
# Заявление о практике сертификации

## Выпускающие Удостоверяющие центры «Сименс»

# История изменений документа

| Версия | Дата | Автор | Комментарий к изменению |
|---|---|---|---|
| 1.0 | 10 июня 2016 г. | Александр Виннен, Михаэль Мунцерт | Первая версия |
| 1.1 | 1 декабря 2016 г. | Руфус Бушарт | Незначительно обновленная версия |
| 1.2 | 26 мая 2017 г. | Руфус Бушарт | Обновление Выпускающих УЦ 2017 г. |
| 1.3 | 31 июля 2017 г. | Бьёрн Хундертмарк | Обновление главы по авторизации центра сертификации (CAA) |

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 Выпускающих удостоверяющих центров «Сименс» (Выпускающих УЦ). Целью настоящего документа является публичное раскрытие подписчикам и доверяющим сторонам политик и методов ведения деятельности, в соответствии с которыми работают данные Выпускающие УЦ.

# Статус документа

Настоящий документ с версией 1.3 и статусом «Выпущен» был классифицирован как «Без ограничений».

| | **Название** | **Отдел** | **Дата** |
|---|---|---|---|
| **Автор** | Различные авторы, подробная информация в истории изменений документа | | |
| **Проверил:** | Тобиас Ланге<br>Руфус Бушарт | Siemens LS<br>Siemens GS IT HR 7 4 | 10 июня 2016 г.<br>23 августа 2017 г. |
| **Утвердил:** | Маркус Вихманн | Siemens GS IT ISEC | 23 августа 2017 г. |

Настоящее Заявление о практике сертификации (ЗПС) было утверждено ответственным сотрудником по информационной безопасности «Сименс» 23 августа 2017 года.

# Содержание

**История изменений документа** ..... 2
**Область применения** ..... 2
**Статус документа** ..... 2
**1 Введение** ..... 8
**1.1 Обзор** ..... 8
**1.2 Название и идентификационное обозначение документа** ..... 9
**1.3 Участники ИОК** ..... 9
**1.3.1 Центры сертификации** ..... 9
**1.1.1 Центры регистрации** ..... 9
**1.1.2 Подписанты** ..... 9
**1.1.3 Доверяющие стороны** ..... 9
**1.1.4 Другие участники** ..... 9
**1.2 Использование сертификата** ..... 9
**1.2.1 Надлежащее использование сертификата** ..... 9
**1.2.2 Запрещенное использование сертификата** ..... 9
**1.3 Управление политикой** ..... 9
**1.3.1 Организация, управляющая документом** ..... 9
**1.3.2 Контактное лицо** ..... 9
**2 Обязанности по публикации и хранению** ..... 9
**2.1 Хранилища** ..... 9
**2.2 Публикация информации о сертификации** ..... 9
**2.3 Время или периодичность публикации** ..... 9
**2.4 Контроль доступа в хранилищах** ..... 9
**3 Идентификация и аутентификация** ..... 10
**3.1 Присвоение имени** ..... 10
**3.1.1 Типы имен** ..... 10
**3.1.2 Информативность имен** ..... 10
**3.1.3 Анонимность или псевдоним подписчиков** ..... 10
**3.1.4 Правила интерпретации различных форм имен** ..... 10
**3.1.5 Уникальность имен** ..... 10
**3.1.6 Признание, аутентификация и роли товарных знаков** ..... 10
**3.2 Первоначальная проверка личности** ..... 10
**3.2.1 Метод подтверждения наличия закрытого ключа** ..... 10
**3.2.2 Идентификация и аутентификация организации** ..... 10
**3.2.3 Идентификация и аутентификация физического лица** ..... 10
**3.2.4 Неподтвержденная информация о подписчиках** ..... 10
**3.2.5 Проверка центра** ..... 10
**3.2.6 Критерии взаимодействия между доверенными сообществами** ..... 10

