документе «Профиль сертификата», доступном на веб-сайте .com/pki.

6.1.6 Генерация и проверка качества параметров открытого ключа

Не предусмотрено.

6.1.7 Цели использования ключа

Поля расширения «KeyUsage» сертификатов УЦ «Сименс» указаны в соответствии с RFC 5280 и определены в документе «Профиль сертификата».

6.2 Защита закрытого ключа и технические средства контроля криптографического модуля

6.2.1 Стандарты и средства контроля криптографического модуля

Криптографический модуль (HSM), используемый для работы ЦС «Сименс», сертифицирован для уровня 3 FIPS 140-2 и общих критериев (CC), уровня гарантии оценки (EAL) 4+, который в целом эквивалентен Критериям оценки безопасности информационных технологий (ITSEC) уровня гарантии E3.

6.2.2 Многопользовательский контроль закрытого ключа (n из m)

Внедрены технические и процедурные механизмы, требующие участия нескольких доверенных сотрудников для выполнения важных криптографических операций Корневого УЦ. Чтобы получить доступ к закрытым ключам, требуется N из M лиц. Одно лицо не имеет всех данных активации, необходимых для доступа к любому из закрытых ключей УЦ «Сименс».

6.2.3 Депонирование закрытых ключей

Не предусмотрено.

6.2.4 Резервное копирование закрытого ключа

Закрытый ключ Корневого УЦ «Сименс» будет скопирован и надежно сохранен для маловероятного случая потери ключа из-за неожиданного прерывания питания или сбоя оборудования на отдельных объектах. Резервное копирование ключей выполняется в рамках процедуры создания ключей УЦ. Резервная копия закрытого ключа УЦ остается секретной, а их целостность и аутентичность сохраняются.

Закрытые ключи повторно генерируются с использованием набора карт регенерации ключей. Процедура повторной генерации ключа оформляется документально и должна выполняться под двойным контролем на физически защищенном объекте.

6.2.5 Архив закрытых ключей

Не предусмотрено.

6.2.6 Передача закрытого ключа в криптографический модуль или из него

Пары ключей Корневого УЦ «Сименс» генерируются в модулях HSM, в которых будут использоваться ключи.

6.2.7 Хранение закрытых ключей на криптографическом модуле

Закрытый ключ Корневого УЦ «Сименс» хранится в резервных модулях HSM в зашифрованном виде.

6.2.8 Способ активации закрытого ключа

Закрытый ключ Корневого УЦ «Сименс» можно активировать, введя заданное количество карт оператора в HSM. Для активации закрытого ключа Корневого УЦ требуется ввод и проверка ПИН-кода / кодовой фразы, соответствующих указанным параметрам безопасности.

6.2.9 Способ деактивации закрытого ключа

После использования закрытые ключи деактивируются, карты оператора вынимаются из HSM.

6.2.10 Метод уничтожения закрытого ключа

Закрытые ключи уничтожаются, если они больше не нужны или, когда Сертификаты, которым они соответствуют, истекают или отзываются. Для уничтожения закрытого ключа УЦ требуется участие, по крайней мере, трех доверенных сотрудников. Закрытые ключи должны быть уничтожены таким образом, чтобы предотвратить их потерю, кражу, модификацию, несанкционированное раскрытие или несанкционированное использование.

После завершения процесс уничтожения регистрируется.

6.2.11 Рейтинг криптографического модуля

В целом, модули HSM работают с уровнями прошивки, которые сертифицированы в соответствии с уровнем 3 FIPS 140-2. «Сименс» оставляет за собой право использовать свои HSM с прошивкой OEM с уровнями или конфигурациями, которые не сертифицированы в соответствии с уровнем 3 FIPS 140-2, если это требуется для работы или безопасности, а также если не доступна новая прошивка FIPS или ее конфигурация.

6.3 Другие аспекты управления парой ключей

6.3.1 Архив открытых ключей

Открытые ключи УЦ «Сименс» копируются и архивируются в рамках процедур регламентного резервного копирования.

6.3.2 Периоды функционирования сертификата и периоды использования пары ключей

Период функционирования Сертификата заканчивается в случае истечения срока его действия или отзыва. Период функционирования пары ключей совпадает с периодом функционирования соответствующих сертификатов, за исключением случаев, когда они могут продолжать использоваться для проверки подписи. Максимальные периоды функционирования сертификатов Корневого ЦС приведены в таблице ниже.

Сертификат	Срок действия
Сертификат Корневого УЦ «Сименс»	До двенадцати (12) лет

Применимость криптографических алгоритмов и параметров постоянно контролируется PMA. Если алгоритм или соответствующая длина ключа не обеспечивают достаточную безопасность в течение срока действия сертификата, то соответствующий сертификат отзывается, и инициируется новая заявка на сертификат.

6.4 Данные активации

Данные активации относятся к значениям данных, необходимым для работы криптографических модулей, таких как ПИН-код, кодовая фраза. Защита данных активации соответствует уровню 3 FIPS 140-1.

6.4.1 Генерация и установка данных активации

Не предусмотрено.

6.4.2 Защита данных активации

Не предусмотрено.

6.4.3 Другие аспекты данных активации

Не предусмотрено.

6.5 Контроль компьютерной безопасности

Все технические средства контроля компьютерной безопасности, внедренные для УЦ «Сименс» и Службы проверки сертификатов, создаются и документируются в соответствии с Правилами СМИБ. Все компьютеры в УЦ «Сименс» подлежат постоянному мониторингу. Результаты мониторинга доступны 24 часа в сутки 7 дней в неделю. Конфигурирование компонентов системы может выполняться только при двойном контроле.

6.6 Контроль безопасности на протяжении жизненного цикла

6.6.1 Контроль за разработкой систем

Средства контроля за разработкой систем предоставляются в соответствии со стандартами разработки систем и управления изменениями, предусмотренными СМИБ. Разработка систем осуществляется доверенными поставщиками программного обеспечения в соответствии со спецификациями для безопасного программирования.

6.6.2 Средства управления безопасностью

Средства управления безопасностью УЦ «Сименс» предоставляются в соответствии с СМИБ «Сименс».

6.6.3 Жизненный цикл средств контроля безопасности

Все средства контроля безопасности проверяются ежегодно внешним аудитором.

6.7 Контроль сетевой безопасности

Корневой УЦ «Сименс» работает автономно и не подключен к сети с любыми внешними компонентами.

6.8 Процесс присвоения отметок времени

Не предусмотрено.

7 Сертификат, профили CRL и OCSP

Все цифровые сертификаты, выданные корневыми УЦ, соответствуют цифровым сертификатам и профилям CRL, как описано в [RFC 5280].

7.1 Профиль сертификата

Подробное описание профилей Корневого УЦ можно загрузить по ссылке

7.2 Профиль CRL

Подробное описание профилей CRL можно загрузить по ссылке

7.3 Профиль OCSP

Подробное описание профилей OCSP можно загрузить по ссылке

8 Аудит соответствия и другие оценки

Указано в Регламенте УЦ.

9 Прочие коммерческие и юридические вопросы

Указано в Регламенте УЦ.

10 Справочные материалы

Указано в Регламенте УЦ.

Приложение A: Сокращения и определения

A.1 Определения

Указано в Приложении Регламенту УЦ.

A.2 Сокращения

Указано в Приложении к Регламенту УЦ.