**3.3 Идентификация и аутентификация запросов повторного ключа .....10**

**3.4 Идентификация и аутентификация запросов на отзыв.....10**

**4 Требования к использованию сертификата на протяжении жизненного цикла 10**

**4.1 Заявка на сертификат .....11**

**4.1.1 Кто может подать заявку на сертификат? .....11**

**4.1.2 Процесс регистрации и обязанности.....11**

**4.2 Обработка заявок на сертификаты.....11**

**4.2.1 Выполнение функций идентификации и аутентификации.....11**

**4.2.2 Утверждение или отклонение заявок на сертификаты .....11**

**4.2.3 Время обработки заявок на сертификаты.....11**

**4.2.4 Авторизация центра сертификации (CAA) .....11**

**4.3 Выдача сертификата.....11**

**4.3.1 Действия Корневого УЦ во время выдачи сертификата .....11**

**4.3.2 Уведомление подписчика УЦ о выдаче сертификата .....11**

**4.4 Принятие сертификата.....11**

**4.4.1 Поведение, подтверждающее принятие сертификата .....11**

**4.4.2 Публикация сертификата УЦ.....11**

**4.4.3 Уведомление УЦ о выдаче сертификата другим организациям.....12**

**4.5 Пара ключей и использование сертификата.....12**

**4.5.1 Закрытый ключ субъекта и использование сертификата.....12**

**4.5.2 Открытый ключ доверяющей стороны и использование сертификата .....12**

**4.6 Продление сертификата .....12**

**4.6.1 Обстоятельства для продления сертификата.....12**

**4.6.2 Кто может запросить продление?.....12**

**4.6.3 Обработка запроса на продление сертификата .....12**

**4.6.4 Уведомление о выдаче нового сертификата субъекту .....12**

**4.6.5 Поведение, подтверждающее принятие продленного сертификата .....13**

**4.6.6 Публикация продленного сертификата УЦ .....13**

**4.6.7 Уведомление УЦ о выдаче сертификата другим организациям.....13**

**4.7 Сертификат с повторным ключом .....13**

**4.7.1 Обстоятельства для выдачи сертификатов с повторным ключом.....13**

**4.7.2 Кто может запросить сертификацию нового открытого ключа? .....13**

**4.7.3 Обработка запроса на выдачу сертификата с повторным ключом.....13**

**4.7.4 Уведомление о выдаче нового сертификата подписчику.....13**

**4.7.5 Поведение, подтверждающее принятие сертификата с повторным ключом.....13**

**4.7.6 Публикация сертификата с повторным ключом УЦ .....13**

**4.7.7 Уведомление УЦ о выдаче сертификата другим организациям.....13**

**4.8 Изменение сертификата .....13**

**4.9 Отзыв и приостановка сертификата.....13**

**4.9.1 Обстоятельства для отзыва .....13**

4.9.2 Кто может запросить отзыв? ....13
4.9.3 Процедура подачи запроса на отзыв ....13
4.9.4 Период отсрочки для подачи запроса на отзыв ....13
4.9.5 Время, в течение которого УЦ должен обработать запрос на отзыв ....13
4.9.6 Требование к проверке отзыва для доверяющих сторон ....13
4.9.7 Частота выпуска списков отзыва сертификатов (CRL) ....13
4.9.8 Максимальное время ожидания для списков отзыва сертификатов (CRL) ....13
4.9.9 Требования к проверке отзыва в режиме онлайн ....14
4.9.10 Другие доступные формы сообщений об отзыве ....14
4.9.11 Специальные требования к компрометации закрытого ключа ....14
4.9.12 Обстоятельства для приостановки ....14
4.10 Службы проверки статуса сертификатов ....14
4.10.1 Эксплуатационные характеристики ....14
4.10.2 Доступность службы ....14
4.10.3 Дополнительные характеристики ....14
4.11 Окончание подписки ....14
4.12 Депонирование и восстановление ключей ....14
5 Управление, операционный и физический контроль ....14
5.1 Контроль физической безопасности ....14
5.1.1 Расположение и строительство объекта ....14
5.1.2 Физический доступ ....14
5.1.3 Электроснабжение и кондиционирование воздуха ....14
5.1.4 Водоснабжение ....14
5.1.5 Противопожарная защита ....14
5.1.6 Средства хранения данных ....14
5.1.7 Утилизация отходов ....14
5.1.8 Внешнее резервное копирование ....14
5.2 Контроль процедур ....14
5.2.1 Доверенные роли ....14
5.2.2 Количество лиц, необходимое для выполнения одной задачи ....15
5.2.3 Идентификация и аутентификация для каждой роли ....15
5.2.4 Роли, требующие разделения обязанностей ....15
5.3 Контроль безопасности персонала ....15
5.3.1 Требования к квалификации, опыту и наличию разрешений ....15
5.3.2 Процедуры специальной проверки сведений ....15
5.3.3 Требования к обучению ....15
5.3.4 Частота и требования к переподготовке ....15
5.3.5 Частота и последовательность ротации должностей ....15
5.3.6 Санкции за несанкционированные действия ....15
5.3.7 Требования к независимым подрядчикам ....15
5.3.8 Документы, предоставленные персоналу ....15

**5.4 Процедуры ведения журнала аудита ..... 15**
**5.4.1 Типы регистрируемых событий ..... 15**
**5.4.2 Частота обработки данных журнала аудита ..... 15**
**5.4.3 Период хранения данных журнала аудита ..... 15**
**5.4.4 Защита журналов аудита ..... 15**
**5.4.5 Процедуры резервного копирования данных журнала аудита ..... 15**
**5.4.6 Система сбора информации для мониторинга (внутренняя или внешняя) ..... 15**
**5.4.7 Уведомление субъекта, инициирующего событие ..... 15**
**5.4.8 Оценки уязвимостей ..... 15**
**5.5 Архив записей ..... 16**
**5.5.1 Типы архивируемых записей ..... 16**
**5.5.2 Период хранения архивируемых данных журнала аудита ..... 16**
**5.5.3 Защита архивированных данных журнала аудита ..... 16**
**5.5.4 Процедуры архивирования резервных копий ..... 16**
**5.5.5 Требования к присвоению отметок времени записям ..... 16**
**5.5.6 Система сбора архивированных данных (внутренняя или внешняя) ..... 16**
**5.5.7 Процедуры получения и проверки архивированных данных ..... 16**
**5.6 Смена ключа ..... 16**
**5.7 Компрометация и аварийное восстановление ..... 16**
**5.7.1 Процедуры обработки инцидентов и случаев компрометации ..... 16**
**5.7.2 Повреждение вычислительных ресурсов, программного обеспечения и / или данных ..... 16**
**5.7.3 Порядок действий в случае компрометации закрытого ключа организации ..... 16**
**5.7.4 Возможности по обеспечению непрерывности бизнеса после аварийной ситуации ..... 16**
**5.8 Прекращение УЦ ..... 16**
**6 Технический контроль безопасности ..... 16**
**6.1 Генерация и установка пары ключей ..... 16**
**6.1.1 Генерация пары ключей ..... 16**
**6.1.2 Предоставление закрытого ключа субъекту ..... 17**
**6.1.3 Предоставление закрытого ключа эмитенту сертификата ..... 17**
**6.1.4 Предоставление закрытого ключа УЦ доверяющим сторонам ..... 17**
**6.1.5 Размеры ключа ..... 17**
**6.1.6 Генерация и проверка качества параметров открытого ключа ..... 17**
**6.1.7 Цели использования ключа ..... 17**
**6.2 Защита закрытого ключа и технические средства контроля криптографического модуля ..... 17**
**6.2.1 Стандарты и средства контроля криптографического модуля ..... 17**
**6.2.2 Многопользовательский контроль закрытого ключа (n из m) ..... 17**
**6.2.3 Депонирование закрытых ключей ..... 17**
**6.3 Резервное копирование закрытого ключа ..... 17**
**6.3.1 Архив закрытых ключей ..... 17**
**6.3.2 Передача закрытого ключа в криптографический модуль или из него ..... 17**
**6.3.3 Хранение закрытых ключей на криптографическом модуле ..... 18**

6.3.4 Способ активации закрытого ключа....18
6.3.5 Способ деактивации закрытого ключа....18
6.3.6 Способ уничтожения закрытого ключа....18
6.3.7 Рейтинг криптографического модуля....18
6.4 Другие аспекты управления парой ключей....18
6.4.1 Архив открытых ключей....18
6.4.2 Периоды функционирования сертификата и периоды использования пары ключей....18
6.5 Данные активации....19
6.5.1 Генерация и установка данных активации....19
6.5.2 Защита данных активации....19
6.5.3 Другие аспекты данных активации....19
6.6 Контроль компьютерной безопасности....19
6.7 Контроль безопасности на протяжении жизненного цикла....19
6.7.1 Контроль за разработкой систем....19
6.7.2 Средства управления безопасностью....19
6.7.3 Жизненный цикл средств контроля безопасности....19
6.8 Контроль сетевой безопасности....19
6.9 Процесс присвоения отметок времени....20
7 Сертификат, профили CRL и OCSP....20
7.1 Профиль сертификата....20
7.2 Профиль CRL....20
7.3 Профиль OCSP....20
8 Аудит соответствия и другие оценки....20
9 Прочие коммерческие и юридические вопросы....20
10 Справочные материалы....20
Приложение A: Сокращения и определения....20
A.1 Определения....20
A.2 Сокращения....20

# 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 Выпускающими УЦ «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).
Если в будущем будут введены новые Выпускающие УЦ, то могут быть созданы дополнительные документы ЗПС для учета специальных требований.

Изображение иерархии ИОК «Сименс» можно найти в ЗПС Корневого УЦ «Сименс».

В следующей таблице перечислены действующие в настоящее время Выпускающие УЦ, а также требования к выданным ими сертификатам в соответствии с [ETSI 102 042], включая соответствующие защищенные устройства. Минимальным требованием является NCP.

| **Выпускающий УЦ** | **Требования к выданным сертификатам** | | | | | | |
|---|---|---|---|---|---|---|---|
| | **Уровень качества ETSI** | | | **Защищенное устройство** | | | |
| | **NCP+** | **OVCP** | **DVCP** | **Смарт-карта** | **Смарт-фон** | **HSM** | **NwSC** |
| ZZZZZZA2 Siemens Issuing CA EE Auth 2016 | X | | | X | | | |
| ZZZZZZA3 Siemens Issuing CA EE Enc 2016 | X | | | X | X | | X |
| ZZZZZZA4 Siemens Issuing CA Intranet Code Signing 2016 | | | | | | | |
| ZZZZZZA5 Siemens Issuing CA Multipurpose 2016 | | | | | | | |
| ZZZZZZA6 Siemens Issuing CA Medium Strength Authentication 2016 | | | | | | | |
| ZZZZZZA7 Siemens Issuing CA Intranet Server 2016 | | X | X | | | | |
| ZZZZZZB7 Siemens Issuing CA Intranet Server 2017 | | X | X | | | | |
| ZZZZZZA8 Siemens Issuing CA Internet Code Signing 2016 | | | | | | | |
| ZZZZZZA9 Siemens Issuing CA Class Internet Server 2016 | | X | X | | | | |
| ZZZZZZB9 Siemens Issuing CA Class Internet Server 2017 | | X | X | | | | |
| ZZZZZZAD Siemens Issuing CA EE Network Smartcard Auth 2016 | | | | | | | X |
| ZZZZZZAB Siemens Issuing CA MSA Impersonated Entities 2016 | | | | | | | |
| ZZZZZZY2 Siemens Issuing CA EE Auth 2013 | X | | | X | | | |
| ZZZZZZY3 Siemens Issuing CA EE Enc 2013 | X | | | X | X | | X |
| ZZZZZZY4 Siemens Issuing CA Intranet Code Signing 2013 | | | | | | | |
| ZZZZZZY5 Siemens Issuing CA Multipurpose 2013 | | | | | | | |
| ZZZZZZY6 Siemens Issuing CA Medium Strength Authentication 2013 | | | | | | | |
| ZZZZZZY7 Siemens Issuing CA Intranet Server 2013 | | X | X | | | | |
| ZZZZZZY8 Siemens Issuing CA Internet Code Signing 2013 | | | | | | | |
| ZZZZZZY9 Siemens Issuing CA Class Internet Server 2013 | | X | X | | | | |
| ZZZZZZYB Siemens Issuing CA MSA Impersonated Entities 2013 | | | | | | | |
| ZZZZZZV2 Siemens Issuing CA EE Auth 2011 | X | | | X | | | |
| ZZZZZZV3 Siemens Issuing CA EE Enc 2011 | X | | | X | X | | X |
| ZZZZZZV4 Siemens Issuing CA Intranet Code Signing 2011 | | | | | | | |
| ZZZZZZV6 Siemens Issuing CA Medium Strength Authentication 2011 | | | | | | | |
| ZZZZZZV8 Siemens Issuing CA Internet Code Signing 2011 | | | | | | | |
| ZZZZZZVN Siemens Issuing CA Class PGP | | | | | | | |

Таблица 1: Внедрение требований ETSI выпускающим УЦ

Выпускающие УЦ «Сименс» выпускает сертификаты для указанных ниже групп Конечных пользователей или класса приложений с общими требованиями безопасности («Сообщества»).

Для ИОК «Сименс» существуют следующие Сообщества:

- Сотрудник «Сименс» (S-E)
- Функциональная группа (FG)
- Деловой партнер (BP)
- Устройство (например, Сервер — SRV)

## 1.2 Название и идентификационное обозначение документа

ЗПС означает «Заявление о практике сертификации» Выпускающих УЦ «Сименс».

Наименование: Заявление о практике сертификации Выпускающих центров сертификации «Сименс»
OID: 1.3.6.1.4.1.4329.99.2.2.1.1.0
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.

### 1.1.1 Центры регистрации

Указано в Регламенте УЦ.

### 1.1.2 Подписанты

Указано в Регламенте УЦ.

### 1.1.3 Доверяющие стороны

Указано в Регламенте УЦ.

### 1.1.4 Другие участники

Указано в Регламенте УЦ.

## 1.2 Использование сертификата

### 1.2.1 Надлежащее использование сертификата

Указано в Регламенте УЦ.

### 1.2.2 Запрещенное использование сертификата

Указано в Регламенте УЦ.

## 1.3 Управление политикой

### 1.3.1 Организация, управляющая документом

Указано в Регламенте УЦ.

### 1.3.2 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 имен

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 доверенными сообществами

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

В приведенной ниже таблице указаны обязанности для каждого типа подписчиков и сертификата аутентификации/цифровых подписей («Сертификат A/D»); сертификата шифрования (Сертификат E) и сертификата сервера (Сертификат S). Для сертификатов конечных пользователей Выпускающий УЦ «Сименс» не предоставляет операции «Продление» и «Изменение», поскольку они охватываются процессом «Повторный ключ».

**Сокращения:**

«Конечный пользователь» = EE; «Уполномоченная сторона» = AP; «Спонсор «Сименс» = SS;

Служба самообслуживания ИОК = PKISS

| **Владелец сертификата** | | **Жизненный цикл сертификата** | | | | |
|---|---|---|---|---|---|---|
| **Сообщество** | **Подписчик** | **Первоначальная заявка** | **Продление** | **Повторный ключ** | **Изменение** | **Отзыв** |
| Сообщество «Сименс» | Сотрудник «Сименс»<br>• *Сертификат A/D*<br>• Сертификат E<br>• Сертификат EFS | AP через RA | Не предусмотрено | EE или AP через RA или PKISS | Не предусмотрено | EE или AP через RA или PKISS (только для *Сертификата E)* |
| | • | | | | | |
| | «Сименс» Функциональное Группа<br>• *Сертификат A/D*<br>• *Сертификат E*<br>• *Подписание кода* | AP через RA | Не предусмотрено | AP или SS через RA | Не предусмотрено | AP или SS через RA |
| Деловой партнер Сообщество | Деловой партнер<br>• *Сертификат A/D*<br>• *Сертификат E*<br>• *Универсальный сертификат* | SS или AP через RA | Не предусмотрено | EE или AP через RA или PKISS | Не предусмотрено | AP или SS через RA и EE через PKISS |
| Сервер Сообщество | Сервер<br>• *S Сертификат* | AP через RA | Не предусмотрено | AP через RA | Не предусмотрено | AP через RA |

Таблица 2: Жизненный цикл сертификата для Выпускающих УЦ «Сименс»

## 4.1 Заявка на сертификат

### 4.1.1 Кто может подать заявку на сертификат?

Члены сообщества «Сименс», сообщества делового партнера и сообщества сервера могут выступать в качестве заявителей на получение сертификата.

### 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.

### 4.2.4 Авторизация центра сертификации (CAA)

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

Сертификаты подписчиков публикуются в хранилище в соответствии со следующей таблицей.

| | «Сименс» SCD | «Сименс» AD | Внешнее хранилище |
|---|---|---|---|
| Хранилище Классификация | Внутренние | Внутренние | Внешние |
| Сертификаты аутентификации | Нет | Нет | Нет |
| Сертификаты шифрования | Есть | Да | Есть |
| Универсальные сертификаты | Нет | Нет | Есть |
| Сертификаты EFS | Нет | Нет | Нет |
| Сертификаты подписи кода | Нет | Нет | Нет |
| Сертификаты сервера | Нет | Нет | Нет |

Таблица 3: Публикация сертификатов подписчиков

#### 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

Для субъектов сообщества «Сименс» (сотрудники «Сименс» и функциональные группы): Выпускающие УЦ «Сименс» или соответствующие центры регистрации несут ответственность за информирование каждого субъекта об этих обязанностях и любых применимых ограничениях на использование сертификатов и пар ключей, налагаемых внутренними политиками «Сименс» в соответствии с трудовым законодательством и практикой, регулирующей соответствующие центры регистрации.

Для субъектов сообщества делового партнера, которые являются физическими лицами и независимыми подрядчиками: Спонсор «Сименс» или его центр регистрации несет ответственность за информирование субъектов об этих обязанностях и любых ограничениях на использование, налагаемых внутренними политиками «Сименс» в соответствии с трудовым законодательством и практикой. Для субъектов сообщества делового партнера, которые являются сотрудниками или агентами юридических лиц, являющихся деловыми партнерами, соответствующий центр регистрации делового партнера несет ответственность за информирование каждого субъекта об этих обязанностях и любых применимых ограничениях на использование, налагаемых внутренними политиками делового партнера в соответствии с трудовым законодательством и практикой, регулирующей соответствующий центр регистрации.

Для субъектов сообщества сервера: Выпускающие УЦ «Сименс» или соответствующие центры регистрации несут ответственность за информирование каждого субъекта об этих обязанностях и любых применимых ограничениях на использование сертификатов и пар ключей, налагаемых внутренними политиками «Сименс» в соответствии с трудовым законодательством и практикой, регулирующей соответствующие центры регистрации.

#### 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

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 Требования к проверке 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

Указано в ЗПС Корневых УЦ.

### 5.1 Контроль физической безопасности

#### 5.1.1 Расположение и строительство объекта

Указано в ЗПС Корневых УЦ.

#### 5.1.2 Физический доступ

Указано в ЗПС Корневых УЦ.

#### 5.1.3 Электроснабжение и кондиционирование воздуха

Указано в ЗПС Корневых УЦ.

#### 5.1.4 Водоснабжение

Указано в ЗПС Корневых УЦ.

#### 5.1.5 Противопожарная защита

Указано в ЗПС Корневых УЦ.

#### 5.1.6 Средства хранения данных

Указано в ЗПС Корневых УЦ.

#### 5.1.7 Утилизация отходов

Указано в ЗПС Корневых УЦ.

#### 5.1.8 Внешнее резервное копирование

Указано в ЗПС Корневых УЦ.

### 5.2 Контроль процедур

#### 5.2.1 Доверенные роли

Указано в ЗПС Корневых УЦ.

#### 5.2.2 Количество лиц, необходимое для выполнения одной задачи

Указано в ЗПС Корневых УЦ.

#### 5.2.3 Идентификация и аутентификация для каждой роли

Указано в ЗПС Корневых УЦ.

#### 5.2.4 Роли, требующие разделения обязанностей

Указано в ЗПС Корневых УЦ.

## 5.3 Контроль безопасности персонала

#### 5.3.1 Требования к квалификации, опыту и наличию разрешений

Указано в ЗПС Корневых УЦ.

#### 5.3.2 Процедуры специальной проверки сведений

Указано в ЗПС Корневых УЦ.

#### 5.3.3 Требования к обучению

Указано в ЗПС Корневых УЦ.

#### 5.3.4 Частота и требования к переподготовке

Указано в ЗПС Корневых УЦ.

#### 5.3.5 Частота и последовательность ротации должностей

Указано в ЗПС Корневых УЦ.

#### 5.3.6 Санкции за несанкционированные действия

Указано в ЗПС Корневых УЦ.

#### 5.3.7 Требования к независимым подрядчикам

Указано в ЗПС Корневых УЦ.

#### 5.3.8 Документы, предоставленные персоналу

Указано в ЗПС Корневых УЦ.

## 5.4 Процедуры ведения журнала аудита

Указано в ЗПС Корневых УЦ.

#### 5.4.1 Типы регистрируемых событий

Указано в ЗПС Корневых УЦ.

#### 5.4.2 Частота обработки данных журнала аудита

Указано в ЗПС Корневых УЦ.

#### 5.4.3 Период хранения данных журнала аудита

Указано в ЗПС Корневых УЦ.

#### 5.4.4 Защита журналов аудита

Указано в ЗПС Корневых УЦ.

#### 5.4.5 Процедуры резервного копирования данных журнала аудита

Не предусмотрено.

#### 5.4.6 Система сбора информации для мониторинга (внутренняя или внешняя)

Указано в ЗПС Корневых УЦ.

#### 5.4.7 Уведомление субъекта, инициирующего событие

Указано в ЗПС Корневых УЦ.

#### 5.4.8 Оценки уязвимостей

Указано в ЗПС Корневых УЦ.

## 5.5 Архив записей

### 5.5.1 Типы архивируемых записей

Указано в ЗПС Корневых УЦ.

### 5.5.2 Период хранения архивируемых данных журнала аудита

Указано в ЗПС Корневых УЦ.

### 5.5.3 Защита архивированных данных журнала аудита

Указано в ЗПС Корневых УЦ.

### 5.5.4 Процедуры архивирования резервных копий

Указано в ЗПС Корневых УЦ.

### 5.5.5 Требования к присвоению отметок времени записям

Указано в ЗПС Корневых УЦ.

### 5.5.6 Система сбора архивированных данных (внутренняя или внешняя)

Указано в ЗПС Корневых УЦ.

### 5.5.7 Процедуры получения и проверки архивированных данных

Указано в ЗПС Корневых УЦ.

## 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.

| УЦ | Срок действия | Период функционирования (Дата прекращения выдачи) |
|---|---|---|
| Выпускающий УЦ «Сименс» | 6 лет | 3 года |

В Дату прекращения выдачи «Сименс» УЦ 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 УЦ.

## 5.7 Компрометация и аварийное восстановление

### 5.7.1 Процедуры обработки инцидентов и случаев компрометации

Указано в ЗПС Корневых УЦ.

### 5.7.2 Повреждение вычислительных ресурсов, программного обеспечения и / или данных

Указано в ЗПС Корневых УЦ.

### 5.7.3 Порядок действий в случае компрометации закрытого ключа организации

Указано в ЗПС Корневых УЦ.

### 5.7.4 Возможности по обеспечению непрерывности бизнеса после аварийной ситуации

Указано в ЗПС Корневых УЦ.

## 5.8 Прекращение УЦ

Указано в ЗПС Корневых УЦ.

# 6 Технический контроль безопасности

Указано в ЗПС Корневых УЦ.

## 6.1 Генерация и установка пары ключей

### 6.1.1 Генерация пары ключей

Указано в ЗПС Корневых УЦ.

#### 6.1.2 Предоставление закрытого ключа субъекту

Во время работы Выпускающих УЦ «Сименс» доверенный оператор обеспечивает, чтобы закрытый ключ УЦ не выходил за пределы защищенного объекта.
Для сертификата аутентификации/цифровых подписей закрытый ключ не предоставляется подписчикам, потому что каждый подписчик генерирует свой собственный закрытый ключ с помощью устройства создания защищенной подписи («SSCD»). Для сертификата шифрования закрытый ключ предоставляется субъекту надежным образом через соответствующее центры регистрации либо путем физической передачи закрытого ключа субъекту лично после подтверждения личности субъекта или путем надежной рассылки или доставки через курьера закрытого ключа в соответствии с процедурой подтверждения личности субъекта или через PKISS.
Для сертификатов сервера, запрошенных PKCS #10, заявитель на получение сертификата отвечает за секретность закрытого ключа. Выпускающий УЦ «Сименс» не хранит или не генерирует этот ключ.

#### 6.1.3 Предоставление закрытого ключа эмитенту сертификата

Не предусмотрено.

#### 6.1.4 Предоставление закрытого ключа УЦ доверяющим сторонам

Указано в ЗПС Корневых УЦ.

#### 6.1.5 Размеры ключа

Указано в ЗПС Корневых УЦ.

#### 6.1.6 Генерация и проверка качества параметров открытого ключа

Указано в ЗПС Корневых УЦ.

#### 6.1.7 Цели использования ключа

Указано в ЗПС Корневых УЦ.

## 6.2 Защита закрытого ключа и технические средства контроля криптографического модуля

#### 6.2.1 Стандарты и средства контроля криптографического модуля

Указано в ЗПС Корневых УЦ.

#### 6.2.2 Многопользовательский контроль закрытого ключа (n из m)

Указано в ЗПС Корневых УЦ.

#### 6.2.3 Депонирование закрытых ключей

Для подписчиков конечных пользователей, имеющих сертификат шифрования, закрытый ключ будет храниться доверенным оператором УЦ «Сименс». Для подписчиков конечных пользователей, имеющих сертификаты аутентификации/цифровой подписи/сервера, не предусмотрено никаких условий.

## 6.3 Резервное копирование закрытого ключа.

Для закрытых ключей Выпускающего УЦ отдельные аппаратные криптографические модули для резервного копирования используются и хранятся в безопасности на отдельных объектах в местах резервного копирования доверенного оператора во время работы Выпускающего УЦ. К закрытым ключам Выпускающего УЦ применяются следующие требования:

1. Аппаратные криптографические модули, используемые для хранения закрытых ключей Выпускающего УЦ, должны соответствовать требованиям § 6.2.1.
2. Закрытые ключи Выпускающего УЦ копируются на аппаратные криптографические модули для резервного копирования в соответствии с § 6.2.6.
3. Модули, содержащие резервные копии на объекте и копии аварийного восстановления закрытых ключей Выпускающего УЦ, должны соответствовать требованиям § 5.1 и § 6.2.1.

В § 6.2.3 рассматривается резервное копирование закрытых ключей подписчиков.

#### 6.3.1 Архив закрытых ключей

Архив закрытых ключей Выпускающего УЦ: Не предусмотрено.

Архив закрытых ключей подписчика конечного пользователя: После окончания срока действия пара ключей архивируется на срок не менее тридцати (30) лет.

#### 6.3.2 Передача закрытого ключа в криптографический модуль или из него

Закрытые ключи Выпускающих УЦ надежно хранятся исключительно на аппаратных криптографических модулях. Если резервное копирование пары ключей Выпускающего УЦ осуществляется на эквивалентный аппаратный криптографический модуль, такие пары ключей переносятся между модулями в зашифрованном виде

внутри ячейки повышенной безопасности защищенного объекта.

#### 6.3.3 Хранение закрытых ключей на криптографическом модуле

Закрытые ключи Выпускающего УЦ хранятся на аппаратных криптографических модулях с общими критериями (CC), уровнем гарантии качества оценки (EAL) 4+, который в целом эквивалентен Критериям оценки безопасности информационных технологий (ITSEC) уровня гарантии E3.

#### 6.3.4 Способ активации закрытого ключа

После выдачи, закрытые ключи Выпускающего УЦ активируется на аппаратном криптографическом модуле в ячейке повышенной безопасности доверенного оператора, что подтверждается представителем УЦ «Сименс» и, по крайней мере, двумя (2) уполномоченными сотрудниками доверенного оператора и документируется для целей ведения журнала аудита.

Закрытые ключи подписчиков конечного пользователя обычно активируются посредством использования подписчиком данных активации. Все участники ИОК «Сименс» обязаны защищать данные активации для своих закрытых ключей от потери, кражи, модификации, несанкционированного раскрытия или несанкционированного использования.

#### 6.3.5 Способ деактивации закрытого ключа

Закрытые ключи Выпускающего УЦ на аппаратных криптографических модулях могут быть деактивированы (и повторно активированы, если необходимо) с помощью программного обеспечения деактивации в ячейке повышенной безопасности доверенного оператора, что подтверждается, по крайней мере, двумя (2) уполномоченными сотрудниками доверенного оператора и документируется для целей ведения журнала аудита.

#### 6.3.6 Способ уничтожения закрытого ключа

Закрытые ключи Выпускающего УЦ хранятся исключительно в криптографических аппаратных модулях (см. 6.2.7). Их уничтожение (если они больше не нужны) требует участия трех доверенных сотрудников. После завершения процесс уничтожения регистрируется.

Если закрытые ключи субъекта больше не нужны, соответствующий сертификат отзывается. В соответствии с требованиями к восстановлению ключей для ключей шифрования эти ключи надежно архивируются соответствующим Выпускающим УЦ. Например, если сотрудник покинет компанию, соответствующая карта сотрудника (включая закрытый ключ) будет убрана и уничтожена надежным образом. Процесс уничтожения документируется соответствующим образом.

#### 6.3.7 Рейтинг криптографического модуля

Указано в ЗПС Корневых УЦ.

## 6.4 Другие аспекты управления парой ключей

#### 6.4.1 Архив открытых ключей

Указано в ЗПС Корневых УЦ.

#### 6.4.2 Периоды функционирования сертификата и периоды использования пары ключей

Период использования пары ключей Выпускающего УЦ зависит от срока действия сертификатов, выданных УЦ. Срок действия закрытого ключа и открытого ключа Выпускающего УЦ, центров регистрации и субъектов заканчивается после его истечения или отзыва. Этот срок действия основан на сроке действия сертификата Корневого УЦ, как указано в таблице ниже.

| | Сертификат УЦ | Сертификат аутентификации / цифровой подписи | Сертификат шифрования | Сертификат EFS | Сертификат сервера | Универсальный сертификат | Сертификат подписи кода |
|---|---|---|---|---|---|---|---|
| **Выпускающие УЦ «Сименс»** | **6** | Не применимо | Не применимо | Не применимо | Не применимо | Не применимо | Не применимо |
| **Сотрудник «Сименс»** | Не применимо | **3** | **3** | **3** | Не применимо | Не применимо | Не применимо |
| **Функциональная группа** | Не применимо | 1 | **1** | Не применимо | Не применимо | Не применимо | 3 |
| **Деловой партнер** | Не применимо | **1** | **1** | Не применимо | Не применимо | 1 | Не применимо |
| **Серверы** | Не применимо | Не применимо | Не применимо | Не применимо | **1** | Не применимо | Не применимо |

Таблица 4 Срок действия сертификатов (в годах с даты выпуска)

## 6.5 Данные активации

Данные активации относятся к значениям данных, отличным от целых закрытых ключей, которые необходимы для работы с закрытыми ключами или аппаратными криптографическими модулями, содержащими закрытые ключи, например, ПИН-код, пароль или части закрытого ключа, используемые в схеме разделения ключей. Защита данных активации предотвращает несанкционированное использование закрытого ключа и потенциально должна учитываться для Выпускающего УЦ «Сименс», центров регистрации и субъектов.

Данные активации для закрытых ключей Выпускающего УЦ «Сименс» в настоящее время предоставляются его доверенным оператором для обеспечения полностью автоматизированного функционирования УЦ с минимальным ручным вмешательством.

### 6.5.1 Генерация и установка данных активации

Указано в ЗПС Корневых УЦ.

### 6.5.2 Защита данных активации

Указано в ЗПС Корневых УЦ.

### 6.5.3 Другие аспекты данных активации

Указано в ЗПС Корневых УЦ.

## 6.6 Контроль компьютерной безопасности

Указано в ЗПС Корневых УЦ.

## 6.7 Контроль безопасности на протяжении жизненного цикла

### 6.7.1 Контроль за разработкой систем

Указано в ЗПС Корневых УЦ.

### 6.7.2 Средства управления безопасностью

Указано в ЗПС Корневых УЦ.

### 6.7.3 Жизненный цикл средств контроля безопасности

Указано в ЗПС Корневых УЦ.

## 6.8 Контроль сетевой безопасности

Средства контроля сетевой безопасности Выпускающего УЦ, которые защищают сети, объединяющие единые компьютерные платформы и их приложения (как указано в § 6.5.1), предоставляются доверенным оператором в соответствии с его СМИБ. Они включают следующее:

1. брандмауэры и другие средства контроля для защиты целостности сетей участников ИОК от вторжения из внешних доменов;
4. достаточно надежная аутентификация для обеспечения обмена данными между соответствующими

объектами (например, центр регистрации с Выпускающим УЦ), механизмов защиты целостности, гарантирующих, что обмениваемая информация не будет изменена, а также механизмов конфиденциальности, защищающих выбранную информацию от несанкционированного рассмотрения (например, посредством передачи сообщений с цифровыми подписями или зашифрованных сообщений);
5. средства контроля доступа для защиты сетей от несанкционированного использования; а также
6. механизмы предотвращения ущерба от атак типа «отказ в обслуживании».

Все компоненты информационных технологий (ИТ) на защищенном объекте доверенного оператора защищаются брандмауэрами от разных производителей, которые разрешают только выделенный доступ к его внутренним системам, необходимым для функционирования Выпускающего УЦ. Итоговый уровень безопасности постоянно проверяется с помощью целенаправленных попыток проникнуть во внутреннюю сеть «Сименс» через независимые подразделения «Сименс» в соответствии с графиками, не известными доверенному оператору.

### 6.9 Процесс присвоения отметок времени

Указано в ЗПС Корневых УЦ.

# 7 Сертификат, профили CRL и OCSP

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

### 7.1 Профиль сертификата

Подробное описание профилей Выпускающего УЦ можно загрузить по ссылке

### 7.2 Профиль CRL

Подробное описание политик 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 к Регламенту УЦ.

## A.2 Сокращения

Указано в Приложении к Регламенту УЦ.